Ruijie RG-WLAN Series Access Controllers

AC_RGOS 11.9(6)W6B1

Configuration Guide

Document Version: V1.1
Date: June 4, 2025
Copyright © 2025 Ruijie Networks

Copyright

Copyright © 2025 Ruijie Networks

All rights are reserved in this document and this statement.

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

 and  trademarks are owned by Ruijie Networks.

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

Disclaimer

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

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

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

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

Personal Data Statement

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

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

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

Preface

Intended Audience

This document is intended for:

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

Technical Support

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

Conventions

1. Conventions

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

Convention	Description
//	A line starting with double slashes is comments.

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

Specification

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

3. Notes

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

Configuring Basic Configuration

1. Configuring CLI
2. Configuring Basic Management
3. Configuring Lines
4. Configuring HTTP Service
5. Configuring Syslog
6. Configuring Software Authorization Management
7. Configuring USB
8. Configuring Package Management
9. 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.

Protocols and Standards

N/A

1.2 Applications

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

1.2.1 Configuring and Managing Network Devices Through the 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

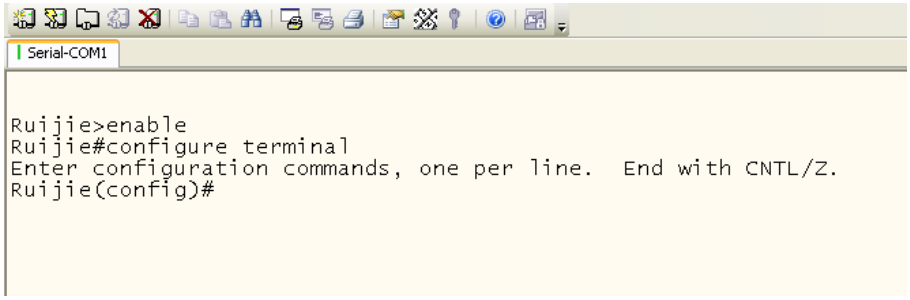


Remarks	A is the network device to be managed. PC is a terminal.

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 the 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 help information of the system during CLI configuration.
Abbreviated Commands	If the input string can be used to identify a unique command, you do not need to enter the full string of the command.
No and Default Forms of Commands	You can use the **no** form of a command to disable a function or perform the operation opposite to the command, or use the **default** form of the command to restore default settings.
Prompts Indicating Incorrect Commands	An error message will be displayed if an incorrect command is entered.
Historical Commands	You can use shortcut keys to display or call history commands.
Featured Editing	The system provides shortcut keys for editing commands.
Searching and Filtering of the Show Command Output	You can run the **show** command to search for or filter specified commands.
Command Alias	You can configure the alias of a command to replace the command.

1.3.1 Accessing the 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 being used for the first time, the network device can be connected only through the console port, which is called out-of-band management. After performing the configuration, you can connect and manage the network device through Telnet.

1.3.2 Command Modes

A device provides many commands. The commands are classified by function to facilitate the use of commands. The CLI provides several command modes, and all commands are registered in one or more command modes. You must first enter the command mode of a command before using this command. Different command modes are interconnected yet distinct from one another.

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

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

Using commands in a specified configuration mode such as the global or interface configuration mode will affect the configuration in use. If you save the configuration, these commands will be saved and executed next time the system is restarted. You must enter the global configuration mode before entering another configuration mode, such as the 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 mode	Enter the user EXEC mode by default when accessing a network device.	Hostname>	Run the **exit** command to exit the user EXEC mode. Run the **enable** command to enter the privileged EXEC mode.	Use this command mode to conduct basic tests or display system information.
Privileged EXEC mode	In User EXEC mode, run the **enable** command to enter Privileged EXEC mode.	Hostname#	Run the **disable** command to return to the user EXEC mode. Run the **configure** command to enter the global configuration mode.	Use this command mode to check whether the configuration takes effect. This mode is password protected.
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 the privileged EXEC mode. Run the **interface** command to enter the interface configuration mode. When using the **interface** command, you must specify the interface. Run the **vlan** *vlan_id* command to enter the VLAN configuration mode.	Using commands in this mode will affect global parameters of the network device.

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

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 (?) following a keyword of a command to list the next keyword or variable associated with the keyword.

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 (?) following 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.

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.

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 sufficient portion of it to identify the command keyword.

For example, to run the **interface** *gigabitEthernet 0/1* command in the configuration mode of GigabitEthernet 0/1, enter the following abbreviated command.

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

1.3.5 No and Default Forms of Commands

Most commands have the **no** form. Typically, the **no** form of a command 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** form is used to enable a disabled feature or a feature that is disabled by default.

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

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

1.3.6 Prompts Indicating Incorrect Commands

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

The following table lists common CLI error messages.

Error Message	Description	How to Obtain Help
% Ambiguous command: "show c"	The input characters are insufficient for identifying a unique command.	Re-enter the command, and enter a question mark (?) following 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 Historical Commands

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

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

The standard terminals such as VT100 series support arrow keys.

1.3.8 Featured Editing

When editing a command line, you can use the keys or shortcut keys listed in the following table.

Function	Key or Shortcut Key	Description
Move the cursor on the editing line.	Left arrow key or **Ctrl+B**	Move the cursor to the previous character.
	Right arrow key or **Ctrl+F**	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.
	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.

When the editing cursor is close to the right boundary, the command line shifts left by 20 characters, with the hidden part at the front replaced by the symbol ($). You can use specific keys or shortcuts to move the cursor to preceding characters or return to the beginning of the command line.

For example, the **access-list** command may exceed the width of one screen. As the cursor approaches the end of the line for the first time, the command line shifts left by 20 characters, with the hidden part at the front replaced by the symbol ($). This shift by 20 characters occurs each time the boundary is approached.

```
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 beginning of the command line. At this point, the hidden part at the end of the command line will be replaced by the symbol ($).

```
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 (|). Up to 32 filtering conditions can be defined in the command. You can select the searching or filtering rules and contents (character or string) following the vertical line (|). 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 simplify 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 Step

Displaying Default Alias

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

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

The 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 ir 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.

```
*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 for network device management. It describes how to manage, monitor, and maintain network devices.

1.2 Applications

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

1.2.1 Network Device Management

Scenario

Network device management described in this document is performed through the CLI. A user logs in to network device A from a terminal and runs commands on the CLI to manage device configurations.

Figure 1-1



1.3 Features

Basic Concepts

TFTP

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

AAA

AAA is short for authentication, authorization and accounting.

Authentication refers to verification of user identities and network services.

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

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

RADIUS

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

Telnet

Telnet is a terminal emulation protocol in the TCP/IP protocol suite that 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. A Telnet connection is established between the local PC and a remote host.

System Information

System information includes the system description, power-on time, hardware and software versions, and control-layer and boot-layer software versions.

Hardware Information

Hardware information includes 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 numbers of physical ports.

Overview

Feature	Description
User Access Control	Controls terminals' access to network devices on the Internet based on passwords and privilege levels.
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	Configures system parameters including the clock, banner, and console baud rate.
Displaying Configurations	Displays system configurations, including the configurations that the system is running and device configurations stored in the nonvolatile random access memory (NVRAM).
Telnet	Provides the standard governing remote login and virtual terminal communication on the Internet.
Restart	Introduces system restart. Telnet is an application-layer protocol in the TCP/IP protocol suite.
Running Batch File Commands	Runs commands stored in the batch file.
Character Set Encoding	After an STA enters a command in the CLI, the command is automatically converted into a command in the unified character set encoding format before delivery.
Configuring Active Backup of the Running Configuration File to a Remote Server	Configures the device to automatically backs up the running configuration file to the remote server when the device running configuration changes.

1.3.1 User Access Control

User access control refers to control of terminals' access to network devices on the Internet based on passwords and privileges.

Working Principle

Privilege Level

Sixteen privilege levels are defined ranging from 0 to 15 for the 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 the 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 the privilege level requires the input of the password of the target level, whereas a decrease in the 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 to ensure security.

Command Authorization

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

Related Configuration

Configuring a Simple Encrypted Password

Run the **enable password** command.

Configuring a Secure Encrypted Password

- Run the **enable secret** command.
- A secure encrypted password is used to control 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 to ensure security.

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 or 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 the level to obtain access to commands at different privilege levels.
- Run the **login privilege log** command to enable the log information prompt for raised user privilege level.

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.

1.3.2 Login Authentication Control

In login authentication with AAA disabled, the input password is checked against the configured line password. If they are consistent, a user can access the network device. In local authentication mode, 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 when AAA is disabled.
- Perform this configuration on each 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 terminated 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 with 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.

1.3.3 Basic System Parameters

System Time

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

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

Configuring a System Name and Command Prompt

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

Banner

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

- Daily notification is displayed on all terminals connected to network devices upon 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 a network device through a console port. When a network device is used for the first time, the configuration must be performed through the console port. The serial port's baud rate can be changed as needed. 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 with remote hosts). A connection will be ended when no input is detected during the timeout time.

Related Configuration

Configuring the System Date and Clock

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

Updating the Hardware Clock

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

Configuring a System Name

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

Configuring a Command Prompt

Run the **prompt** command.

Configuring Daily Notification

- By default, no daily notification is configured.

- Run the **banner motd** command to configure daily notification.
- Daily notification is displayed on all terminals connected to network devices upon 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 9600 bps.

1.3.4 Displaying Configurations

System configurations include the configurations that the system is running and 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. When the system is started, a component process is restarted, and a hot patch is executed, the configurations collected during this period may be inaccurate due to the component's unstable status. For example, the configurations of a component may 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 running or the configurations on an interface or all interfaces.

Displaying Startup Configurations

Run the **show startup-config** command to display configurations executed during device startup.

Storing Startup Configurations

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

1.3.5 Telnet

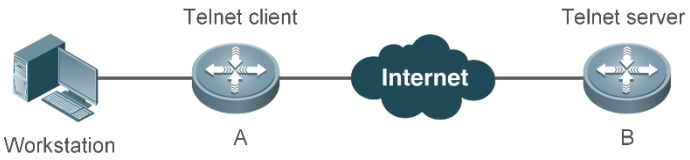
Working Principle

Telnet is an application-layer protocol in the TCP/IP protocol suite. 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 1-2, a user's 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 1-2



Related Configuration

Enabling the Telnet Client Service

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

Enabling the Do Telnet Client Service

Run the **do telnet** command to log in to a remote device 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

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

1.3.6 Restart

The scheduled 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 minutes. You can specify the interval name to represent 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 become invalid if the system is restarted before the plan takes effect.

⚠ The span between the restart time and current time cannnot exceed 31 days, and 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 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.

1.3.7 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. The commands can be placed in a batch file according to configuration steps. Executing the file will complete all configurations.

ℹ 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 commands in a batch file.
- Use this command to configure multiple commands in batch for a function, simplifying user operations.

1.3.8 Character Set Encoding

The character set encoding function enables the device to specify a unified character set encoding format. After a client enters a command in the CLI, the command is automatically converted into a command in the unified character set encoding format before delivery.

ℹ When current running configurations in different formats exist on a device, you can set a unified character set encoding format only after manually delete running configurations that are not in the unified character set encoding format.

Related Configuration

Setting the Character Set Encoding Format

Run the **language character-set** { **UTF-8** | **GBK** | **default** } command to set the character set encoding format.

The value **default** indicates that mixed codes are supported.

Displaying the Character Set Encoding Format

Run the **show language character-set** command to display the current character set encoding format.

1.3.9 Configuring Active Backup of the Running Configuration File to a Remote Server

After active backup of running configurations to a remote server is configured, the device automatically backs up the running configuration file to the remote server when the device running configuration changes.

When the running configuration file is backed up to the remote server, NETCONF sends real-time configuration update notifications. Only the HTTPS protocol is supported. A remote HTTPS file server needs to be set up in advance. Only one file server can be configured. To replace the existing file server, delete the existing file server and then configure a new one.

Related Configuration

Enabling Active Backup of the Running Configuration File

Run the **auto-backup running-config** command to enable active backup of the running configuration file and enter the backup configuration mode.

Configuring Active Backup of the Running Configuration File to a Remote Server

Run the **server** *ipv4-address* **port** *port-number* **transport https** [**username** *username* **password** { [**0**] *password* | **7** *encrypted-password* }] [**remote-path** *path*] command to configure a remote server.

1.4 Configuration

Configuring Passwords and Privileges	(Optional) It is used to configure passwords and command privilege levels.	
	enable password	Configures a simple encrypted password.
	enable secret	Configures a secure encrypted password.
	enable	Raises a user privilege level.
	login privilege log	Outputs 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.

Configuring Login and Authentication	(Optional) It is used to configure different login modes and authentication modes.	
	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.
	do telnet	Enables the Do Telnet client.
	enable service telnet-server	Enables the Telnet server.
	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 a line.
	ip telnet source-interface *interface-name*	Specifies the IP address of the interface as the source IP address of a 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.
	Bannerlogin *c message c*	Configures a login banner.
	banner prompt-timeout *c message c*	Configures the 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 system configurations (running-config) to a specific directory.
	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 batch file commands.	
	execute { [**flash:**] *filename* }	Runs batch file commands.
Configuring the Character Set Encoding Format	⚠ (Optional) It is used to configure the language character set.	
	language character-set { **UTF-8** | **GBK** | **default** }	Configures the language character set.
Configuring Active Backup of the Running Configuration File to a Remote Server	**auto-backup running-config**	Enables active backup of the running configuration file.
	server	Configures active backup of the running configuration file to a remote server.

1.4.1 Configuring Passwords and Privileges

Configuration Effect

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

Notes

- You can use the password configuration command with the **level** option to configure a password for a specific privilege level. After you specify the level and 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 if both simple and secure encrypted passwords are configured.

Configuration Step

Configuring a Simple Encrypted Password

- Optional. Perform this configuration when you need to establish simple encrypted password verification during user switching 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 during user switching 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 to ensure security.

Configuring Command Privilege Levels

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

Raising or Lowering a User Privilege Level

- After logging in to a network device, a user can change the level to obtain access to commands at different privilege levels.
- Run the **enable** or **disable** command to raise or lower a user privilege level respectively.
- Run the **login privilege log** command to enable the log information prompt for raised user privilege level.

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	**nable password** [**level** *level*] [{ *password* | { **0** [*password*] | **7** *encrypted-password* } }]
Parameter Description	*level*: Indicates a specific user level. *password:* Indicates the password used to enter the privileged EXEC mode. **0***:* Indicates that the password is entered in cleartext.

	7*:* Indicates that the password is entered in ciphertext. *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	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 level-15 simple encrypted password and secure encrypted password are the same, a warning is displayed. If you specify an encryption type and enter a password in plaintext, you cannot re-enter the privileged EXEC mode. An encrypted password cannot be retrieved once being lost. You have to configure a new password.

Configuring a Secure Encrypted Password

Command	**enable secret** [**level** *level*] { *secret* | { [**0** | **5**] *encrypted-secret* } }
Parameter Description	*level*: Indicates a specific user level. *secret:* Indicates the cleartext password used to enter the privileged EXEC mode. **0** | **5**: Indicates the encryption type for a password. **0** indicates no encryption while **5** indicates that a password is encrypted using the MD5 encryption algorithm. *encrypted-password:* Indicates the password text.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure passwords for different privilege levels.

Raising a User Privilege Level

Command	**enable** [*privilege-level*]
Parameter Description	*privilege-level*: Indicates a specific privilege level.
Command Mode	Privileged EXEC mode
Usage Guide	An increase in the privilege level requires 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 decrease in the privilege level does not require password input.

	Use this command to exit the privileged EXEC mode and return to the 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.

Enabling Log Information Prompt for Raised User Privilege Level

Command	**login privilege log**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the monitoring of an increase in user privilege level. This function applies to all terminals.

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. The value range is from 0 to 15. **reset**: Restores the command privilege level to the default level. *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* | **reset** } *command-string* command in global configuration mode.

Specifying a Line Password

Command	**password** [{ [**0**] [*password*] | **7** *encrypted-password* }]
Parameter Description	**0**: Configures 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`

1.4.2 Configuring Login and Authentication

Configuration Effect

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

Configuration Step

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 each device.

Configuring Local Authentication for Line-Based Login

- Mandatory.
- Configure local authentication for line-based login when AAA is disabled.
- Perform this configuration on each 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 when AAA is enabled.
- Perform this configuration on each 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

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

Configuring the Connection Timeout Time

- Optional.
- An established connection will be terminated 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 connected 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.
- When AAA is disabled, and local user information and line-based local authentication are configured, check whether a user is asked to enter the username and password for access to the CLI.
- When AAA is enabled, and local user information and local AAA authentication are configured, check whether a user is asked to enter the username and password input for access to the CLI.
- Run the **show user** command to display information about the users who have logged in to the CLI.
- Telnet clients can connect to devices enabled with the Telnet server.
- When a user presses **enter** on a locked CLI, the user is prompted for password input. The session is unlocked only when the input password is the same as the configured one.
- Run the **show sessions** command to display each 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. **aux**: Sets the login mode to AUX. **login mode**: Indicates the login mode. **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. The value range is from 0 to 15. **reject remote-login**: Rejects remote login by using the account. **web-auth**: Allows only web-based authentication for the account. **pwd-modify**: Allows the account owner to change the password. The parameter 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. The value 0 indicates that the password is input in cleartext, and the value 7 indicates that the password is input in ciphertext. The default is plaintext. **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. The value 0 indicates that the password is input in cleartext, and the value 7 indicates that the password is input in ciphertext. 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 ciphertext string must consist of an even number of characters. This setting is applicable to the scenario where encrypted passwords may be copied and pasted. In other cases, the value 7 is not selected.

Configuring Local Authentication for Line-based Login

Command	**login local**
Parameter Description	N/A
Command Mode	Line configuration mode
Usage Guide	Use this command to configure local authentication for line-based login when 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 when AAA is enabled. The AAA authentication modes, including RADIUS authentication, local authentication, and non-authentication, are used during authentication.

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 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	You can log in to a remote device identified by an IPv4 host name, IPv6 host name, IPv4 address, or IPv6 address in Telnet mode.

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 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.
Command Mode	Privileged EXEC mode, user EXEC mode, or 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. The configuration varies with different models.

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 session information.

Closing a Suspended Telnet Client Connection

Command	**disconnect** *session-id*
Parameter Description	*session-id*: Indicates the suspended Telnet client session ID.
Command Mode	User EXEC mode
Usage Guide	Use this command to close a specific Telnet client session by entering the session ID.

Enabling the Telnet Server

Command	**enable service telnet-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to enable the Telnet server. 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 minutes. *seconds*: Indicates the connection timeout time, in 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 minutes. **output**: Indicates whether to use data output for determining the timeout.
Command Mode	Line configuration mode
Usage Guide	Use this command to configure the timeout time for 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 a 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 type can be the aggregate interface, gigabit interface, loopback interface, null interface, tunnel interface, or VLAN interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Establishing a Telnet Session with a Remote Network Device

Configuration Steps	● Establish a Telnet session with a remote network device at 192.168.65.119. ● Establish a Telnet session with a remote network device at 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:`

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

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

Configuring the Connection Timeout Time

Configuration Steps	Set the connection timeout time to 20 minutes.

	`Hostname# configure terminal//Enter the global configuration mode.`
	`Hostname# line vty 0 //Enter the 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.

1.4.3 Configuring Basic System Parameters

Configuration Effect

Configure basic system parameters.

Configuration Step

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 more 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. The value range is from 1993 to 2035. The 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 this command is configured, the time of the software clock will overwrite that of the hardware clock.

Configuring the System Name

Command	**hostname** *name*
Parameter Description	*name*: Indicates the system name, which must consist of printable characters and cannot exceed 63 bytes.
Command Mode	Global configuration mode
Usage Guide	To restore the default system name, 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 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 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	After entering the delimiter and pressing **enter**, you can start entering the text. To conclude text input, you need to type the delimiter again followed by pressing **enter**. Note that any characters entered after the concluding delimiter will be discarded by the system. The delimiter letters should not appear in the text of the notification, and the text length cannot exceed 2047 bytes.

Configuring a Login Banner

Command	**banner login** *c message c*
Parameter Description	*c*: Indicates a delimiter, which can be any character, such as &.
Command Mode	Global configuration mode
Usage Guide	After entering the delimiter and pressing **enter**, you can start entering the text. To conclude text input, you need to type the delimiter again followed by pressing **enter**. Note that any characters entered after the concluding delimiter will be discarded by the system. The delimiter letters should not appear in the text of the banner, and the text length cannot exceed 2047 bytes. To remove the login banner configuration, run the **no banner login** command in global configuration mode.

Configuring the Timeout Message to Notify Timeout

Command	**banner prompt-timeout** *c message c*
Parameter Description	*c*: Indicates the separator of the message. Delimiters are not allowed in the message. *message*: Indicates the content of the message.
Command	Global configuration mode

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*: Indicates the separator of the message. Delimiters are not allowed in the message. *message*: Indicates the content 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 bps. The serial port baud rate can be set to 9600 bps, 19200 bps, 38400 bps, 57600 bps, or 115200 bps. The default is 9600 bps.
Command Mode	Line configuration mode
Usage Guide	You can configure the asynchronous line baud rate as needed. The **speed** command is used to configure receive and transmit rates for the asynchronous line.

Saving System Configurations to a Specific Directory

Command	**write** [**memory** | **terminal**]
Parameter	**memory**: Writes system configurations to the NVRAM. It has the same effect as running the **copy**

Description	**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 this command is widely used. If the device where the file is stored exists, the system automatically creates a file and writes the system configurations to the file. If the device does not exist, for example, 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 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 a 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 a 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
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
```

1.4.4 Enabling and Disabling a Specific Service

Configuration Effect

Dynamically adjust system services when the system is running, and enable and disable specific services (SNMP agent, SSH server, and Telnet server).

Configuration Step

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

- 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 status.

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. IPv4 and IPv6 services are also enabled with this service. **telnet-server:** Enables or disables the Telnet server. IPv4 and IPv6 services are also enabled with this service. **snmp-agent:** Enables or disables the SNMP agent. IPv4 and IPv6 services are also enabled 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

Configuration Steps	Enable the SSH server.
	`Hostname# configure terminal //Enter the global configuration mode.` `Hostname(config)#enable service ssh-server //Enable the SSH server.`
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.

1.4.5 Configuring a Restart Policy

Configuration Effect

Configure a restart policy to restart a device as scheduled.

Configuration Step

Configuring Direct Restart

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

Configuring Scheduled 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. The value range is from 1 to 12. *day*: Indicates a date. The value range is from 1 to 31. *year*: Indicates a year. The value range is from 1993 to 2035. The abbreviation is not supported.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to enable a device to restart at a specific time.

1.4.6 Running Batch File Commands

Configuration Effect

Run commands in a batch file.

Configuration Step

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 a batch file.
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to execute multiple commands in batch for a function, simplifying user operations.

1.4.7 Configuring the Character Set Encoding Format

Configuration Effect

A unified character set encoding format is used on a device.

Notes

None

Configuration Step

Setting a Character Set Encoding Format

Run the **language character-set** command to set a character set encoding format.

When current running configurations in different formats exist on a device, you can set a unified character set encoding format only after manually delete running configurations that are not in the unified character set encoding format.

Verification

Run the **show language character-set** command to display the specified character set encoding format.

Related Commands

Command	**language character-set** { **UTF-8** | **GBK** | **default** }
Parameter Description	**UTF-8**: Sets the character set encoding format to UTF-8. **GBK**: Sets the character set encoding format to GBK. **default**: Sets the character set encoding format to the default format (mixed codes supported).
Command Mode	Global configuration mode
Usage Guide	Run this command to use a unified character set encoding format on a device.

Common Errors

None

1.4.8 Configuring Active Backup of the Running Configuration File to a Remote Server

Configuration Effect

After active backup of the running configuration file to a remote server is configured, the device automatically backs up the running configuration file to a remote server when the device running configuration changes.

Notes

- This command is used to configure active backup of the running configuration file. When the running configuration is changed, the device checks the change in the running configuration file one minute later. If the running configuration file is changed, the device backs up the current running configuration file to the remote server. If the configuration is consecutively changed at an interval of one minute, the device backs up the running configuration one minute after the last change or five minutes after the first change.
- When the device restarts, it backs up the running configurations to the remote server once.
- When the running configuration file is backed up to the remote server, NETCONF sends real-time configuration update notifications.
- Only the HTTPS protocol is supported. A remote HTTPS file server needs to be set up in advance.
- Only one file server can be configured. To replace the existing file server, delete the existing file server and configure a new one.

Configuration Steps

(1) Enter the privilege EXEC mode.
enable

(2) Enter the global configuration mode.
configure terminal

(3) Enable active backup of the running configuration file and enter the backup configuration mode.
auto-backup running-config
By default, this function is disabled.

(4) Configure active backup of the running configuration file to a remote server.
server ipv4-address port *port-number* **transport https** [**username** *username* **password** { [0] *password* | 7 *encrypted-password* }] [remote-path path]
By default, this function is disabled.

Verification

N/A

1.5 Monitoring

Displaying

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

1 Configuring Lines

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 the console terminal line (CTY), teletype terminal line (TTY), auxiliary line (AUX), and virtual terminal line (VTY).

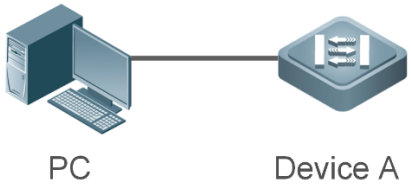
1.2 Applications

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

1.2.1 Accessing a Device Through the Console

Scenario

Figure 1-1



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

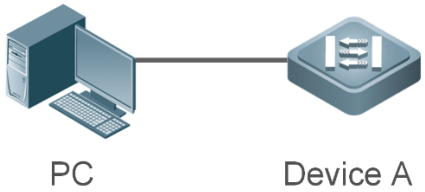
Deployment

The network management station connects to the console port of a network device through a serial cable. Using the console software (HyperTerminal 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 the VTY

Scenario

Figure 1-2



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

Deployment

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

1.3 Features

Basic Concepts

CTY

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

Overview

Feature	Description
Basic Features	Configures a terminal, and 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 a network device, the corresponding terminal line is occupied. You can run the **show user** command to display the connection status of these terminal lines. To disconnect the terminal from the network device, run the **clear line** command to clear the terminal line. After the terminal line is cleared, corresponding connection (such as Telnet and SSH) is terminated, the CLI exits, and the terminal lines restore to the unoccupied status. You can reestablish 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 five 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 the 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 an 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 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 an 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 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 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 the Line Configuration Mode

Configuration Effect

Enter the line configuration mode to configure other functions.

Configuration Step

Entering the Line Configuration Mode

- Mandatory.
- Unless otherwise specified, enter the 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 or 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 range is 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

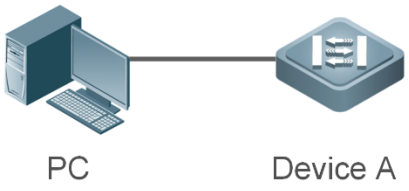
Command	**show line** { **console** *line-num* | **vty** *line-num* **|** *line-num* }
Parameter Description	**console**: Indicates the console port. **vty**: Indicates a virtual terminal line, which supports Telnet or SSH. *line-num*: Indicates the line to be displayed.
Command Mode	Privileged EXEC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

Verification

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

Configuration Example

Configuring the Number of VTY Terminals

Scenario Figure 1-3	
Configuration Steps	• Connect the PC to 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 the global configuration mode and run the **line vty** command to increase the number of VTY terminals to 36.
Device 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.
Device 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 Step

↘ Configuring Login into the Terminal Through an IPv4 ACL

Command	**access-class** { *access-list-number* | *access-list-name* } { **in** | **out** }
Parameter Description	*access-list-number*: Specifies the ACL number. A standard IP ACL number is from 1 to 99 and from 1300 to 1999. An extended IP ACL number is from 100 to 199 and from 2000 to 2699. *access-list-name*: Specifies the ACL name. **in**: Filters incoming connections. **out**: Filters 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 accounting. The value range is from 0 to 15. Information needs to be recorded for execution of commands of a specified level. **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	*level*: Indicates the level of commands that need authorization. The value range is 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 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: Indicates the ASCII decimal value of the hot key that disconnects terminal service connections. The value range is from 0 to 255.
Command Mode	Line configuration mode
Usage Guide	This command is used to configure the hot key for disconnecting terminal connections as needed. 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*: Indicates the ASCII value in decimal notation of the user-defined character for exiting the current terminal. The value 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. The value range is from 0 to 256.
Command Mode	Line configuration mode
Usage Guide	N/A

Configuring Login into the Terminal Through an IPv6 ACL

Command	**ipv6 access-class** *access-list-name* { **in** | **out** }
Parameter Description	*access-list-name*: Specifies the ACL name. **in**: Filters incoming connections. **out**: Filters 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-length*: Indicates the line height. The value range is 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 a 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. The value range is 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: Indicates the ASCII value in decimal notation of the user-defined character for exiting the current terminal. The value 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. The value range is 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-engath*: Indicates the line height. The value range is from 0 to 512.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuring the Location Description for a 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. The value range is 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 value 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, in seconds. The value range is from 1 to 300.
Command Mode	Line configuration mode

Usage Guide	N/A

Specifying 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

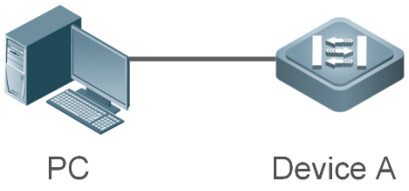
Command	**width** *screen-width*
Parameter Description	*screen*-width: Indicates the maximum number of columns displayed in a single line, that is, the line width. The value range is from 0 to 256.
Command Mode	Line configuration mode
Usage Guide	N/A

Verification

- Run the **show line** command to display the 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 AP1 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.
AP1	`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.

AP1

```
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

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

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

Displaying

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

1 Configuring HTTP Service

1.1 Overview

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

The 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 protects the device against main-in-the-middle attacks. 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 Applications

Application	Description
HTTP Application Service	Devices are managed based on web.
HTTP Remote Upgrade Service	HTTP remote upgrade is used to upgrade files.

1.2.1 HTTP Application Service

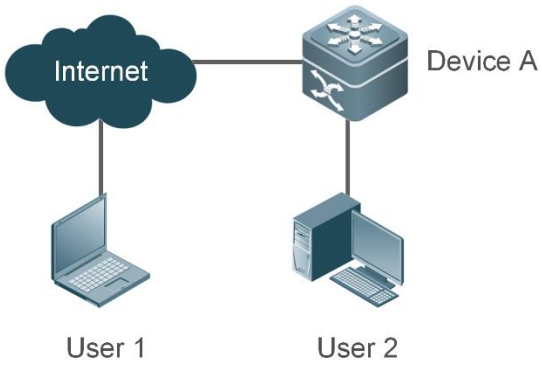
Scenario

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

The following figure is used here to describe web management.

- You can remotely access devices on the Internet or configure and manage devices on the Local Area Network (LAN) by logging in to the web server.
- You can choose to enable the HTTPS or HTTP service independently or enable both of them.
- You can also access the HTTP service of devices by setting and using HTTP/1.0 or HTTP/1.1 in the browser.

Figure 1-1



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

Deployment

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

1.2.2 HTTP Remote Upgrade Service

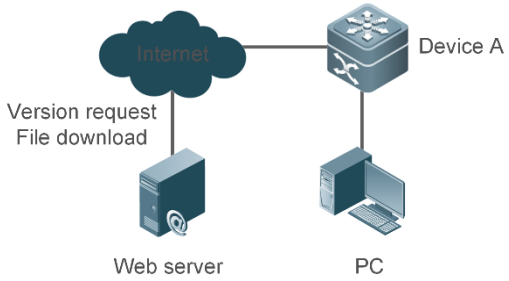
Scenario

The HTTP remote upgrade service allows a device to connect to a remote HTTP server as a client and upgrade the local files by obtaining files from the server.

As shown in the following figure, you use the HTTP remote upgrade service to upgrade files.

- The device remotely accesses the upgradeable files from the server at a scheduled time every day.
- The latest files are downloaded from the server and the upgrade device is updated.

Figure 1-1



Deployment

When the device runs HTTP, you can send commands directly to the device through a browser to obtain the latest upgradeable files from the web server.

1.3 Features

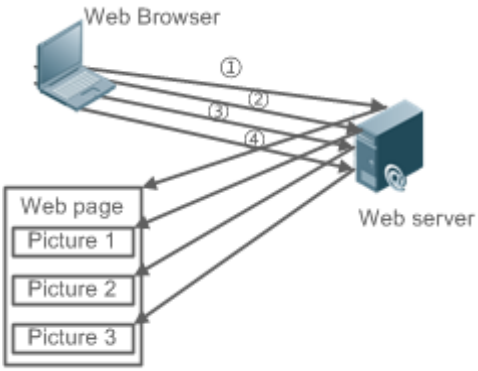
Basic Concepts

HTTP Service

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

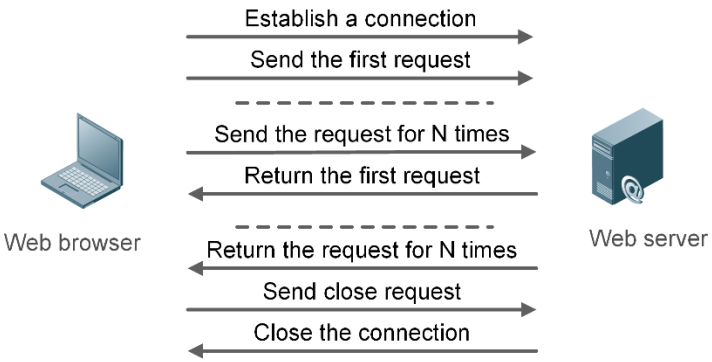
For example, a web page may require many pictures. However, the web page contains not real picture contents but URLs of the pictures. In this case, the browser sends multiple requests during access. Each request requires establishment of an independent connection and each connection is completely isolated. Establishing and releasing connections is troublesome, which severely affects the performance of the client and server, as shown in the following figure.

Figure 1-2



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

Figure 1-3



The device supports both HTTP/1.0 and HTTP/1.1.

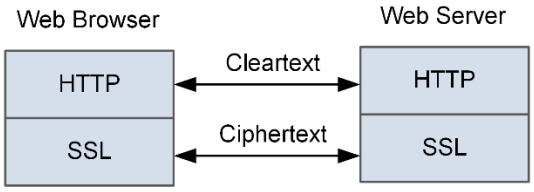
The HTTP version that can be used by a device is decided by the web browser.

HTTPS Service

The HTTPS service adds SSL based on the HTTP service. 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 intercepted
- Maintaining data integrity and ensuring that data is not changed during transmission

Figure 1-4



HTTP Upgrade Service

HTTP upgrade includes local and remote HTTP upgrade:

- During local upgrade, a device serves as an HTTP server. You can log in to the device through a web browser and upload upgrade files to the device to realize file upgrade on the device.
- During remote upgrade, a device is connected to a remote HTTP server as a client and realizes local file upgrade by obtaining files from the server.

Features

Feature	Description
HTTP Service	You 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.
HTTP Remote Upgrade Service	The device is connected to a remote HTTP server as a client and upgrades local files by obtaining files from the server.
HTTP Local Upgrade Service	The files to be upgraded are uploaded to the device, achieving the upgrade of files on the device.

1.3.1 HTTP Service

HTTP is a service provided for web management. You can log in to devices through web pages to configure and manage devices.

Working Principle

Web management covers web clients and 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. Information exchange between the client and server is as follows:

- A TCP connection is established between the client and server. The default port IDs of the HTTP service and HTTPS service are 80 and 443, respectively.
- The client sends a request message to the server.
- The server resolves the request message sent by the client. The request includes obtaining a web page, executing a CLI command, and uploading a file.
- After executing the request, the server sends a response message to the client.

Related Configuration

Enabling the HTTP Service

By default, the HTTP service is disabled.

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

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

Configuring HTTP Authentication Information

By default, the system creates the **admin** and the **guest** account. The accounts 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 **admin** account owns all permissions on the Web client and can edit other management accounts and authorize the accounts to access pages. The **guest** account corresponds to the level 2 permission. The **guest** account can only view the homepage. The new accounts that are added correspond to the level 1 permission.

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

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

Configuring an HTTP Service Port

By default, the HTTP service port ID is 80.

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

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

Configuring an HTTPS Service Port

By default, the HTTPS service port ID is 443.

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

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

1.3.2 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.

1.3.3 HTTPS Service Certificate

An HTTPS service certificate is used to authenticate a server and encrypt data transmission. You 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. You 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 determine 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.

1.3.4 HTTP Remote Upgrade Service

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

Working Principle

- When the device attempts to connect to the server, the device first attempts to connect to the server address configured by the user. If it fails to connect, it attempts to connect to the server address in the local upgrade record file.
- The device sends version numbers of its various service modules to the server.
- The server analyzes information and provides a list of downloadable files.
- The device connects to the file server according to the list and downloads the files that need to be upgraded. You can connect to different servers to download different files.
- The device upgrades the files.

1.3.5 HTTP Local Upgrade Service

The device serves as the HTTP server. Users log in to the device through a Web browser and upload the files to be upgraded (including the component package and web package) to the device or directly upload files to the device through the Trivial File Transfer Protocol (TFTP).

Working Principle

- A component package or web package is uploaded through the local upgrade function in the web management system.
- After receiving the file package, the device checks the version for validity.
- After the file check is successful, if the file is a web package, the device performs the upgrade directly; if the file is a component package, a user determines whether to perform the upgrade in the browser by restarting the device.

1.4 Configuration

Configuration	Description and Command	
Configuring the HTTP Service	(Mandatory) It is used to enable the HTTP service.	
	enable service web-server	Enables the HTTP service.
	webmaster level	Configures HTTP authentication information.
	http port	Configures an HTTP service port.
	http secure-port	Configures an HTTPS service port.
Configuring HTTP Redirection to HTTPS	(Optional) It is used to enable automatic HTTP redirection to HTTPS.	
	web-server http redirect-to-https	Configures HTTP redirection to HTTPS.
Configuring the Maximum Number of Concurrent Logins Using the Same Account	(Optional) It is used to configure the maximum number of concurrent login using the same account from different clients.	
	http limit	Configures the maximum number of concurrent logins using the same account from different clients.
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.
Configuring HTTP Remote Upgrade	(Mandatory) It is used to realize HTTP remote upgrade.	
	http update server	Configures the HTTP upgrade server.
	http update mode	Configures the HTTP upgrade mode.
	http update time	Configures the HTTP automatic detection time.

Configuration	Description and Command	
	http check-version	Checks upgradeable file information from the HTTP server.
	http update	Upgrades files manually.
Configuring HTTP Local Upgrade	(Mandatory) It is used to implement HTTP local upgrade.	
	upgrade download	Automatically downloads the web package from the server and automatically upgrades the web package.
Allowing AAA Users to Log In to the Web Page	(Mandatory) It is used to allow AAA users to log in to the web page.	
	http authen login local	Allows AAA users to log in to the web page.

1.4.1 Configuring the HTTP Service

Configuration Effect

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

Configuration Step

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.
- You can 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 both HTTP and HTTPS services. By default, both HTTP and HTTPS services are enabled.
Command Mode	Global configuration mode.
Usage Guide	If no keyword or **all** is placed at the end of the command when the command is run, both HTTP and HTTPS services are enabled. If **http** is placed at the end of the command, only the HTTP service is enabled; if **https** is placed 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 keyword is placed at the end of the **no enable service web-server** or **default enable service web-server** command, HTTP and HTTPS services are disabled.

Configuring HTTP Authentication Information

- Unless otherwise specified, 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*: Indicates the permission level bound to a user. *name*: Indicates the user name. *password*: Indicates the user password. **0** | **7**: Indicates the password encryption type. The value 0 indicates no encryption and the value 7 indicates simple encryption. The default value is 0. *encrypted-password*: Indicates the 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 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 level-1 permission.

Configuring an HTTP Service Port

- If an HTTP service port needs to be changed, the HTTP service port must be configured.
- Unless otherwise specified, 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 is 80 and ranges from 1025 to 65535.
- Configure an HTTP service port number to reduce attacks initiated by unauthorized users on the HTTP service.

Command	**http port** *port-number*
Parameter Description	*port-number*: Configures an HTTP service port. The value is 80 and ranges from 1025 to 65535.

Command Mode	Global configuration mode.
Usage Guide	Run the command to configure 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.
- Unless otherwise specified, 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 is 443 and ranges from 1025 to 65535.
- Configure an HTTPS service port number to reduce attacks initiated by unauthorized users on the HTTPS service.

Command	**http secure-port** *port-number*
Parameter Description	*port-number*: Configures an HTTPS service port. The value is 443 and ranges from 1025 to 65535.
Command Mode	Global configuration mode.
Usage Guide	Run the command to configure an HTTPS service port.

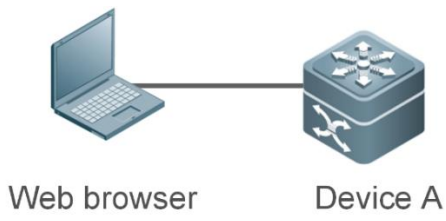
Verification

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

Configuration Example

Managing One Device by Using the 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 unauthorized users on HTTP.

Scenario **Figure 1-5**	
Configuration Steps	• Enable both HTTP and HTTPS services. • Set the HTTP service port ID to 8080 and the HTTPS service port ID to 4430.

Device A	`Hostname#configure terminal`
	`Hostname(config)# enable service web-server`
	`Hostname(config)# http port 8080`

	Hostname(config)# http secure-port 4430
Verification	Check the HTTP configuration.
Device A	Hostname# 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.

1.4.2 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 Step

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 the HTTPS service to improve security and reduce information leakage 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 is automatically redirected 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. The HTTP service is automatically redirected to the HTTPS service only when the HTTP and HTTPS services are enabled. Whether this command is supported is subject to devices. If an IP address to be accessed is a Network Address and Port Translation (NAPT) address, the redirection function may become ineffective. To access the device through HTTP, disable NAPT.

	To access the device through HTTPS, use HTTPS directly.

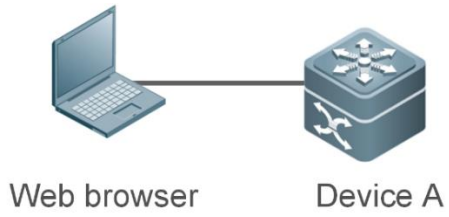
Verification

- 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 HTTP and HTTPS services. ● Configure HTTP redirection to HTTPS.

Device A	`Hostname#configure terminal`
	`Hostname(config)# enable service web-server`
	`Hostname(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***.

Device A	`Hostname#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`

1.4.3 Configuring the Maximum Number of Concurrent Logins Using the Same Account

Configuration Effect

The number of concurrent logins using the same account from different clients (with different IP addresses) is limited. For example, if the maximum number of concurrent logins is set to 2, the account can be logged in from two different clients simultaneously.

Configuration Steps

Configuring the Maximum Number of Concurrent Logins Using the Same Account

- The maximum number of concurrent logins using the same account is 10 by default.
- You can configure the concurrent logins using the same account to restrict the logins from different IP addresses. This enhances access security and reduces the risk of information leakage and malicious attacks.

Command	**http limit** *limit-number*
Parameter Description	*limit-number*: Indicates the maximum number of concurrent logins using the same account. The value range is from 1 to 256.
Command Mode	Global configuration mode
Usage Guide	1. The login count is calculated based on the IP addresses of the devices where the same account is logged in. If the account is logged in on multiple pages from the same device, the login count is considered as 1 because the IP address is the same. If the account is logged in from two different devices at the same time, the login count is considered as 2, and so on. The login limit is the configured maximum number of concurrent logins. 2. When the login count reaches the upper limit, a login failure message will be displayed when a new client attempts to log in to the account.

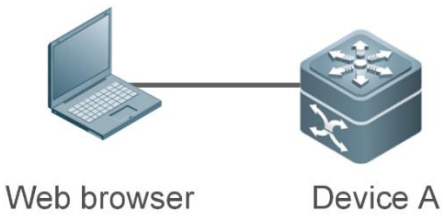
Verification

- When the maximum number of concurrent logins is set to 1, a user has logged in to the web system using an account on PC1 and attempts to log in using the same account on PC2, a login failure occurs.
- After the account is logged out on PC1, it can be logged in on PC2.
- After the login times out on PC1, the account can be logged in on PC2. (If you directly close the web page, you can only wait for the login timeout or manually log out from PC1. Otherwise, the login restriction cannot be removed.)
- Run the **http limit** command to set the maximum number of concurrent logins to 2, the same account can be logged in on PC2, but a login failure will occur on PC3.
- Run the **show web-server status** command to display the maximum number of concurrent logins. The configuration is not displayed when the default value is used.

Configuration Examples

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

To enhance security, the maximum number of concurrent logins using the same account is set to 1.

Scenario Figure1-2	
Configuration Steps	Set the maximum number of concurrent logins using the same account to 1.
Device A	`Hostname#configure terminal` `Hostname(config)#http limit 1`
Verification	● Run the **show web-server status** command to display the web server configuration. ● After logging in to a web account on a device, you cannot log in to the web management system

	using the same account on another device. The system prompts that the number of concurrent logins has reached the upper limit.

Device A	`Hostname#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`
	`User login is limited to (1)`

1.4.4 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 Step

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 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 to access 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.

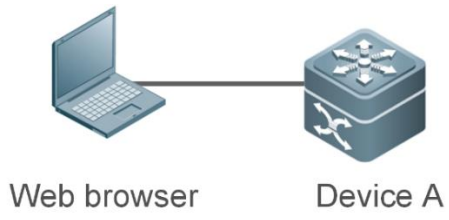
Command	**web-server https certificate** { **pem** *cert-filename* **private-key** *key-filename* } | { **pfx** *cert-filename* } [**password** *password-text*]
Parameter Description	**pem**: Imports the certificate file and private key file in pem. format. **pfx**: Imports the certificate file in pfx. format from which a private key is exported. *cert-filename*: Indicates the file name in the **flash:** partition. *key-filename*: Indicates the private key file name in the **flash:** partition. **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 or private key file to the **flash:** partition before running the command to install the third-party HTTPS service certificate. Then you can delete the certificate or private key file from the **flash:** partition. Run the **no web-server https certificate** command to remove the installed HTTPS service certificate. Then 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 devices. After the HTTPS service certificate is installed, the browser may require you to add the trust certificate again before you continue access to the wWeb 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 information about 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.

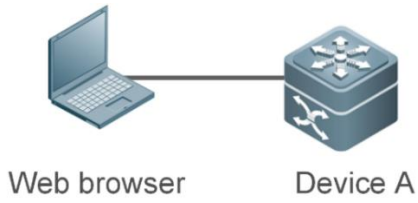
Device A	`Hostname#configure terminal`
	`Hostname(config)# web-server https generate self-signed-certificate`
	`RSA key modulus bits (1024~4096) [2048]:`
	`Common Name (e.g. server IP) [Self-Signed-600B16C2]:`
	`% Generate self-signed certificate successfully`

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

Device A	`Hostname#show web-server https certificate information`
	`Source: Default`
	`Certificate:`
	`  Data:`
	`  Version: 3 (0x2)`
	`  Serial Number: 1 (0x1)`
	`  Signature Algorithm: sha256WithRSAEncryption`
	`  Issuer: CN=Self-Signed-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:`
	……

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.** The TFTP server is enabled on the PC and the certificate file is in the directory of the TFTP server.

Scenario **Figure 1-6**	
Configuration Steps	● Run the **copy** command to copy the certificate or private key file to the **flash:** partition. ● Run the **web-server https certificate** command to install the HTTPS service certificate.

Device A	`Hostname# copy tftp://192.168.1.1/usercert.pfx flash:usercert.pfx`
	`Press Ctrl+C to quit`
	`!`
	`Copy success.`
	`Hostname#configure terminal`
	`Hostname(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 information about the certificate.
Device A	`Hostname#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:
……
```

1.4.5 Configuring HTTP Remote Upgrade

Configuration Effect

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

Notes

- Before configuring the HTTP upgrade server domain name, users are required to enable the device's DNS function and configure the DNS server address.

Configuration Step

↘ Configuring the HTTP Upgrade Server

- Mandatory if you want to change the server address and port number for HTTP remote upgrade.
- Unless otherwise specified, there is no need to configure the HTTP upgrade server on each device.
- By default, the server address for HTTP remote upgrade is 0.0.0.0 and the port number is 80.
- Use the **http update server** command to configure the address and port number for the HTTP remote upgrade server.
- During HTTP upgrade, the device will try to connect to the server address configured with this command first. If the connection fails, it will try to connect to the locally recorded server addresses one by one. If all servers cannot be connected, the upgrade cannot proceed.

Command	**http update server** { *host-name* | *ip-address* } [**port** *port-number*]
Parameter Description	*host-name*: Indicates the server domain name. *ip-address*: Indicates the IP address of the server. **port** *port-number*: Indicates the server port number. The value range is from 1 to 65535 and the default value is 80.

Command Mode	Global configuration mode
Usage Guide	This command is used to configure the address and port number for the HTTP upgrade server. During HTTP upgrade, the device will try to connect to the server address configured with this command first. If the connection fails, it will try to connect to the locally recorded server addresses one by one. If all servers cannot be connected, the upgrade cannot proceed. The system records one or more upgrade server addresses, which cannot be modified. Whether this configuration is supported depends on the actual product version. The server address can be left unconfigured because the local upgrade record file records possible upgrade server addresses. By default, DNS needs to be enabled and the DNS server address needs to be configured. The IPv6 server address is not supported.

Configuring the HTTP Upgrade Mode

- Mandatory if the manual HTTP upgrade mode is required.
- Unless otherwise specified, the default HTTP upgrade mode is automatic.
- By default, HTTP uses automatic upgrade mode.
- Use the **http update mode** command to configure the HTTP upgrade mode as manual.

Command	**http update mode manual**
Parameter Description	**manual**: Indicates the manual upgrade mode.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the HTTP upgrade mode. This command is used to configure a manual upgrade mode. Run the **no** form of this command to set the HTTP upgrade mode to automatic mode. When the automatic upgrade time arrives, the device will automatically detect the upgradable file information on the server by default and download the files for upgrade. Whether this configuration is supported depends on the actual product version.

Configuring the HTTP Automatic Upgrade Time

- Mandatory if you want to change the HTTP automatic upgrade time.
- If there are no special requirements, the HTTP automatic upgrade time is random by default.
- By default, the HTTP remote automatic upgrade time is a random time within the range of 00:00–23:59.
- The **http update time** command can be used to change the automatic upgrade time, which can only be configured to a specific time each day, accurate to minutes.
- By configuring this command, if the upgrade mode is automatic, the device will check the file version on the server and upgrade the files on the device at a specified time every day.

Command	**http update time daily** *hh*:*mm*

Parameter Description	*hh*:*mm*: Indicates the specific upgrade time, in the format of hour(24-hour clock):minute.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the HTTP automatic upgrade time. The device automatically connects to the web server at the specified time each day to check whether there is any upgradeable file information. The file information obtained can be viewed through the web interface. If the **no** form of the command is executed, the device upgrade time will be a random time within the range of 00:00–23:59. Whether this configuration is supported depends on the actual product version.

Checking Upgradeable File Information from the HTTP Server

- Mandatory if you want to check upgradeable file information on the HTTP server.
- Unless otherwise specified, you do not need to perform this task because automatic upgrade is enabled by default.
- By default, the device is disabled from detecting upgradeable HTTP files.
- The **http check-version** command can be used to detect upgradeable files on the server.
- By configuring this command, you can detect files on the server that are more up-to-date than local files.

Command	**http check-version**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to detect the file types to be upgraded. The detected files are those that are more up-to-date on the server than on the local device. Whether this configuration is supported depends on the actual product version.

Upgrading Files Manually

- Mandatory.
- Unless otherwise specified, configure manual file upgrade on each device.
- The **http update** command can be used to manually upgrade files.

Command	**http update** { **all** | *string* **}**
Parameter Description	**all**: Indicates that all service modules are upgraded. *string*: Indicates the name of the service module to be upgraded.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to manually upgrade a specified service module or all service modules. Whether this configuration is supported depends on the actual product version.

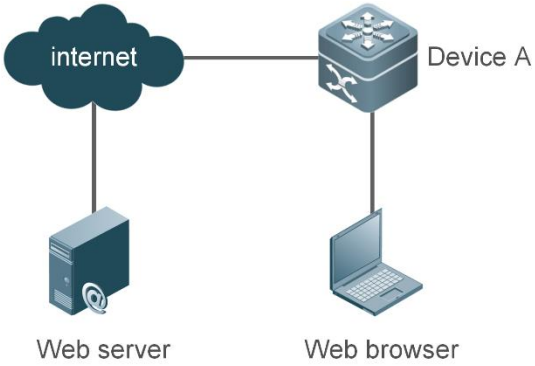
Verification

- Run the **ping** command to verify that the device can establish a connection with the server.
- Run the **http check-version** command to obtain version information about relevant files on the device.

Configuration Example

Upgrading the Files Using HTTP Remote Upgrade

- The device can automatically obtain upgradeable file information from the server and download the files for upgrading at 2:00 a.m. every day.
- Check the currently upgradeable file information.
- The latest files are downloaded from the server and the upgrade device is updated.

Scenario **Figure** 1-3	
Configuration Steps	● Configure DNS information. ● Set the device's scheduled remote monitoring time to 2:00 a.m. ● Obtain upgradeable file information from the remote server. ● Download the files from the server and update them.

Device A	`Hostname#configure terminal`
	`Hostname(config)#ip domain-lookup`
	`Hostname(config)#ip name-server 192.168.58.110`
	`Hostname(config)#http update time daily 02:00`
	`Hostname(config)#http check-version`
	`Hostname(config)#end`
	`Hostname# http update all`

Common Errors

The DNS services are disabled, resulting in the device being unable to establish a connection with the server.

1.4.6 Configuring HTTP Local Upgrade

Configuration Effect

This section describes how to perform an HTTP upgrade through the browser or the **upgrade download** command.

Notes

- If a web package is uploaded by browser and passes the version check, the device directly upgrades the web package to the latest one.
- Run the **upgrade download** command to automatically download the file from the TFTP server and perform automatic upgrade.

Configuration Steps

Downloading a Web Package from the TFTP Server

- Run the **upgrade download** command to download a web package from the TFTP server.
- After the configuration, the device downloads a web package from the TFTP server and performs validity check. If the web package is valid, the device directly upgrades the web package, eliminating the need for a device restart.

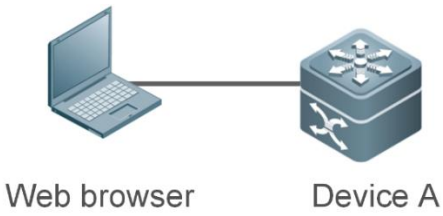
Command	**upgrade download tftp:***path*
Parameter Description	**tftp**: Indicates that the web package is downloaded through the common data port connected to the TFTP server. *path*: Indicates the path of the web package on the TFTP server.
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to download a web package from the TFTP server and automatically upgrade the device the web package.

Verification

You can directly access the web system by browser to view the latest web pages.

Configuration Example

Configuring the Device to Run the Latest Web Package After It Is Obtained from the Official Website

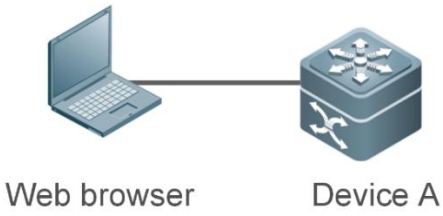
Scenario **Figure1-4**	
Configuration Steps	● Connect the device to a local PC, whose IP address is 10.10.10.13. Configure an IP address 10.10.10.131 in the same network segment for the device. ● Log in to the device through the web system and upload the latest web package to the device.

Device A	`Hostname#configure terminal`
	`Hostname(config)# vlan 1`
	`Hostname(config-vlan)# exit`
	`Hostname(config)# interface vlan 1`
	`Hostname(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0`
	`Hostname(config-VLAN 1)# exit`
	`Hostname(config)# enable service web-server`

	On the PC, use the local upgrade function on the web page to upload the web package for upgrade.
Verification	On the PC, perform web-based authentication again for login and check whether the latest web page

	is displayed.

Running the upgrade download Command to Upgrade a Web Package

Scenario **Figure1-9**	
Configuration Steps	● Connect the device to a local PC, whose IP address is 10.10.10.13. Configure an IP address 10.10.10.131 in the same network segment for the device. ● Enable the TFTP server.

Device A	`Hostname#configure terminal`
	`Hostname(config)# vlan 1`
	`Hostname(config-vlan)# exit`
	`Hostname(config)# interface vlan 1`
	`Hostname(config-VLAN 1)# ip address 10.10.10.131 255.255.255.0`
	`Hostname(config-VLAN 1)# end`
	`Hostname#upgrade download tftp:// 10.10.10.13/web.upd`
	`Press Ctrl+C to quit`
	`!!!!!!!!`
	`download 3896704 bytes`
	`Begin to upgrade the web package...`
	`Web package upgrade successfully.`

Verification	On the PC, perform web-based authentication again for login and check whether the latest web page is displayed.

Common Errors

If the new web package is not updated after you access the web system by browser, the local browser may have a cache. Clear the browser cache and access the web system again.

1.4.7 Allowing AAA Users to Log In to the Web Page

Configuration Effect

- Users can successfully log in to the web page by using usernames and passwords in the local AAA database or remote AAA server, and they have the admin permission after login.

Notes

N/A

Configuration Steps

Allowing AAA Users to Log In to the Web Page

- Optional.
- Configure this function when AAA users need to be authorized to log in to the web page.

Command	http authen login local
Parameter Description	**local**: Allows users in the local AAA database to log in to the web page.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running-config** command to check whether AAA users can log in to the web page.
- An AAA user can log in to the web page successfully and has the admin permission.

Configuration Example

Allowing AAA Users to Log In to the Web Page

Configuration Steps	Allows users in the local AAA database to log in to the web page.
	`Hostname(config)# http authen login local`
Verification	Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`…`
	`http authen login local`
	`…`

1.5 Monitoring

Displaying

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

1 Configuring Syslog

1.1 Overview

During device running, status changes (such as link Up and Down) or abnormal events (such as abnormal packets or processing exceptions) may occur. 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 in the media such as the memory buffer or log files, or sent to a group of log servers on a network so that the administrator can analyze network performance and identify faults based on the log packets. Log packets can be added with the timestamps and sequence numbers and classified by severity so that the administrator can easily read and manage log packets.

Protocols and Standards

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

1.2 Applications

Application	Description
Sending Syslogs to the Console	Monitor syslogs through the console.
Configuring the Device to Send Syslogs to the Log Server	Monitor syslogs through the server.

1.2.1 Sending Syslogs to the Console

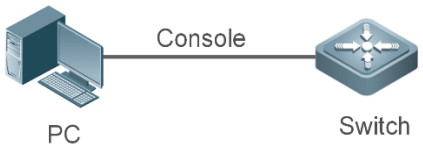
Scenario

Syslogs can be sent to the console, so an administrator can monitor the performance of the system. The requirements are as follows:

1. Send logs of severity 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

Perform the following configurations:

1. Set the severity of logs that can be sent to the console to informational (severity 6).
2. Set the filtering direction of logs to terminal.
3. Set the 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 Configuring the Device to Send Syslogs to the Log Server

Scenario

When the device is configured to send syslogs to the log server, an administrator can easily monitor logs of devices on the server. The requirements are as follows:

1. Send syslogs to the log server at 10.1.1.1.
2. Send syslogs from the source interface Loopback 0 to the log server.
3. Configure the logs that cannot be received. Send the logs of IP address assignment by DHCP to the log server.
4. Configure warning (severity 4) logs that can be sent to the log server.

Figure 1-2 shows the network topology.

Figure 1-2 Network topology



Deployment

Perform the following configurations:

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.
4. Configure the log filtering rules in audit mode to allow the device to send logs of IP address assignment by DHCP and warning (severity 4) logs to the log server.

1.3 Features

Basic Concepts

↘ Classification of Syslogs

Syslogs can be classified into two types:

- Log type
- Debug type

Severities of Syslogs

Eight severities of syslogs are defined in descending order, including emergency, alert, critical, error, warning, notification, informational, and debugging. These severities correspond to eight numerals in the range of 0 to 7. A smaller value indicates a higher severity.

Only logs with a severity that is the same as or higher than the specified severity can be output. For example, if the severity of logs is set to informational (severity 6), logs of severity 6 or higher will be output.

The following table describes the log severities.

Severity	Numerical Value	Description
emergencies	0	Indicates that the system cannot run normally.
alerts	1	Indicates that 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

Syslogs can be output to the console, monitor, server, buffer, and file. The default severity 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 Severity	Description
Console	Console	Debugging (severity 7)	Logs and debugging information are output.
Monitor	Monitoring terminal	Debugging (severity 7)	Logs and debugging information are output.
Server	Log server	Informational (severity 6)	Logs and debugging information are output.
Buffer	Log buffer	Debugging (severity 7)	Logs and debugging information are output. The log buffer is used to store syslogs.
File	Log file	Informational (severity 6)	Logs and debugging information are output. Logs in the log buffer are periodically written into files.

RFC 3164 Log Format

Formats of syslogs may vary with the syslog output direction.

- If syslogs can be output to 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 syslogs can be output to the log server, the syslog format is as follows:

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

For example, if you exit the 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
```

Each field in the log is described as follows.

1. Priority

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

The priority is calculated using the following formula:

Priority = Facility x 8 + Severity

The severity indicates the numerical code of the log severity and the 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 easily. Devices support two syslog timestamp formats: datetime and uptime.

If the device does not have the real time clock (RTC) that 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 has 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 a string of 2 to 20 upper-case characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in log information, and optional in debugging information.

6. Severity

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

7. Mnemonic

This field indicates brief information about the log. The mnemonic is a string of 4 to 32 upper-case characters, which contains upper-case letters, digits, or underscores. The mnemonic field is mandatory in log information, and optional in debugging information.

8. Content

This field indicates the detailed content of the syslog.

RFC 5424 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
```

Each field in the log is described as follows

1. Priority

   The priority is calculated using the following formula:

   Priority = Facility x 8 + Severity

   The severity indicates the numerical code of the log severity and the facility indicates the numerical code of the facility. When the RFC 5424 format is enabled, the default value of the facility field is local0 (16).

2. Version

According to RFC 5424, the version has a fixed value of 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 RFC 5424 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 a string of 2 to 20 upper-case characters, which contain upper-case letters, digits, or underscores. The module field is mandatory in log information, and optional in debugging information.

6. Severity

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

7. Mnemonic

This field indicates brief information about the log. The mnemonic is a string of 4 to 32 upper-case characters, which contains upper-case letters, digits, or underscores. The mnemonic field is mandatory in log information, and optional in debugging information.

8. Structured-Data

Structured-data introduced in RFC 5424 is parsed as a string containing parameter information. Each log may contain no parameter or multiple parameters. If there is no parameter, use the 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 RFC 5424.
enterpriseID	Enterprise ID	The enterprise ID is maintained by the Internet Assigned Numbers Authority (IANA). The enterprise ID of devices has a fixed value of 4881. You can query the enterprise ID at 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 system logging functions.
Syslog Format	Configure the syslog format.
Logging Direction	Configure the parameters in syslogs sent 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 logging, redirection logging, and log statistics collection functions.

Related Configuration

Enabling 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 system performance.

Enabling Log Statistics

By default, log statistics collection is disabled.

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

1.3.2 Syslog Format

Configure the syslog format, including the RFC 5424 log format, timestamp format, sysname, and sequence number.

Related Configuration

Enabling the RFC 5424 Log Format

By default, the RFC 5424 log format is disabled.

After the new format (RFC 5424 log format) is enabled, **service sequence-numbers**, **service sysname**, **service timestamps**, **service private-syslog**, and **service standard-syslog** that are applicable only to the old format (RFC 3164 log format) take ineffective and are hidden.

After the old format (RFC 3164 log format) is enabled, **logging delay-send**, **logging policy**, and **logging statistic** that are applicable only to the RFC 5424 log format take ineffective 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 or 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. 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. 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, buffer, log server, and log files.

Related Configuration

Configuring Synchronization of User Input and Log Output

Synchronization of user input and log output is disabled by default.

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

Configuring the Rate Limit for Logging

By default, logging is not rate-limited.

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

Configuring the Severity of Logs Sent to the Console

By default, the severity of logs sent to the console is debugging (severity 7).

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

Sending Logs to the Monitor Terminal

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

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

Configuring the Severity of Logs Sent to the Monitor Terminal

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

Run the **logging monitor** [*level*] command in global configuration mode to configure the severity 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 severity of logs is debugging (severity 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 severity.

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 Severity of Logs Sent to the Log Server

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

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

Configuring the Facility Value of Logs Sent to the Log Server

If the RFC 5424 log format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC 5424 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 device is enabled to write logs into log files, the severity of logs written into log files is informational (severity 6) by default.

Run the **logging file** { **sata0:***filename* | **flash:***filename* | **usb0**:*filename* | **usb1**:*filename* | **sd0**:*filename* } [*max-file-size*] [level] command in global configuration mode to configure parameters for writing logs into log files, including the type of device where the file is stored, file name, file size, and log severity.

Configuring the Number of Log Files

By default, the number of log files is 16.

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

Configuring the Interval at Which Logs Are Written into Log Files

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

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

Configuring the Storage Time of Log Files

By default, the storage time is not configured.

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

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 when the buffer is full or the timer expires.

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

1.3.4 Syslog Filtering

By default, logs generated by the system are sent in all directions. To view some specified syslogs, use syslog filtering.

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 in combinations to filter out logs sent in various directions, or used 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 filtering rules are output. You may focus on 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 many logs, information is flooded on the terminal interface. If you do not care about this type of logs, you can apply the filter-only mode and configure filtering rules to filter out logs.

The two filtering modes cannot be configured simultaneously.

Filtering Rule

Two filtering rules are available:

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

If the same module, severity, or mnemonic is configured for both the single-match and exact-match rules, the single-match rule takes effect.

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 severity-based logging, delayed logging, and periodical logging. If the RFC 5424 log format is enabled, logs can be sent in all directions, delayed logging is enabled, and periodical logging is disabled by

default. If the RFC 5424 log format is disabled, severity-based logging, delayed logging, and periodical logging are disabled.

Working Principle

Severity-based Logging

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

Delayed Logging

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

If the device generates 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 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 in the local flash memory 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 memory in the device that is used to buffer 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 performance statistic logs and send logs to the remote syslog server in real time. 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. The interval can be set to 0, 15, 30, 60, or 120. The value 0 indicates that periodical logging is disabled.

Related Configuration

Configuring the Severity-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 memory 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 access attempts of users and generates logs.

Working Principle

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

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

Related Configuration

Enabling Logging of Login or Logout Attempts

By default, a device generates logs when users log in or log out of the device.

Run the **logging userinfo** command in global configuration mode to enable logging of login or logout 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 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 logs to notify the administrator of configuration changes.

1.4 Configuration

Configuration	Description and Command	
Configuring the Syslog Format	(Optional) It is used to configure the syslog format.	
	service timestamps [*message-type* [**uptime**| **datetime** [**msec**] [**year**]]]	Configures the timestamp format of syslogs.
	service sysname	Adds the sysname to the syslog.
	service sequence-numbers	Adds the sequence number to the syslog.
	service standard-syslog	Enables the standard syslog format.
	service private-syslog	Enables the private syslog format.
	service log-format rfc5424	Enables the RFC 5424 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 collection.
	logging console [*level*]	Configures the severity of logs displayed on the console.
	logging rate-limit { *number* | **all** *number* | **console** {*number* | **all** *number* } } [**except** [*severity*]]	Configures the rate limit for logging.
Sending Syslogs to the Monitor Terminal	(Optional) It is used to configure parameters for sending syslogs to the monitor terminal.	

Configuration	Description and Command	
	terminal monitor	Enables the monitor terminal to display logs.
	logging monitor [*level*]	Configures the severity 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 severity.
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 [**server**] { *ip-address* | **ipv6** *ipv6-address* } [**via** *mgmt-name*] [**tcp-transport** [**tcp-port** *tcp_port*] [**tls**]]	Configures TCP connection and TLS encryption for the specified port of the log server.
	logging trap [*level*]	Configures the severity 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 severity of logs that can be sent to the log server.
	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 severity.
	logging file numbers *numbers*	Sets the number of log files. The value is 16 by default.
	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	⚠ (Optional) It is used to enable the syslog filtering function.	

Configuration	Description and Command	
Filtering	**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 Severity-based Logging	⚠ (Optional) It is used to configure logging policies for the device to send syslogs based on module and severity.	
	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.
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.
Configuring Periodical Logging	⚠ (Optional) It is used to enable the periodical logging function.	
	logging statistic enable	Enables the periodical logging function.
	logging statistic terminal	Enables periodical display of logs on the console and remote terminal.
	logging statistic mnemonic *mnemonic* **interval** *minutes*	Configures the interval at which logs of a performance statistic object are sent to the server.
Configuring Syslog Monitoring	⚠ (Optional) It is used to configure parameters of the syslog monitoring function.	
	logging userinfo	Enables logging of login or logout attempts.
	logging userinfo command-log	Enables logging of operations.
Synchronizing User Input	⚠ (Optional) It is used to configure synchronization of user input and log output.	

Configuration	Description and Command	
with Log Output	**logging synchronous**	Configures synchronization of user input and log output.

1.4.1 Configuring the Syslog Format

Configuration Effect

Configure the format of syslogs.

Notes

RFC 3164 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.

RFC 5424 Log Format

- After the RFC 5424 log format is enabled, the timestamp is uniform.
- In the RFC 5424 log format, the timestamp may contain the time zone or not. The device supports only the timestamp without the time zone.

Configuration Step

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 RFC 5424 Log Format

- Optional.
- By default, the RFC 5424 log format is disabled.
- Unless otherwise specified, perform this configuration on the device to enable the RFC 5424 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
Usage Guide	Two syslog timestamp formats are available: 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	Global configuration mode

Mode	
Usage Guide	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
Usage Guide	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

Usage Guide	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

Usage Guide	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 RFC 5424 Syslog Format

Command	**service log-format rfc5424**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After the new format (RFC 5424 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 (RFC 3164 log format) become ineffective and are hidden. After the old format (RFC 3164 log format) is enabled, the **logging delay-send**, **logging policy**, and **logging statistic** commands that are applicable only to the RFC 5424 log format become ineffective and are hidden. After log format switchover, the outputs of the **show logging** and **show logging config** commands change accordingly.

Configuration Example

Enabling the RFC 3164 Log Format

Scenario	The timestamp format needs to be configured as follows: 1. Enable the RFC 3164 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 RFC 3164 format. ● Run the **show logging config** command to display the configuration. ● Enter or exit the 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 RFC 5424 Log Format

Scenario	The RFC 5424 format needs to be enabled.
Configuration Steps	Configure the syslog format.
	Hostname# configure terminal Hostname(config)# service log-format rfc5424
Verification	Verify that new syslogs are displayed in RFC 5424 format. ● Run the **show logging config** command to display the configuration. ● Enter or exit the 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 system performance.

Notes

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

Configuration Step

Enabling Logging

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

Enabling Log Statistics Collection

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

Configuring the Severity of Logs Displayed on the Console

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

Configuring the Rate Limit for Logging

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

Verification

Run the **show logging config** command to display the severity of logs displayed on the console.

Related Commands

Enabling Logging

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

Enabling Log Statistics Collection

Command	**logging count**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, log statistics collection is disabled. If log statistics collection 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 was generated.

Configuring the Severity of Logs Displayed on the Console

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

Configuring the Rate Limit for Logging

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 range is from 1 to 10,000. **all**: Indicates that the rate limit is applied to all logs ranging from severity 0 to severity 7. **console**: Indicates the number of logs displayed on the console per second. **except** *severity*: The rate limit is not applied to logs with a specified severity or lower. By default, the severity is error (severity 3), that is, rate limit is not applied to logs of severity 3 or lower.
Command Mode	Global configuration mode
Usage Guide	By default, no rate limit is configured.

Configuration Example

Sending Syslogs to the Console

Scenario	Syslogs need to be displayed on the console: 1. Enable log statistics collection. 2. Set the severity of logs that can be displayed on the console to informational (severity 6). 3. Set the 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 system performance.

Notes

- If 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 Step

↘ 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 each monitor terminal connected to the device.

↘ Configuring the Severity of Logs Displayed on the Monitor Terminal

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

Verification

Run the **show logging config** command to display the severity 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
Usage Guide	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 Severity of Logs Displayed on the Monitor Terminal

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

Configuration Example

Sending Syslogs to the Monitor Terminal

Scenario	Syslogs need to be displayed on the monitor terminal: 1. Display logs on the monitor terminal. 2. Set the severity of logs that can be displayed on the monitor terminal to informational (severity 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 but not 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 Step

↘ Writing Logs into the Memory Buffer

- Optional.
- By default, the system writes logs into the memory buffer, and the default severity of logs is debugging (severity 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 severity of logs written into the memory buffer.
- Run the **show logging** command to display the severity 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 severity of logs that can be written into the memory buffer.
Command Mode	Global configuration mode
Usage Guide	By default, the severity of logs written into the memory buffer is debugging (severity 7). Run the **show logging** command in privileged EXEC mode to display the severity of logs written into the memory buffer and the buffer size.

Configuration Example

↘ Writing Syslogs into the Memory Buffer

Scenario	Syslogs need to be written into the memory buffer: 1. Set the log buffer size to 128 KB (131,072 bytes). 2. Set the information severity of logs that can be written into the memory buffer to informational (severity 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, logs are not sent to the log server.

Configuration Step

↘ 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 each device.

Configuring the Severity of Logs Sent to the Log Server

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

Configuring the Facility Value of Logs Sent to the Log Server

- Optional.
- If the RFC 5424 format is disabled, the facility value of logs sent to the log server is local7 (23) by default. If the RFC 5424 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 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 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 configuration related to the log server.

Related Commands

Sending Logs to a Specified Log Server

Command	**logging** { *ip-address* | **ipv6** *ipv6-address* } [**udp-port** *port*]
Parameter Description	*ip-address*: Specifies the IPv4 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
Usage Guide	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 to all these log servers simultaneously.

	Up to five log servers can be configured on the device. Whether this parameter is supported and the value range of this parameter depend on the actual product version.

Configuring TCP Connection and TLS Encryption for the Specified Port of the Log Server

Command	**logging** [**server**] { *ip-address* | **ipv6** *ipv6-address* } [**tcp-transport** [**tcp-port** *tcp_port*] [**tls**]]
Parameter Description	*ip-address*: Specifies the IP address of the server that receives logs. **ipv6** *ipv6-address*: Specifies the IPv6 address of the server that receives logs. **tcp-transport**: Indicates TCP flags. **tcp-port** *tcp_por*: Specifies the port number of the log server (the default TCP port number is 601). **tls**: Indicates whether TLS encryption is enabled.
Command Mode	Global configuration mode
Usage Guide	This command is used to specify the IP address of the server that receives logs based on TCP. You can specify multiple log servers. The logs will be sent to all configured log servers. The **tls** parameter can be configured only when the **tcp-transport** parameter is configured in this command. Up to five log servers are configured for a Ruijie product.

Configuring the Severity of Logs Sent to the Log Server

Command	**logging trap** [*level*]
Parameter Description	*level*: Indicates the log severity.
Command Mode	Global configuration mode
Usage Guide	By default, the severity of logs sent to the log server is informational (severity 6). You can run the **show logging config** command in privileged EXEC mode to display the severity 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
Usage Guide	If the RFC 5424 format is disabled, the facility value of logs sent to the server is local7 (23) by default. If the RFC 5424 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
Usage Guide	By default, the source interface of logs sent to the log server is the interface sending logs. To facilitate management, you can use this command to configure the source interface of all logs so that the administrator can identify the device that sends 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
Usage Guide	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 configure the source IP address of all logs so that the administrator can identify the device that sends logs based on the unique address..

Configuration Example

Sending Syslogs to the Log Server

Scenario	Syslogs need to be sent to the log server: 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 address assignment by DHCP to the log server. 4. Set the warning (severity 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`

Scenario	Syslogs need to be sent to the log server: 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 address assignment by DHCP to the log server. 4. Set the warning (severity 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.

	`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 historical 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 periodically (at the interval of one hour by default) or when the buffer is full.

Configuration Step

↘ Writing Logs into Log Files

- Mandatory.
- By default, syslogs are not written to any log file.
- Unless otherwise specified, perform this configuration on each 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 being configured.

Verification

Run the **show logging config** command to display the configuration 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*]
Parameter Description	**sata0**: Indicates that log files are stored on the hard disk drive. **flash**: Indicates that log files will be stored in the extended flash. **flash2**: Indicates that log files are stored in the extended FLASH2. **usb0**: Indicates that log files will be stored in USB 0. This parameter is available 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 in USB 1. This parameter is available 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 in the SD card. This parameter is available 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 range is from 128 KB to 6 MB. The default value is 128 KB. *level*: Indicates the severity of logs that can be written into a log file.
Command Mode	Global configuration mode
Usage Guide	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 the file size is 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 be 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 Number of Log Files

Command	**logging file numbers** *numbers*
Parameter Description	*numbers*: Indicates the number of log files. The value range is from 2 to 32.
Command Mode	Global configuration mode
Usage Guide	This command can be used to set the number of log files for writing log information. Modifying the number of log files will not delete the log files already generated. To save the extended flash space, you need to manually delete the log files already generated (you can transfer the log files to an external server through TFTP before deletion). For example, after the device is enabled to write logs, 16 log files will be written by default. Assuming that the device has already generated 16 log files, if you want to change the number of log files to 2, the newly generated log information will be continuously overwritten and rewritten in the log files with index values of 0 and 1. However, the log files with index values of 2 to 16 that have been previously generated will still be retained, and the system will not delete them. You can manually delete these log files as needed.

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 range is from 1s to 51840s.
Command Mode	Global configuration mode
Usage Guide	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 severity. *days*: Indicates the storage time of log files, in days. The storage time is not less than seven days.
Command Mode	Global configuration mode
Usage Guide	After the log storage time is configured, the system writes logs of the same severity 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 configured by the **logging file flash** command, and **level** is the log severity. After you specify the storage time for logs of a severity, the system deletes the logs after the storage time expires. The storage time ranges from 7 days 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
Usage Guide	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 being configured. That is, after this command is configured, logs in the buffer are immediately written into log files.

Configuration Example

Writing Syslogs into Log Files

Scenario	Syslogs need to be written into log files: 1. Set the log file name to syslog. 2. Set the severity of logs sent to the console to debugging (severity 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`
	`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`

Scenario	Syslogs need to be written into log files: 1. Set the log file name to syslog. 2. Set the severity of logs sent to the console to debugging (severity 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.

	`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 required 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, severity, or mnemonic is configured in both the single-match and exact-match rules, the single-match rule takes effect.

Configuration Step

↘ 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-config** 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, 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
Usage Guide	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
Usage Guide	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 severity. Logs of this severity will be filtered out.
Command Mode	Global configuration mode
Usage Guide	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	Syslog filtering function needs to be configured: 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 logging** command to display the configuration. ● Enter and exit the 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`
	`Hostname#configure`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#exit`
	`Hostname#`
	`Hostname#show running-config | include logging`
	`logging filter direction server`
	`logging filter direction terminal`
	`logging filter rule single-match module SYS`

1.4.8 Configuring Severity-based Logging

Configuration Effect

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

Notes

Severity-based logging takes effect only when the RFC 5424 format is enabled.

Configuration Step

Configuring Severity-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 the module and severity.

Verification

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

Related Commands

Configuring Severity-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 parameter is specified, logs of the specified severity or higher will be sent to the specified destination, and other logs will be filtered out. If this parameter is not specified, logs of the specified severity or lower will be sent to the specified destination, and other logs will be filtered out. *level*: Indicates the severity 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
Usage Guide	This command is used to configure logging polices to send syslogs to different destinations based on module and severity.

Configuration Example

Configuring Severity-based Logging

Scenario	Logging policies need to be configured: 1. Send logs of severity 5 or higher that are generated by the system to the console. 2. Send logs of severity 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 RFC 5424 format is enabled.
- You are advised 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 a large interval so that many logs can be sent to the remote server at a time.

Configuration Step

↘ Enabling Delayed Display of Logs on the 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 the Console and Remote Terminal

Command	**logging delay-send terminal**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	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
Usage Guide	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, in seconds.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the delayed logging interval. The value range is from 600 to 65535.

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 IPv4 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**: Indicates that the password is in cleartext, which is optional. **7**: Indicates that the following password is encrypted.
Command Mode	Global configuration mode
Usage Guide	This command is used to specify an FTP or a TFTP server for receiving 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	Delayed logging needs to be configured: 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. The 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 intervals of all statistic objects.

Notes

- Periodical logging takes effect only when the RFC 5424 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.
- You are advised 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.
- The timer will be restarted when you modify the periodical logging interval of a statistic object, so the server can collect all performance statistic logs at the same time point

Configuration Step

↘ **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 the 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-config** command to display the configuration.

Related Commands

Enabling Periodical Logging

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

Enabling Periodical Display of Logs on the Console and Remote Terminal

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

Configuring the Periodical Logging Interval

Command	**logging statistic mnemonic** *mnemonic* **interval** *minutes*
Parameter	*mnemonic*: Identifies a performance statistic object.

Description	*minutes*: Indicates the periodical logging interval, in minutes.
Command Mode	Global configuration mode
Usage Guide	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. The value 0 indicates that periodical logging is disabled.

Configuration Example

Configuring Periodical Logging

Scenario	Periodical logging needs to be configured: 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 or logout attempts. After logging of login or logout attempts is enabled, logs are displayed on the device when users access the device through Telnet or SSH. This helps the administrator to monitor device connections.
- Record modification of device configurations. After logging of operations is enabled, corresponding logs are displayed on the device when users modify device configurations. This helps the administrator to monitor changes in device configurations.

Notes

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

Configuration Step

Enabling Logging of Login or Logout Attempts

- Optional.
- By default, logging of login or logout attempts is disabled.
- Unless otherwise specified, perform this configuration on each line of the device to enable logging of login or logout attempts.

Enabling Logging of Operations

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

Verification

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

Related Commands

Enabling Logging of Login or Logout Attempts

Command	**logging userinfo**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, a device generates related logs when users log in to or out of the device.

Enabling Logging of Operations

Command	**logging userinfo command-log**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The system generates related logs when users run configuration commands. By default, a device does not generate logs when users modify device configurations.

Configuration Example

Configuring Syslog Monitoring

Scenario	Syslog monitoring needs to be configured: 1. Enable logging of login or logout attempts. 2. Enable logging of operations.
Configuration Steps	Configure the syslog monitoring function.

	Hostname# configure terminal Hostname(config)# logging userinfo Hostname(config)# logging userinfo command-log
Verification	● Run the **show running-config | include logging** command to display the configuration. ● Run a command in global configuration mode, and verify that the system generates a log.
	Hostname#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#interface gigabitEthernet 0/0 *Jun 16 15:03:43: %CLI-5-EXEC_CMD: Configured from console by admin command: interface GigabitEthernet 0/0 Hostname#show running-config | include logging logging userinfo command-log

1.4.12 Synchronizing User Input with Log Output

Configuration Effect

By default, user input is not synchronized with 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 each line as required.

Configuration Step

↘ Synchronizing User Input with Log Output

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

Verification

Run the **show running-config** 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
Usage Guide	This command is used to synchronize user input with log output to prevent user input from being interrupted.

Configuration Example

Synchronizing User Input with Log Output

Scenario	User input needs to be synchronized with log output: 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

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

Command	Description
clear logging	Clears logs in the memory buffer.

Displaying

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

1 Configuring Software Authorization Management

1.1 Overview

Software authorization is an intermediary process that enables users to access certain extended features on their devices. Users need to install the correct license file before utilizing the corresponding extended functionalities. The extension functions provided by Ruijie Operating System (RGOS) include the Virtual Switch Device (VSD), Transparent Interconnection of Lots of Links (TRILL), Fibre Channel over Ethernet (FCoE), number of users supported by an access point (AP), and number of concurrent users supported by Secure Shell (SSL) Virtual Private Network (VPN). A user can use basic functions and extended functions of the RGOS after being authorized.

- Typically, all features of the RGOS are installed for the device before device delivery. However, users cannot use some features of the RGOS before they obtain a corresponding license file.
- Whether a feature requires authorization and the authorization type are specified in the configuration guide of the feature. Unless otherwise specified, basic functions of the system can be used without authorization.

1.2 Applications

1.2.1 VSD

Scenario

VSD, a network system virtualization technology, is used to virtualize one physical device into multiple logical devices. In addition, VSD maximizes use of existing resources, reducing the network operation cost.

Before being authorized, a user can only use VSD0 (that is, common CLI). After being authorized, the user can create other VSDs.

Deployment

The authorization module only functions on VSD0. License files cannot be installed on other VSDs.

1.2.2 FCoE

Scenario

FCoE technology can map a fiber channel to the Ethernet and insert fiber channel information into Ethernet packets, so requests and data over a fiber channel between a server and the SAN device can be transmitted over the Ethernet. This eliminates the need of specified fiber channels.

Before the FCoE license file is installed on the device, FCoE is unavailable. After the FCoE license file is installed, users can use FCoE.

Deployment

N/A

1.3 Features

Basic Concepts

License File for a Feature

A license for a certain special feature obtained by means of license file, hardware entity, or legal contract. This license stipulates the maximum number of users allowed to use it, the maximum number of instances allowed to be used, and validity period.

Authorized Software

Software function that can be used after being authorized.

Host ID

Unique serial number for identifying each device.

⚠ In a VSU, a license can adopt the host ID of any chassis. When the chassis exits the VSU, the feature corresponding to the license becomes invalid.

Authorization by Product

One license file is applied to only one device, which matches the host number. License file migration is not supported.

Purchase Voucher

The purchase voucher contains the product activation key (PAK) and the website for downloading the license file.

Product Activation Key (PAK)

The legal owner of the purchase voucher logs in to the website (listed on the purchase voucher) for downloading the license file and uses the PAK for registration. Then a corresponding license file is provided on the webpage for downloading or directly sent to the registered mailbox.

License File

After a license file is installed on a device, users can use corresponding functions. Each license file contains a digital signature to avoid manipulation. A license file is used for authorization based on products.

License Stacking

Different license files can be used on one device. For example, if a device provides both FCoE and TRILL functions, users can purchase the license files of the two functions and use them on the same device.

Temporary License File

A temporary license file becomes invalid after a period of time.

Evaluation License File

The evaluation license file is temporary. Typically, an evaluation license file is installed on a device before delivery, and it is mainly used to provide users with the function of using a trial feature. This type of license file is independent of the host number.

Permanent License File

A permanent license file is permanently valid.

Single-instance License File

Only one license file can be installed for a feature at a time.

The license file for the feature such as the number of concurrent users supported by VSD, TRILL, FCoE, and SSL VPN is a single-instance license file.

Multi-instance License File

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

Only the license file for the number of users supported by an AP is a multi-instance license file.

Periodic Warning

A periodic warning is advertised through a log or trap message several days before the license file expires. It is set to prevent a license file with a validity period from stopping working suddenly when the validity period expires, ensuring network performance.

Functions and Features

Function and Feature	Description
Obtaining and Using a License File	Obtain and use a license file.
Backing Up, Updating, and Removing a License File	Back up, update, and remove a license file.

1.3.1 Obtaining and Using a License File

Using a License File

A license file must be purchased from the website or marketing channel of formal authorization. Authorization is based on each device. To obtain a license file, visit the website on the purchase voucher and provide the PAK and host ID. The license file can be directly downloaded by a user or sent to a user by email. After obtaining the license file, users need to install the license file. After installing the license file, users can use the features corresponding to the license file.

The license files of the RGOS include permanent and temporary license files (evaluation license file is a type of temporary license file). Once a user starts using a temporary license for a certain feature, timekeeping is started for this license file, and this feature is disabled after the validity period of the license file expires. To continue using this feature, the user can purchase another license file (permanent or temporary license file) from the website or marketing channel.

In a VSU, multiple devices form one virtual device. In this scenario, as long as one device obtains the license file for a certain feature, the VSU obtains the license file for this feature. However, when these devices are used separately again, authorization is still based on each device.

The VSD function provided by RGOS virtualized one RGOS device into multiple virtual devices. For users, each virtual device behaves as an independent device. License files are managed in global configuration mode. That is, when the license file for a certain feature is obtained, the license files for this feature in all VSD domains are obtained. In addition, license files are installed and managed in the default VSD exclusively.

Check of the License File

After a device starts to run, the license file for each authorized feature needs to be checked. If the corresponding license file is properly installed, this feature is ready. Otherwise, this feature becomes invalid and cannot be used.

Checking the license files for various features occurs at different time points. That is, the license files for some features are checked during startup, and the license files for some features are checked in real time.

Loss of the License File

License files are stored in the **data** directory of a device and will not be lost after software upgrade.

If the memory or file system is damaged with the license file backed up, you can install the backup license file again after system recovery. If the license file is not backed up, you can visit the authorization website and obtain the license file again. The process of regaining the license file is the same as the process of obtaining a new license file (you do not need to purchase the license file again).

Authorization is based on each device. After a license file is provided for a specified device, authorization through this license file can be conducted on this device exclusively. The host ID may change during device maintenance or replacement. In case of host ID change, the license file obtained before can no longer be identified. In this case, contact after-sales engineers.

1.3.2 Backing Up, Updating, and Removing a License File

Backing Up a License File

When a fault such as file system storage media damage occurs on a device, the license file on the device may be lost after you rectify this fault. Therefore, you need to back up the license file for reinstallation in case of a fault.

Updating a License File

If the existing license file in the system cannot meet users' requirements for a feature, users can visit the website to purchase a license file and then update the license file locally.

Removing a License File

If a feature is not required, the user can remove the license file for this feature to improve the utilization rate of various resources such as the memory. If the user want to use this feature again after removing its license file, reinstall the license file. It is recommended that license files be kept properly.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of Software Authorization	(Mandatory) It is used to install a license file.	
	show license hostid	Obtains the host ID of the device.
	license install	Installs a license file manually.
	license auto-install	Installs a license file by automatic matching.
	(Optional) It is used to back up a license file.	

Backing Up the License File	**license copy**	Backs up a license file.
Configuring the Periodic Warning	(Optional) It is used to set the time of issuing a warning before the validity period of a license file expires.	
	license grace-peroid	Sets a friendly period warning.
Updating the License File	(Optional) It is used to update an existing license file on the device.	
	license update	Updates a license file.
Removing the License File	(Optional) It is used to remove an existing license file on the device.	
	license uninstall	Removes a license file manually.
	license auto-uninstall	Removes a license file by auto-match.
Unbinding a **License**	(Optional) It is used to unbind the license on the device.	
	license unbind	Unbinds the license.

1.4.1 Configuring Basic Functions of Software Authorization

Configuration Effect

Install a license file to enable the corresponding function.

Notes

- After downloading a license file from a specified website, upload this license file to the device (or store it in a USB flash drive) for installation. You do not need to connect the device to the Internet during installation.
- Different devices cannot share the same license file.
- After a license file is installed on a device, this license file is automatically backed up in the **data** directory of the system (the name of a license file ends with **.lic**). When you remove a license file, the backup file of this license file is also removed.

Configuration Step

↘ Obtaining the Host ID of the Device

- Mandatory.
- **hostid** indicates the host ID.
- If you want to apply a feature requiring authorization without installing the license file, the CLI displays a prompt indicating that the unauthorized feature is unavailable and provides the website for downloading the license file.

Command	**show license hostid**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	The name of a license file cannot be modified.

	This command does not require license.

Obtaining the PAK

- Mandatory.
- A PAK is provided in a paper purchase voucher by a vendor after a user purchases a license file.

Obtaining the License File of the Product from a Website

- Mandatory.
- After logging in to the authorization website, you can obtain the license file as prompted.

Copying the License File to the File System of the Device

- Mandatory.
- Use conventional file system operation commands to perform this operation. For example, download the license file through the TFTP protocol or copy the license file to a USB flash drive.

Installing the License File

- Optional.
- You can use the **license-install** or **license auto-install** command to install a license file. If you use the **license install** command in a VSU, only the device configured with the command is installed with the license file.
- If you use the **license auto-install** command in a VSU, all devices are installed with the license file through automatic matching. The two commands have the same effect in the non-VSU environment.

If you use the **license install** command in a VSU, the VSU is configured with the feature corresponding to the license file as long as one device obtains that feature. Once the devices are separated, the license takes effect on only the device configured with the command.

In a VSU, if the license install command is executed, licenses can only be installed locally. If the license auto-install command is run, licenses can be automatically matched and installed on all devices in the VSU.

The **license auto-install** command enables the automatic matching function only in the VSU. In the non-VSU environment, it has the same effect as the **license install** command.

In the VSD, license files are managed in global configuration mode. That is, when the license file for a certain feature is obtained, the license files for this feature in all VSD domains are obtained. In addition, license files are installed and managed in the default VSD exclusively.

Command	**license install** { **flash: | usb0:** } *filename*
Parameter Description	**flash**: Indicates that the license file is installed in the internal flash file system. **usb0**: Indicates that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	**license auto-install** { **flash:	usb0:** } *filename*
Parameter Description	**flash**: Indicates that the license file is installed in the internal flash file system. **usb0**: Indicates that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- You can run the **show license all_license** command to check the license name in a non-VSU. If the license name is displayed, the corresponding license file is installed.
- You can run the **show license dev_license** command to check the license name in a VSU. If the license name is displayed, the corresponding license file is installed.

Command	**show license** { **all_license	file** [*license*] }
Parameter Description	**all_license**: Displays all license files installed on the device. *license*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	You can check whether a license file is installed by checking the feature name.

Verification	`Hostname#show license all-license`
	`Searching license in the system...`
	`1. Service name: LIC-FCoE`
	`Attribute: Permanent, Single_instance, Releasable`
	`Licensed serial number: LIC-FCOE00000012268889`
	`2. Service name: LIC-VSD`
	`Attribute: Temporary, Single_instance, Releasable`
	`Left days: 362`
	`Licensed serial number: LIC-VSD00000012268888`

Command	**show license dev-license**
Parameter Description	**dev-license**: Displays all license files in all environments.
Command Mode	Privileged EXEC mode
Usage Guide	You can check whether a license file is installed by checking the feature name.

Verification	`Hostname#show license dev-license`
	`Searching license in the system...`
	`Dev 1`
	`1. Service name: LIC-FCoE`
	`Attribute: Permanent, Single_instance, Releasable`

	Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 Dev 2 1. Service name: LIC-AP-64 Attribute: Multiple_instance, Releasable [Permanent licenses] [Licensed serial number] 19880966.lic LIC-AP-6400000012264966 19880988.lic LIC-AP-6400000012264988 [Temporary license] [Licensed serial number] 19880900.lic LIC-AP-6400000012264900 (63 days left)

Configuration Examples

Installing a VSD License File in Non-VSU Environment

Network Environment	The VSD function needs to be enabled.
Configuration Steps	● Run the **show license hostid** command to obtain the host ID of the device. ● Register at the authorization website, and perform operation as prompted to obtain the license file **vsd.lic** for the VSD feature (the host ID of the device and PAK are required). The detailed operation is omitted in this example. ● Store the **vsd.lic** file in a USB flash drive, and connect the USB flash drive to the device. ● Install the **vsd.lic** file.
	Hostname#show license hostid 8708EH5F00042 Hostname#license install usb0:vsd.lic License file install success, service name: LIC-VSD.
Verification	Run the **show license all_license** command to check the license name. If the license name is displayed, the corresponding license file is installed.
	Hostname(config)#show license all-license Searching license in the system... 1.Service name: LIC-VSD Attribute: Temporary, Single instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888

Installing an FC License File in the VSU Environment

Network Environment	The FC function needs to be enabled.

Configuration Steps	● Run the **show license** *dev-hostid* command to obtain the host ID of device 2. ● Register at the authorization website, and perform operation as prompted to obtain the license file **fc.lic** for the FC feature (the host ID of the device and PAK are required). ● Store the **fc.lic** file in a USB flash drive, and connect the USB flash drive to the device. ● Install the **fc.lic** file.

	`Hostname#show license dev-hostid`
	`Dev 1: 8708EH5F00042`
	`Dev 2: GH3002893D300`
	`Hostname#license auto-install usb0:fc.lic`
	`License file install success, dev 2 installed it, service name: LIC-FC-BLADE-S.`

Verification	Run the **show license dev-license** command to check the license name. If the license name is displayed, the corresponding license file is installed.

	`Hostname#show license dev-license`
	`Searching license in the system...`
	`Dev 1`
	`1.Service name: LIC-VSD`
	`Attribute: Temporary, Single_instance, Releasable`
	`Left days: 362`
	`Licensed serial number: LIC-VSD00000012268888`
	`Dev 2`
	`1. Service name: LIC-FC-BLADE-S`
	`Attribute: Permanent, Single_instance, Releasable`
	`Licensed serial number: LIC-FC-BLADE-S00000012265522`

Common Errors

- A license file that does not belong to the device is installed.
- No matching device is available.
- A license file has been installed.
- A license file with its later version has been installed in the system.

1.4.2 Backing Up the License File

Configuration Effect

The license files of one or all features in the system are backed up.

Notes

- The license file of the evaluation version cannot be backed up.
- License files can be backed up only when the device has sufficient storage space.

One license file occupies a space of 4 KB to 10 KB.

Configuration Step

Backing Up a License File of the System

- The backup license file is a regular file.
- When you back up all license files in the system, a tar file is generated.

Command	**license** { **copy-all** | **copy-file** *filename* } { **flash: | usb0:** } [*target-filename*]
Parameter Description	**copy-all**: Copies all permanent license files in the system. **copy-file** *filename*: Copies the *filename* license file in the system. ***filename*** can be the name of a license file installed in the system or the name of a feature. When ***filename*** is a feature name, all license files installed for this feature are backed up. **flash**: Indicates that the license file is installed in the internal flash file system. **usb0**: Indicates that the license file is installed in the USB file system. *target-filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Uploading a License File to Another System for Storage

You can use a file system management command to further save a license file to other storage devices, such as a USB flash drive.

Verification

You can run the **dir** command to check whether the license file backup is generated. In addition, you can check whether the backup is correct by comparing the output of the **dir** command with the license file name in the **installed license** field of the feature with permanent authorization displayed by running the **show license all-license** command.

Command	**dir** [*filesystem*:] [*file-url*]
Parameter Description	*filesystem*: Indicates the URL of the file system, which is followed by a colon. The file systems include **flash:**, **sata:**, **usb:**, **sd:**, and **tmp:**. *file-url*: Indicates the path name. The path starting with the slash (/) indicates an absolute path. Otherwise, it is a relative path.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require a license.

Verification	`Hostname#dir usb0:rg-license-lics`
	`Directory of usb0:/rg-license-lics`
	`1 drwx 4096 Fri Jun 20 12:29:32 2014 .`
	`2 drwx 4096 Fri Jun 20 12:28:37 2014 ..`
	`3 -rwx 8704 Fri Jun 20 12:29:12 2014 lics.tar`
	`1 file, 2 directories`
	`536870912 bytes total (740,687,872 bytes free)`

Command	**show license** { **all-license | file** [*license*] }

Parameter Description	**all-license**: Displays all license files installed on the device. *license*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	You can check whether a license file is installed by checking the feature name. ⚠ Only a multi-instance license file has the **installed license** field. The multi-instance license file backup is named the ID of the multi-instance license file. At most one single-instance license file exists in the system at a time; therefore, the single-instance license file backup is named the feature.

Verification	`Hostname#show license all-license`
	`Searching license in the system...`
	`1. Service name: LIC-FCoE`
	`Attribute: Permanent, Single_instance, Releasable`
	`Licensed serial number: LIC-FCOE00000012268889`
	`2. Service name: LIC-VSD`
	`Attribute: Temporary, Single_instance, Releasable`
	`Left days: 362`
	`Licensed serial number: LIC-VSD00000012268888`
	`3. Service name: LIC-AP-64`
	`Attribute: Permanent, Multiple_instance, Releasable`
	`[Installed licenses] [Licensed serial number]`
	`19881021.lic LIC-AP-6400000012264966`
	`19881023.lic LIC-AP-6400000012264988`

Configuration Examples

↘ Backing Up All License Files of the System

Network Environment	Back up all license files in the system and name the backup **lics.tar**.
Configuration Steps	● Connect a USB flash drive to the device. ● Back up all permanent license files in the USB flash drive and name the backup lics.tar.
	`Hostname#lic copy-all usb0:rg-license-lics/lics.tar` `Success to copy all permanent license.`
Verification	You can run the **dir** command to check whether the license file package is generated. After decompressing the package, you can check whether the backup is correct by comparing the files in the package with the license file name displayed in the **installed license** field of the feature with permanent authorization displayed by running the **show license all-license** command. ⚠ Only a multi-instance license file has the **installed license** field. The multi-instance license file backup is named the ID of the multi-instance license file. At most one single-instance license file exists in the system at a time; therefore, the internal single-instance license file backup is named the feature.

	⚠ In this example, the IDs **19881021.lic** and **19881023.lic** are embedded in the license file. License files are stored in different folders based on the features during the packing; therefore, you can still identify the mapping between license files and features.
	Hostname#dir usb0:rg-license-lics Directory of usb0:/rg-license-lics 1 drwx 4096 Fri Jun 20 12:29:32 2014 . 2 drwx 4096 Fri Jun 20 12:28:37 2014 .. 3 -rwx 8704 Fri Jun 20 12:29:12 2014 lics.tar 1 file, 2 directories 536870912 bytes total (740,687,872 bytes free) Hostname#show license all-license Searching license in the system... 1. 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 3. Service name: LIC-AP-64 Attribute: Permanent, Multiple_instance, Releasable [Installed licenses] [Licensed serial number] 19881021.lic LIC-AP-6400000012264966 19881023.lic LIC-AP-6400000012264988

Common Errors

- A license file or a file does not exist in the system.
- A temporary license file is used for backup (a temporary license file cannot be backed up).

1.4.3 Configuring the Periodic Warning

Configuration Effect

Before the validity period of an evaluation license file expires, a warning is issued in a log, notifying an administrator of taking measures immediately.

Notes

- Each authorized feature should be set separately.
- This setting may be affected by time adjustment on the device.
- A permanent license file does not need to be configured with the periodic warning.

Configuration Step

↘ **Configuring a Periodic Warning for an Authorized Feature**

Command	**license grace-peroid** *filename days*
Parameter Description	*filename*: Indiates the name of the license file for a feature. *days*: Indiates the period from the expiry time to the warning time.
Defaults	The default value is the smaller one between 120 and half of the evaluation license file's validity period.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

- Method 1: Set the expiry time of a license file to be earlier than the warning time and check whether the warning is displayed at intervals.
- Method 2: Run the **show license** command to check whether the time of the **Alarm starting point** filed is consistent with the setting.

Command	**show license** { **all-license | file** [*license*] }
Parameter Description	**all-license**: Displays all license files installed on the device. *license*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require a license.

Verification	`Hostname#show license file LIC-VSD`
	`Service name: LIC-VSD`
	`Attribute: Temporary, Single instance, Releasable`
	`Left days: 362`
	`Licensed serial number: LIC-VSD00000012268888`

Configuration Examples

Changing the Periodic Warning Time

Network Environment	The temporary license file has already been installed on the device, and the periodic warning time is set to 100 days.
Configuration Steps	Set the periodic warning time to 100 days.
	`Hostname#lic grace-period LIC-VSD 100` `RG_LICENSE: success to set alarm starting point of license LIC-VSD.`
Verification	When the validity period of the license file is shorter than 100 days, the periodic warning is displayed at intervals.
	`Hostname#*Jun 18 10:06:36: %RG_LICENSE-4-LICENSE_DEADLINE_INFO: Service LIC-VSD will be disabled 80 days behind. In order to avoid the inconvenience to you, please log on website http://192.168.5.227:8080/login.jsf to get a new license.`

Common Errors

- The periodic warning is configured for a permanent license file.
- No license file is installed in the preset feature system.

1.4.4 Updating the License File

Configuration Effect

- The license file for a feature of the system is updated. This configuration is performed to update an evaluation license file into a temporary license file.

Notes

- A formal permanent license file does not need to be updated.
- A license file cannot be updated to the earlier version.

A license file has a time filed. The value of this field is subject to the time when the license file is generated from the website. The later the time, the later the version.

Configuration Step

Updating a License File

- You can run the **license update** command to update the license file for a feature.
- Update the license file without connecting the device to the Internet.

Command	**license update** { **flash: | usb0:** } *filename*
Parameter Description	**flash**: Indicates that the license file is installed in the internal flash file system. **usb0**: Indicates that the license file is installed in the USB file system. *filename*: Specifies the name of the license file.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Verification

You can run the **show license** command and check the **Attribute** field. If the field is displayed as **Permanent**, the corresponding attribute is updated.

Command	**show license** { **all-license | file** [*license*] }
Parameter Description	**all-license**: Displays all license files installed on the device. *license*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require a license.

Verification	`Hostname#show  license all-license`
	`Searching license in the system...`
	`  1. Service name: LIC-FCoE`
	`    Attribute: Permanent, Single_instance, Releasable`

	Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888

Configuration Examples

Updating the VSD License File

Network Environment	Update the temporary license file for the VSD in the system to a permanent license file.
Configuration Steps	● Purchase the permanent license file **vsd_perm.lic** for the VSD, store the **vsd_perm.lic** file in a USB flash drive, and connect the USB flash drive to the device. ● Update the license file for the VSD.
	Hostname#license update usb0:vsd_perm.lic License file update success, temporary license LIC-VSD changes into permanent.
Verification	You can run the **show license** command and check the **Attribute** field. If the field is displayed as **Permanent**, the corresponding attribute is updated.
	Hostname(config)#show license all-license Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-VSD00000012266666

Common Errors

- A license file that does not belong to the device is installed.
- The license file of the new version is replaced with that of the old version.
- A license file is re-installed.
- The permanent license file is replaced with the temporary license file.
- The corresponding feature is not installed for the system before the update.

1.4.5 Removing the License File

Configuration Effect

- Remove the license files for one or all features in the system.

If a feature is not required, you can remove the license file for this feature to improve the utilization rate of various resources such as the memory. After being removed, this feature becomes unavailable.

Notes

- If you remove the license file in use, the removal operation takes effect next time when the feature is enabled or restarted.
- To reinstall a license file after removing it, you need to obtain the license file. It is recommended that you back up the license file before removing it.

Configuration Step

Removing a License File from the System

- Run the **license uninstall** command to remove a license file from the system.

Command	**license uninstall** *license* [*filename*]
Parameter Description	*license*: Indicates the name of the license file to be removed. *filename*: Indicates the name of the file to be removed.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After you remove the license file for a feature that is running, the license file cannot be removed. A license file that is removed cannot be restored. It is recommended that you back up the license file before removing it. This command does not require a license.

Verification

You can run the **show license all-license** command to display the **Service name** filed. If the name of a feature corresponding to a license file removed is not displayed, the license file is removed successfully.

Command	**show license** { **all-license | file** [*license*] }
Parameter Description	**all-license**: Displays all license files installed on the device. *license*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require a license.

Verification	`Hostname#show license all-license`
	`Searching license in the system...`
	`1. Service name: LIC-FCoE`
	`Attribute: Permanent, Single_instance, Releasable`
	`Licensed serial number: LIC-FCOE00000012268889`

Removing a License File in the VSU Environment

- Run the **license auto-uninstall** command to remove a license file in the VSU environment.

Command	**license auto-uninstall** *devid license* [*filename*]
Parameter Description	*devid*: Indicates the ID of the device where the file is stored. *license*: Indicates the name of the license to be removed. *filename*: Indicates the name of the file to be removed..

Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	After you remove the license file for a feature that is running, the license file cannot be removed. A license file that is removed cannot be restored. It is recommended that you back up the license file before removing it. This command does not require a license.

Verification

Run the **show license dev-license** command to display the **Service name** field. If the name of a feature corresponding to a license file removed is not displayed, the license file is removed successfully.

Command	**show license dev-license**
Parameter Description	**dev-license:** Displays all license files in all environments.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require a license.

Verification	`Hostname#show  license dev-license`
	`Searching license in the system...`
	`Dev 1`
	`1. Service name: LIC-FCoE`
	`Attribute: Permanent, Single_instance, Releasable`
	`Licensed serial number: LIC-FCOE00000012268889`
	`2. Service name: LIC-VSD`
	`Attribute: Temporary, Single_instance, Releasable`
	`Left days: 362`
	`Licensed serial number: LIC-VSD00000012268888`
	`Dev 2`
	`There’s no license installed in this device.`

Configuration Examples

↘ Removing the VSD License File

Network Environment	Remove the license file for the VSD in the system.
Configuration Steps	Remove the license file for the VSD.
	`Hostname(config)#license uninstall LIC-VSD` `License file uninstall LIC-VSD success.`
Verification	● Run the **show license all-license** command to view the **Service name** filed. If the name of a feature corresponding to a license file already removed is not displayed, the license file is removed successfully.
	`Hostname(config)#show  license all-license`

	Searching license in the system... 1. Service name: LIC-FCoE Attribute: Permanent, Single instance, Releasable Licensed serial number: LIC-FCOE00000012268889
Configuration Steps	Remove the license file for the FC on device 2.
	Hostname#license auto-uninstall 2 LIC-FC-BLADE-S License file uninstall LIC-FC-BLADE-S of device 2 success.
Verification	Run the **show license dev-license** command to display the **Service name** field. If the name of a feature corresponding to a license file already removed is not displayed, the license file is removed successfully.
	Hostname#show license dev-license Searching license in the system... Dev 1 1. Service name: LIC-FCoE Attribute: Permanent, Single_instance, Releasable Licensed serial number: LIC-FCOE00000012268889 2. Service name: LIC-VSD Attribute: Temporary, Single_instance, Releasable Left days: 362 Licensed serial number: LIC-VSD00000012268888 Dev 2 There'heresed serial number: LIC-VSD000000122

Common Errors

- The license file has not been installed on the device.
- A specified license file does not exist on the device.

1.4.6 Unbinding a License

Configuration Effect

Unbind and uninstall a license file.

If you want to unbind a license file from the device, you should unbind the license code from the device first.

Notes

- After the license file is unbound from the device, you will obtain a verification code, which will be used for the unbinding operation at the authorization website.
- After the license code is unbound, the corresponding license file cannot be installed again.

Configuration Step

Unbinding a License File

Run the **license unbind** command to unbind a license file.

Command	**license unbind** *pak*
Parameter Description	*pak*: Indicates the license code.
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run the **show license all-license** command to display the installed license code. This command does not require a license.

Verification

Run the **show license all-license** command to display the **licensed serial number** field. If the license code is not displayed, the license is unbound.

Command	**show license** { **all-license** | **file** [*license*] }
Parameter Description	**all-license**: Displays all license files installed on the device. *license*: Displays a specified license file.
Command Mode	Privileged EXEC mode
Usage Guide	This command does not require a license.

Configuration Example

↘ Unbinding License Code LIC-VSD00000012268888

Network Environment	The license corresponding to license code LIC-VSD00000012268888 is installed.
Configuration Steps	Unbind license code LIC-VSD00000012268888.

	`Hostname#license unbind LIC-VSD00000012268888`
	`Success to unbind license LIC-VSD00000012268888.`
	`The verification string is:`
	`775719468737BA269825589557F558657575B5D5D5D5D785782598859765A8355855`

Verification	Run the **show license all-license** command to display the **licensed serial number** field. If the license code is not displayed, the license is unbound.

	`Before Binding`
	`Hostname#show license all-license`
	`Searching license in the system...`
	`1. Service name: LIC-AP-64`
	`Attribute: Releasable`
	`[Permanent licenses] [Licensed serial number]`
	`19880966.lic LIC-AP-6400000012264966`
	`19880988.lic LIC-AP-6400000012264988`
	
	`[Temporary license] [Licensed serial number]`
	`19880900.lic LIC-AP-6400000012264900`

```
   (63 days left)

 2. Service name: LIC-VSD
   Attribute: Permanent, Releasable
   Licensed serial number: LIC-VSD00000012268888

After Binding
Hostname#show  license all-license
Searching license in the system...
 1. Service name: LIC-AP-64
   Attribute: Releasable
   [Permanent licenses]    [Licensed serial number]
   19880966.lic           LIC-AP-6400000012264966
   19880988.lic           LIC-AP-6400000012264988

   [Temporary license]     [Licensed serial number]
   19880900.lic           LIC-AP-6400000012264900
   (63 days left)
```

Common Errors

No matching license code exists in the system.

1.5 Monitoring

Displaying

Command	Function
show license { **all_license | file** [*license*] }	Displays license configuration.
show license dev-license	Displays the license configuration of all devices.
show license usage	Displays the license in use.
show license hostid	Displays the serial number of the device where the license is installed.
show license dev-hostid	Displays the host ID for the license (all devices).
show license unbind-code	Displays the unbound license code on the current device.
show license dev-unbind-code	Displays the unbound license code on all devices in the system.

1 Configuring USB

1.1 Overview

The universal serial bus (USB) is an external bus standard. In this document, USB refers to a USB-compliant peripheral device, for example, a USB flash drive.

The USB is a hot swappable device. You can use it to copy files (such as configuration and log files) from a communication device, or copy external data (such as system upgrade files) to the flash of the communication device.

For more information about application scenarios of the USB, see configuration guides of related functions. This document describes only how to identify, use, and remove the USB, and view information about the USB.

The device does not support USB viewing, using, or uninstallation.

1.2 Applications

Application	Description
Using a USB Flash Drive to Upgrade a Device	Upgrade files are stored in a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version.

1.2.1 Using a USB Flash Drive to Upgrade a Device

Scenario

Upgrade files are stored in a USB flash drive. After a device is powered on, the device detects the USB flash drive and runs the upgrade command to load the upgrade files. After loading is completed, the device is reset and runs the upgraded version. An example of the upgrade command is as follows:

upgrade usb0:/s12k-ppc_11.0(1B2)_20131025_main_install.bin

If the file is valid and execution of this command succeeds, the device will be automatically reset and run the upgraded version.

Deployment

- Use the prefix "usb0:/" to access USB 0. Run the **show usb** command to display information about the USB with the ID of 0.
- Run the **upgrade** command to perform upgrade.

1.3 Features

Using the USB

Insert a USB into the USB slot. The system automatically searches for the USB. After the USB is located, the driver module automatically initializes the USB. After initialization, the system automatically loads the file system in the USB. Then the system can read or write the USB.

- If the system finds a USB and successfully loads the USB, the following information will be displayed:

```
*Jan  1 00:09:42: %USB-5-USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted to USB port 0!
*Jan  1 00:09:42: %USB-5-USB_DISK_PARTITION_MOUNT: Mount usb0(type:FAT32),size : 1050673152B(1002MB)
```

Mass Storage indicates the name of the searched device, and **usb0:** indicates the first USB. **Size** indicates the size of the partition. For example, according to the preceding information displayed, the USB flash drive has a space of 1002 MB.

Removing the USB

Use a command line interface (CLI) command to remove the USB first; otherwise, an error may occur if the system is currently using the USB.

- If the USB is successfully removed, the following information will be displayed:

```
OK, now you can pull out the device 0.
```

You can remove the USB only after the preceding information is displayed.

1.4 Configuration

Configuration	Description and Command	
Using a USB	Mandatory.	
	N/A	
Removing a USB	(Mandatory) It is used to remove a USB.	
	usb remove	Removes a USB.

1.4.1 Using a USB

Configuration Effect

After a USB is loaded, you can run the file system commands (such as **dir**, **copy**, and **del**) to perform operations on the USB.

Notes

- The Ruijie General Operating System (RGOS) is applicable only to devices (generally common USB flash drives) that support standard Small Computer System Interface (SCSI) commands. Other devices, such as the USB flash drive embedded in the USB network interface card (NIC) and USB flash drive with the virtual CD-ROM drive, cannot be used in the RGOS. Some devices are configured with the function of converting a USB port to the serial port.

- The USB supports only the FAT file system. Other file systems in the USB must be formatted to the FAT file system on a PC before the USB can be used on a device.
- The RGOS supports the hub. When a USB flash drive is inserted to a port on a hub, the access path becomes different. If the USB flash drive is inserted to a USB port on a device, the access path is **usbX:/**, where **X** indicates the device ID. You can run the **show usb** command to display this path. If the USB flash drive is inserted to a USB port through a hub, the access path is **usbX-Y:/**, where **X** indicates the device ID, and **Y** indicates the hub port ID. For example, **usb0-3:/** indicates port 3 on the hub that is connected to USB port 0 on the device.

Configuration Step

Identifying a USB

A USB can be directly inserted to the USB slot without a CLI operation.

Using a USB

Perform the following operations to copy files from a USB to the flash memory:

- Run the **cd** command to enter the partition of the USB.
- Run the **copy** command to copy files in the USB to the flash memory on the device.
- Run the **dir** command to check whether the files are copied to the device.

If the USB has multiple partitions, you can access only the first FAT partition on the device.

The path of the USB does not contain any upper-level directory. After running the **cd usbX:** command to access a USB, you can run the **cd flash:** command to return to the flash file system.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Configuration Example

Using a USB Flash Drive

Scenario	Standalone environment
Configuration Steps	● Insert the USB flash drive into the USB slot of the device. ● Run the **show usb** command on the device console. ● Copy the **config.txt** file from the USB flash drive to the flash memory on the device.
	Hostname#show usb Device: Mass Storage ID: 0 URL prefix: usb0 Disk Partitions: usb0(type:vfat) Size:15789711360B(15789.7MB) Available size:15789686784B(15789.6MB) Hostname# Hostname#

```
Hostname#dir usb0:/
Directory of usb0:/
  1 -rwx           4  Tue Jan  1 00:00:00 1980  fac_test
  2 -rwx           1  Mon Sep 30 13:15:48 2013  config.txt
2 files, 0 directories
15,789,711,360 bytes total (15,789,686,784 bytes free)
Hostname#
Hostname#
Hostname#copy usb0:/config.txt flash:/
Copying: !
Accessing usb0:/config.txt finished, 1 bytes prepared
Flushing data to flash:/config.txt...
Flush data done
Hostname#
Hostname#
```

Verification

- Check whether the **config.txt** file exists in the flash memory.

```
Hostname#
Hostname#dir flash:/
Directory of flash:/
  1 drw-         160  Wed Mar 31 08:40:01 2010  at
  2 drwx         160  Thu Jan  1 00:00:11 1970  dm
  3 drwx         160  Thu Jan  1 00:00:05 1970  rep
  4 drwx         160  Mon Apr 26 03:42:00 2010  scc
  5 drwx         160  Wed Mar 31 08:39:52 2010  ssh
  6 drwx         224  Thu Jan  1 00:00:06 1970  var
  7 d---         288  Sat May 29 06:07:45 2010  web
  8 drwx         160  Thu Jan  1 00:00:11 1970  addr
  9 drwx         160  Sat May 29 06:07:44 2010  cwmp
 10 drwx         784  Sat May 29 06:07:47 2010  sync
 11 --w-          92  Tue Feb  2 01:06:55 2010  config_vsu.dat
 12 -rw-         244  Sat Apr  3 04:56:52 2010  config.text
 13 -rwx           1  Thu Jan  1 00:00:30 1970  .issu_state
 14 -rw-           0  Tue Feb  2 01:07:03 2010  ss_ds_debug.txt
 15 -rw-        8448  Thu Jan  1 00:01:41 1970  .shadow
 16 -rwx         268  Thu Jan  1 00:01:41 1970  .pswdinfo
 17 -rw-           4  Tue May 25 09:12:01 2010  reload
 18 drwx         232  Wed Mar 31 08:40:00 2010  snpv4
 19 drwx        6104  Sat May 29 06:10:45 2010  .config
 20 ----           1  Thu Jan  1 00:04:51 1970  config.txt
 21 d---         160  Thu Jan  1 00:00:12 1970  syslog
 22 drwx         160  Tue May 25 03:05:01 2010  upgrade_ram
 23 drwx         160  Tue Feb  2 01:06:54 2010  dm_vdu
 24 -rwx          16  Thu Jan  1 00:01:41 1970  .username.data
```

	9 files, 15 directories 5,095,424 bytes total (4,960,256 bytes free) Hostname#

Common Errors

- Insert a USB flash drive that supports non-SCSI commands to the device.
- The USB does not use the FAT file system, and cannot be identified by the system.

1.4.2 Removing a USB

Configuration Effect

Remove the USB and ensure that the USB and the device are intact.

Notes

- Run the **usb remove** command before removing the USB; otherwise, a system error occurs.

Configuration Steps

Running the Remove Command

- Mandatory.
- Run the **usb remove** command before removing the USB.

Removing the USB

After the **remove** command is executed, remove the USB.

Verification

Run the **show usb** command to display information about the USB inserted to the device.

Related Commands

Removing a USB

Command	**usb remove** *device-id*
Parameter Description	*device-id*: Indicates the ID of the USB port on the device. You can run the **show usb** command to display this ID.
Command Mode	Privileged EXEC mode
Usage Guide	Before removing a USB, run the **usb remove** command; otherwise, an error occurs if the USB is in use. If the command is executed, related information will be displayed, and you can remove the USB. If the command execution fails, the USB is in use. In this case, do not remove the USB until it is not in use.

Configuration Example

Removing a USB

Scenario	Standalone environment
Configuration Steps	● Run the **show usb** command to display the ID of the USB. ● Run the **usb remove** command to remove the USB.
	Hostname#show usb Device: Mass Storage ID: 0 URL prefix: usb0 Disk Partitions: usb0(type:vfat) Size:15789711360B(15789.7MB) Available size:15789686784B(15789.6MB) Hostname# Hostname# Hostname#usb remove 0 OK, now you can pull out the device 0.
Verification	● Run the **show usb** command again to check whether the USB is removed. If the device with ID 0 is not displayed in output of the **show usb** command, the USB is removed.
	Hostname#show usb Hostname#

1.5 Monitoring

Displaying

Command	Description
show usb	Displays information about the inserted USB.

1 Configuring Package Management

1.1 Overview

Package management refers to the package management and upgrade module. This module is responsible for installing, upgrading/degrading, querying, and maintaining components of the device, among which upgrade is the main function. Through upgrade, you can install new version of software that is more stable or powerful. Adopting the modular architecture, the system supports overall upgrade and subsystem upgrade, and supports separate upgrade of a feature package. In addition, the system supports upgrade through hot patches.

Component upgrade described in this document applies to both the fixed device and rack-type device. In addition, this document is for only version 11.0 and later.

Protocols and Standards

N/A

1.2 Applications

Application	Scenario
Upgrading or Degrading the Subsystem	Upgrade subsystem firmware such as boot, kernel, and rootfs on the box-type device.
Upgrading or Degrading a Single Feature Package	Upgrade a single feature package on the fixed device.
Installing a Hot Patch Package	Install a hot patch, and repair a part of the feature component.

1.2.1 Upgrading or Degrading the 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. Typically, the subsystem firmware of the fixed device is called main package.

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

Deployment

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

1.2.2 Upgrading Subsystem Components with One Click

Scenario

It is typically used in VSU dual-device systems, and is also used for upgrading and degrading subsystem components. In privileged EXEC mode, run the **upgrade auto** command to perform automatic upgrade. This upgrade process requires no user intervention and does not interrupt services. For a single device in VSU or standalone mode, executing the **upgrade auto** command is equivalent to executing the **upgrade** command followed by an automatic restart of the entire system, but this upgrade process interrupts services.

Deployment

Upgrade or degrade subsystem components.

1.2.3 Upgrading or 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, while the other features remain unchanged.

Typically, a feature package is small in size and the upgrade speed is high. After the upgrade is completed, only the corresponding functional module is improved, and other functional modules remain unchanged.

Deployment

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

1.2.4 Installing a Hot Patch Package

Scenario

To fix software bugs without restarting the device, you can install hot patch packages. Hot patch packages are only applicable to fixing a specific software version. In most situations, hot patch packages are released to fix the software of a certain version only when the device cannot be started.

The most significant feature of hot patch upgrade is that all bugs can be fixed without device restart after the upgrade is completed.

Deployment

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

- 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: The kernel is the OS core of the system. The 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

The main package is often used to upgrade or degrade a subsystem of the fixed 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 or degrade.

Rack Package

The rack package is used for upgrading the subsystem component of the rack-type device, which includes the main installation package of the supervisor module and all line cards. This package can upgrade all cards on the rack-type device at one time.

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 hot patches of several features. You can upgrade a hot patch package to install patches for various features. New features are provided immediately without device restart after the upgrade.

⚠ The firmware in this document refers to an installation file that contains a subsystem or feature module.

Overview

Feature	Description
Upgrading or Degrading and Managing Subsystem Components	Upgrades or degrades a subsystem and checks available subsystem components.
Upgrading or Degrading and Managing Functional Components	Upgrades or degrades a functional component, checks available subsystem components, and activates the specified subsystem component.
Upgrading or Degrading and Managing Hot Patch Packages	Installs a hot patch package.

1.3.1 Upgrading or Degrading and Managing Subsystem Components

Subsystem upgrade or degrade aims to upgrade the software by replacing subsystem components of the device with 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 or degrade in most cases. Instead, subsystems are added to the device and then activated during upgrade or degrade.

Working Principle

Upgrade or Degrade

Various subsystems exist in the device in different forms. Therefore, upgrade or degrade varies with different subsystems.

- boot: Typically, this subsystem exists on the norflash device in the form of images. Therefore, upgrading or 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 or degrading this subsystem is to write the file.
- rootfs: In most cases, this subsystem exists on the nandflash device in the form of images. Therefore, upgrading or 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 uses the redundancy design. During the upgrade or degrade:

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

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 or degrade module always records the subsystem component in use, 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 or Degrading and Managing Functional Components

Working Principle

Upgrading a feature is replacing feature files on the device with feature files in the package.

Managing feature components and hot patches is aimed at recording information about feature components and hot patches by using a database. Installing components, displaying component information, and uninstalling components are results of database addition, querying, and deletion.

Relevant Configuration

Upgrade

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

1.3.3 Upgrading or Degrading and Managing Hot Patch Packages

Working Principle

Upgrading a feature component is replacing feature files on the device with feature files in the package.

Upgrading hot patch packages is similar to upgrading features. The difference is that only files to be revised are replaced during hot patch package upgrade. In addition, after the files are replaced, the new files take effect automatically.

After package upgrade, component upgrade cannot be performed.

Management

Similar to feature component management, hot patch management also includes query, installation, and uninstallation operations, which are results of adding, querying and deleting data.

Hot patches and feature components are managed based on the same technology. The difference is that the hot patches involve three different states, that is, non-installed, installed, and activated.

The hot patch in installed state only indicates that this hot patch exists on the device, but does not take effect.

Only the hot patch in activated state is valid.

Relevant Configuration

Upgrade

- Store the upgrade file in the local file system, and then run the **upgrade** command for upgrade.
- Run the **upgrade autoload** command to install and activate hot patches with one click. The patches that have been installed with the **autoload** command do not need to be repeatedly activated with the **patch active** and **patch running** commands.

Activating a Hot Patch

- You can run the **patch active** command to activate a patch temporarily. The patch becomes invalid after device restart. To use this patch after device restart, you need to activate it again.
- You can also run the **patch running** command to activate a patch permanently. The patch is still valid after device restart.
- The patch that is not activated will never become valid.

Deactivating a Hot Patch

To deactivate an activated patch, run the **patch deactive** command.

Uninstalling a Hot Patch

You can run the **patch delete** command to uninstall a hot patch.

1.4 Configuration

Configuration	Description and Command
Upgrading or Degrading a Firmware	(Mandatory) It is used to install and upgrade or degrade a subsystem firmware, feature package, and hot patch package. This command is valid on both the fixed device and rack-type device.

	upgrade [**peer** *ip-address*] **flash:/***/path* [**force**]	Upgrades the firmware stored on the device. *path* is a local path where the firmware is stored.
	upgrade [**peer** *ip-address*] **download tftp:/***/path* [**force | vrf**]	Downloads a firmware from the server and upgrade the package automatically. *path* is the path of the firmware on the server.
	patch active	Temporarily activates installed patches.
	patch running	Permanently activates installed patches.
Deactivating and Uninstalling a Hot Patch	⚠ (Optional) It is used to invalidate activated hot patches or uninstalls hot patches.	
	patch deactive	Invalidates the activated patches.
	patch delete	Uninstalls hot patches.

1.4.1 Upgrading or Degrading a Firmware

Configuration Effect

Available installation 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.

✅ The main package is typically released to upgrade a fixed device.

Notes

N/A

Configuration Step

↘ Upgrading the Main Package for the Device

- Optional.
- Perform the configuration when all system software on the device needs to be upgraded.
- Download the firmware to the local device and run the **upgrade** or **upgrade patch** command.

✅ The main package is typically released to upgrade a fixed device.

↘ Upgrading Each Feature Package

- Optional.
- Perform the configuration 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.

↘ Upgrading a Hot Patch Package

- Optional.
- Perform the configuration to fix software bugs without restarting the device.

- Download the firmware to the local device and run the **upgrade** command.
- After the upgrade, to use the hot patch, first activate it. The configuration in this step is mandatory. You can run the **patch active** command to activate a patch temporarily, or run the **patch running** command to activate a patch permanently.

⚠ The **patch running** command must be used to activate a patch permanently in user scenarios. The **patch active** command can be used to activate a patch only when a user intends to verify the patch.

Upgrading the Server

- Optional. This function is enabled by default. You can perform 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 installed. 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, run the **show upgrade history** command to check whether the upgrade is successful.
- After upgrading a feature component, run the **show component** command to check whether the upgrade is successful.
- After upgrading a hot patch package, run the **show patch** command to check whether the upgrade is successful.

Commands

Upgrade

Command	**upgrade** [**peer** *ip-address*] **flash://***path* [**force**]
Parameter Description	**peer**: Indicates the peer device. *ip-address*: Specifies the IP address of a device. *path*: Indicates the local path where an installation package is stored. **force**: Indicates forcible device upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Command	**upgrade** [**peer** *ip-address*] **download tftp://***path* [**force** | **vrf**]
Parameter Description	**peer**: Indicates the peer device. **all**: Indicates all devices. *ip-address*: Specifies the IP address of a device. *path*: Indicates the path of the upgrade package on the TFTP server. The command enables the device to automatically download the upgrade package from the TFTP server and perform upgrade. **force**: Indicates forcible upgrade. **vrf**: VRF name for upgrade.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Firmware Stored on the Device

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

Display the Upgrade Status of Each Card on the Rack-type Device

Command	**show upgrade status**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Upgrade History

Command	**show upgrade history**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Installed Feature Components

Command	**show component** [*component _name*]
Parameter Description	*component _name*: Indicates the component name. When this parameter value is empty, the command is used to display all components installed on the device and basic information about these components. When this parameter value is not empty, the command is used to display detailed information about the corresponding component, check whether the component is intact, and check whether this component works properly. All parameters apply to rack-type devices only.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying the Upgrade Status

Command	**show upgrade peer** { **all** | *ip-address* } **status**
Parameter Description	**peer**: Indicates the peer device. **all**: Indicates all devices. *ip-address*: Specifies the IP address of a device.

Command Mode	Privileged EXEC mode
Usage Guide	All parameters apply to graded devices only.

Displaying Installed Patch Packages

Command	**show patch**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	All parameters apply to rack-type devices only.

Activating Patches Temporarily

Command	**patch active**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This operation can be performed only on the device that has a patch installed. This command can be used to activate a patch temporarily, and the activated patch becomes invalid after device restart. All parameters apply to rack-type devices only.

Activating the Patches Permanently

Command	**patch running**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This operation can be performed only on the device that has a patch installed. This command can be used to activate a patch permanently. All parameters apply to rack-type devices only.

Configuration Example

Upgrading a Subsystem Firmware on the Fixed 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 such as **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 or SD card 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 device. If version information changes, the upgrade is successful.
	Hostname#show version detail upgrade history 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

Upgrading a Feature Package on the Fixed 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 such as **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 or SD card.
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 component`
	`Package :sysmonit`
	`  Version:1.0.1.23cd34aa  Build time: Wed Dec 7 00:58:56 2011`
	`  Size:12877 Install time :Wed Mar 5 14:23:12 2012`
	`  Description:this is a system monit package`
	`  Required packages: None`
	`----------`
	`package:bridge`
	`  Version: 2.3.1.1252ea  Build time: Wed Dec 7 00:54:56 2011`
	`  Size:26945 Install time : Wed Mar 19:23:15 2012`
	`  Description:this is a bridge package`
	`  Required packages: None`

Verification	● View version information about the device. If version information changes, the upgrade is successful.

	`Hostname-VSU#show version detail`
	`System description  : Hostname Full 10G Routing Switch(S6220-48XS4QXS-II) By Hostname 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

Installing a Patch Package on the Fixed 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 such as **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 or SD card.
Configuration Steps	● Run the **upgrade** command. ● Activate the hot patch.
	Hostname#upgrade download tftp://192.168.201.98/RGOS11.0(1C2)_20131008_patch.bin Accessing tftp://192.168.201.98/RGOS11.0(1C2)_20131008_patch.bin... !!! !!! !!!!!!!!!!!!!!!! Transmission finished, file length 9868 bytes. Upgrade processing is 10% Upgrade processing is 60% Upgrade info [OK] patch_bridge version[1.0.0.1952] Upgrade processing is 90% Upgrade info [OK] patch_install version[1.0.0.192e35a] Hostname#patch running The patch on the system now is in running status
Verification	● Check the hot patches installed on the device.
	:patch package patch_install installed in the system, version:pa1 Package : patch_bridge Status: running

	Version: pa1 Build time: Mon May 13 09:03:07 2013 Size: 277 Install time: Tue May 21 03:07:17 2013 Description: a patch for bridge Required packages: None

Common Errors

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

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

Common error messages are as follows:

- Invalid firmware: The cause is that the firmware may be damaged or incorrect. You are advised to obtain the firmware again and perform the upgrade.
- Firmware not supported by the device: You may incorrectly use the firmware of other devices. You are advised to obtain the firmware again, verify the package, and perform the upgrade.
- Insufficient device space: Typically, this error occurs on a rack-type device. You are advised to check whether the device is equipped with a USB flash drive or SD card. The device often has a USB flash drive.

1.4.2 Deactivating and Uninstalling a Hot Patch

Configuration Effect

An activated hot patch is deactivated or uninstalled.

Notes

A hot patch that is not activated does not take effect; therefore, you cannot deactivate it.

Configuration Steps

↘ Deactivating an Activated Patch

- Optional.
- To deactivate an activated patch, run the **patch deactive** command.

↘ Uninstalling a Hot Patch

- Optional.
- To uninstall a hot patch that is installed, run the **patch delete** command.

Verification

You can run the **show patch** command to check whether a patch is activated or uninstalled.

Commands

↘ Deactivating an Activated Patch

Command	**patch deactive**

Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	You can perform this operation on only an activated patch. All parameters are applicable to only the rack-type device.

Deleting a Hot Patch

Command	**patch delete**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to remove the hot patch package from the device. All parameters are applicable to only the rack-type device.

Configuration Example

Deactivating and Uninstalling a Patch on the Fixed Device

Configuration Steps	● Run the **patch deactivate** command. ● Run the **patch delete** command.

	`Hostname#patch deactive`
	`Deactive the patch package success`
	`Hostname# patch delete`
	`Clear the patch patch_bridge success`
	`Clear the patch success`
	`You use reset patch command have risky, Are you sure? Continue [Y/n]y`
	`Patch operate finish!`

Verification	● Display the patch status.
	`Hostname#show patch` `No patch package installed in the system`

Invalidating and Uninstalling the Patch on the Rack-type Device

Configuration Steps	● Run the **patch deactive** command. ● Run the **patch delete** command.
	Hostname#patch deactive slot M1 [Slot M1]: Deactive the patch package success Hostname# patch delete slot M1 [Slot M1]: Clear the patch patch_bridge success Clear the patch success
Verification	Display the patch status.
	Hostname#show patch slot M1 [Slot M1]: No patch package installed in the system

Common Errors

Run the **patch deactive** command when the patch is not activated. You are advised to check the patch status. You can run the **patch deactive** command only when the patch is in **status:running** state.

1.5 Monitoring

Clearing

Command	Function
patch delete	Deletes a hot patch package that is installed.
clear storage [*url*]	Removes an installation package on the local device.

Displaying

Command	Function
show component [*component _name*]	Displays all components installed on the device and their information.
show patch [*patch _name*]	Displays information about hot patch packages installed on the device.
show upgrade status	Display the upgrade status of each card on the rack-type device.
show upgrade history	Displays the upgrade history.

1 Configuring Time Range

1.1 Overview

The 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.

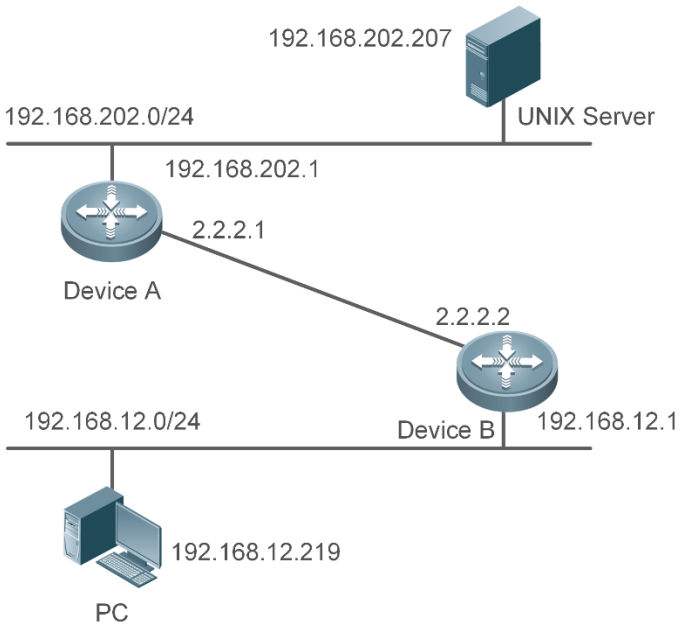
1.2 Applications

Typical Application	Scenario
Applying a 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 a Time Range to an ACL

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



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

Deployment

On Device B, apply an ACL to control Telnet service access of users on 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 Features

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 specified function takes effective within this time range.

Periodic Time

The 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 specified function takes effective periodically from every Monday to Friday.

Overview

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

1.3.1 Using the Absolute Time Range

Working Principle

When a function is enabled for a time-based application, the application determines whether the current time is within the absolute time range. If so, the function becomes effective or ineffective at the current time depending on specific configuration.

1.3.2 Using the Periodic Time

Working Principle

When a function is enabled for a time-based application, the application determines whether the current time is within the period time. If so, the function becomes effective or ineffective at the current time depending on specific configuration.

1.4 Configuration

Configuration	Description and Command
Configuring the Time	(Mandatory) It is used to configure the time range.

Range	**time-range** *time-range-name*	Configures a time range.
	(Optional) It is used to configure parameters of a time range.	
	absolute { [**start** *time date*] [**end** *time date*] }	Configures an absolute time range.
	periodic *day-of-the-week time* **to** [*day-of-the-week*] *time*	Configures the periodic time.

1.4.1 Configuring the Time Range

Configuration Effect

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

Configuration Step

Configuring a Time Range

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

Command Syntax	**time-range** *time-range-name*
Parameter Description	*time-range-name*: Indicates the name of the time range to be created.
Defaults	No time range is configured.
Command Mode	Global configuration mode
Usage Guide	Some applications (such as ACL) may run based on the time. For example, an ACL can be effective within certain time ranges of a week. You must configure a time range, and then you can configure time control in time range configuration mode.

Configuring the Absolute Time Range

Optional.

Command Syntax	**absolute** { [**start** *time date*] | [**end** *time date*] }
Parameter Description	**start** *time date*: Indicates the start time of the time range. **end** *time date*: Indicates the end time of the time range. The maximum time range is from 00:00 January 1, 0000 to 23:59 December 31, 9999.
Defaults	No absolute time range is configured. The maximum time range is used by default.
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 the Periodic Time

Optional.

Command Syntax	**periodic** *day-of-the-week time* **to** [*day-of-the-week*] *time*
Parameter Description	*day-of-the-week*: Indicates the week day when the periodic time starts or ends. *time*: Indicates the exact time when the periodic time starts or ends.
Defaults	No periodic time is configured.
Command Mode	Time range configuration mode
Usage Guide	Use the **periodic** command to configure a periodic time to allow a specified function to take effect within the periodic time. If no periodic time is configured, a certain function takes effect within the periodic time. Before changing the periodic time of a service, disassociate the time range from the service, and then re-associate the time range with the service after the change.

Verification

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

Command Syntax	**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

Displaying

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

Configuring Interface

1. Configuring Interfaces
2. Configuring Aggregate Interface

1 Configuring Interfaces

1.1 Overview

Interfaces are used for data exchange on network devices. Network devices support physical and logical interfaces. A physical interface is a hardware interface on a device, such as the 100M and 1000M Ethernet interfaces. A logical interface is not a hardware interface on the device. A logical interface, such as the loopback interface and tunnel interface, can be associated with a physical interface or independent of any physical interface. For network protocols, physical and logical interfaces serve the same function.

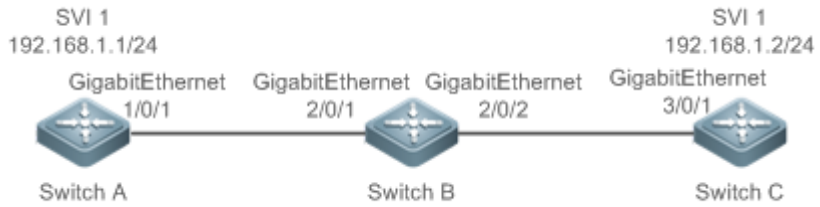
1.2 Applications

Application	Description
Layer 2 Data Switching Through a Physical Ethernet Interface	Implement Layer 2 data communication of network devices through the physical Layer 2 Ethernet interface.
Layer 3 Routing Through a Physical Ethernet Interface	Implement Layer 3 data communication of network devices through the physical Layer 3 Ethernet interface.

1.2.1 Layer 2 Data Switching Through a Physical Ethernet Interface

Scenario

Figure 1-1



As shown in Figure 1-1, Switch A, Switch B, and Switch C form a simple Layer 2 data switching network.

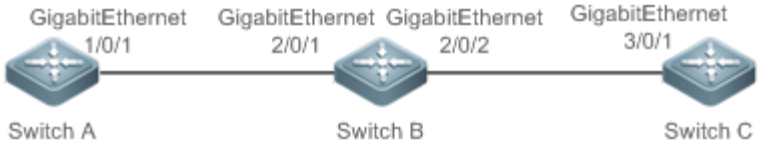
Deployment

- Connect Switch A to Switch B through GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through 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 trunk interfaces.
- Create a switch virtual interface (SVI), SVI 1, on Switch A and Switch C respectively, and configure IP addresses from the same network segment for the two SVIs. The IP address of SVI 1 on Switch A is 192.168.1.1/24, and the IP address of SVI 1 on Switch C is 192.168.1.2/24.
- Run the **ping 192.168.1.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement data switching through Switch B.

1.2.2 Layer 3 Routing Through a Physical Ethernet Interface

Scenario

Figure 1-2



As shown in Figure 1-2, Switch A, Switch B, and Switch C form a simple Layer 3 data communication network.

Deployment

- Connect Switch A to Switch B through GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1.
- Connect Switch B to Switch C through 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 interfaces.
- Configure IP addresses from the same network segment for GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1. The IP addresses of GigabitEthernet 1/0/1 and GigabitEthernet 2/0/1 are 192.168.1.1/24 and 192.168.1.2/24, respectively.
- Configure IP addresses from the same network segment for GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1. The IP addresses of GigabitEthernet 2/0/2 and GigabitEthernet 3/0/1 are 192.168.2.1/24 and 192.168.2.2/24, respectively.
- Configure a static route entry on Switch C so that Switch C can directly access the network segment 192.168.1.0/24.
- Run the **ping 192.168.2.2** command on Switch A and the **ping 192.168.1.1** command on Switch C to implement Layer 3 routing through Switch B.

1.3 Features

Basic Concepts

Interface Classification

Interfaces on devices fall into three categories:

- Layer 2 interface (supported by switches or network bridges)
- Layer 3 interface (supported by Layer 3 devices)

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

- Switch interface
- Layer 2 aggregate interface

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

- Routed interface
- Layer 3 aggregate interface
- SVI
- Loopback interface
- Tunnel interface

Switch Interface

A switch interface is an individual physical interface on the device, and implements only the Layer 2 switching function. The switch interface is used to manage physical interfaces and Layer 2 protocols related to physical interfaces.

Layer 2 Aggregate Interface

An aggregate interface is formed by aggregating multiple physical interfaces. Multiple physical links can be bound together to form a simple logical link. This logical link is called an aggregate interface.

For Layer 2 switching, an aggregate interface is equivalent to a switch interface that combines bandwidth values of multiple interfaces, increasing the link bandwidth. Frames sent over the Layer 2 aggregate interface are load balanced among the member interfaces. If one member link fails, the Layer 2 aggregate interface automatically transfers the traffic on the faulty link to other member links, improving reliability.

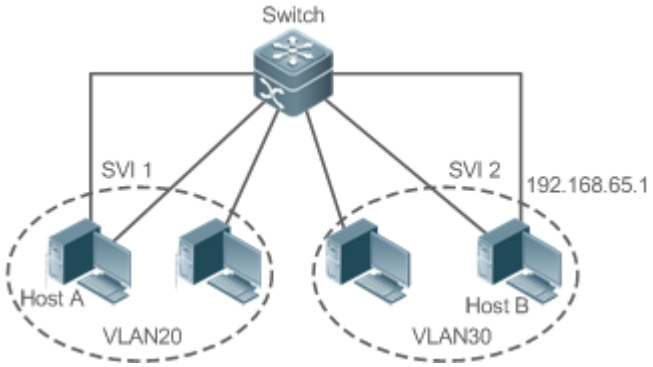
SVI

An SVI can be used as the management interface of the local device, through which an administrator can manage the device. You can also create an SVI as a gateway interface, which is mapped to the virtual interface of each VLAN to implement routing across VLANs among Layer 3 devices. You can run the

interface vlan command to create an SVI and assign an IP address to this interface to implement routing between VLANs.

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

Figure 1-3



Routed Interface

A physical interface on a Layer 3 device can be configured as a routed interface, which functions as the gateway interface for Layer 3 switching. A routed interface is irrelevant to a specific VLAN. Instead, it is just an access interface. The routed interface cannot be used for Layer 2 switching. You can run the **no switchport** command to change a switch interface to a routed interface and assign an IP address to this interface for routing. Running the **no switchport** command will delete all Layer 2 features of the interface.

If an interface is a member interface of the Layer 2 aggregate interface or an interface where 802.1X authentication fails, you cannot run the **switchport** or **no switchport** command to switch the interface.

Layer 3 Aggregate Interface

Similar to a Layer 2 aggregate interface, a Layer 3 aggregate interface is a logical interface that aggregates multiple physical member interfaces. The member interfaces must be the Layer 3 interfaces of the same type. The aggregate interface functions as a gateway interface for Layer 3 switching. Multiple physical links are combined into one logical link, increasing link bandwidth. Frames sent over the Layer 3 aggregate interface are load balanced among member interfaces. If one member link fails, the Layer 3 aggregate interface automatically transfers the traffic on the faulty link to other member links, improving reliability.

A Layer 3 aggregate interface cannot be used for Layer 2 switching. You can run the **no switchport** command to change a Layer 2 aggregate interface that does not contain any member interface into a Layer 3 aggregate interface, add multiple routed interfaces to the Layer 3 aggregate interface, and then assign an IP address to this Layer 3 aggregate interface for routing.

Loopback Interface

A loopback interface is a local Layer 3 logical interface simulated by the software that 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) or for Telnet access. The procedure for configuring a loopback interface is similar to that for configuring an Ethernet interface (the loopback interface can be considered as a virtual Ethernet interface).

Tunnel Interface

A tunnel interface implements tunneling. Transmission protocols such as IP can be used to transmit packets of any protocol over a tunnel interface. Like other logical interfaces, the tunnel interface is also a virtual interface of the system. The tunnel interface provides a standard point-to-point (P2P) transmission mode, without specifying any transmission protocol or load protocol. Therefore, a tunnel interface must be configured for each individual link.

Overview

Feature	Description

Feature	Description
Interface Configuration Commands	Configures interface attributes in interface configuration mode. If you enter the interface configuration mode of a nonexistent logical interface, the interface will be created.
Interface Description and Administrative Status	Configures the description for an interface, which helps you identify the interface and remember functions of the interface. You can also configure the administrative status of the interface.
MTU	Configures the maximum transmission unit (MTU) of an interface to limit the length of a frame that can be received or sent over this interface.
Bandwidth	Configures the bandwidth of an interface.
Load Interval	Specifies the interval for load calculation of an interface.
Carrier Delay	Configures the carrier delay of an interface to adjust the delay after which the status of an interface changes from Down to Up or from Up to Down.
Link Trap Policy	Enables or disables the link trap function on an interface.
Interface Index Persistence	Enables the interface index persistence function so that the interface index remains unchanged after the device is restarted.
Routed	You can configure a physical interface on a Layer 3 device as a routed interface, which functions as the gateway interface for Layer 3 switching.
Layer 3	You can configure an aggregate interface on a Layer 3 device as a Layer 3 aggregate interface, which functions as the gateway interface for Layer 3 switching.
Interface Speed, Duplex Mode, Flow Control Mode, and Auto-negotiation Factor	You can configure the speed, duplex mode, flow control mode, and auto negotiation of an interface.
Interface Errdisable Recovery	After an interface is shut down due to a violation, you can run the **errdisable recovery** command in global configuration mode to recover all the interfaces in errdisable state and enable these interfaces.
Interface Flapping Protection	You can configure the interface flapping protection function. The system can automatically shut down the interface when flapping occurs on the interface.

1.3.1 Interface Configuration Commands

Run the **interface** command in global configuration mode to enter the interface configuration mode. You can configure interface attributes in interface configuration mode.

Working Principle

Run the **interface** command in global configuration mode to enter the interface configuration mode. If you enter the interface configuration mode of a nonexistent logical interface, the interface will be created. You can also run the **interface range** or **interface range macro** command in global configuration mode to configure the range (IDs) of interfaces. Interfaces defined in the same range must be of the same type and have the same attributes.

You can run the **no interface** command in global configuration mode to delete a specified logical interface.

↘ Interface Numbering Rules

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

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

The slot number rules are as follows: The static slot ID is 0, whereas the ID of a dynamic slot (pluggable module or line card) ranges from 1 to the number of slots. Facing the device panel, dynamic slot are numbered from 1 sequentially from front to rear, from left to right, and from top to bottom.

The ID of an interface on the slot ranges from 1 to the number of interfaces on the slot, and is numbered sequentially from left to right.

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

The ID of an aggregate interface ranges from 1 to the number of aggregate interfaces supported by the device.

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

Configuring Interfaces Within a Range

You can run the **interface range** command in global configuration mode to configure multiple interfaces at a time. Attributes configured in interface configuration mode apply to all the interfaces.

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

The **macro** parameter is used to configure the macro corresponding to a range. For details, see *Configuring Macros of Interface Ranges*.

Ranges can be separated by commas (,).

Types of interfaces within all ranges specified in a command must be the same.

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

The following interface range formats are valid:

- **FastEthernet** device/slot/{first interface} - {last interface}
- **GigabitEthernet** device/slot/{first interface} - {last interface}
- **TenGigabitEthernet** device/slot/{first interface} - {last interface}
- **FortyGigabitEthernet** device/slot/{first interface} - {last interface}
- **AggregatePort** *Aggregate-port ID* (The aggregate interface 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 4094.)
- **Loopback** loopback-ID (The loopback interface ID ranges from 1 to 2147483647.)
- **Tunnel** tunnel-ID (The tunnel interface ID ranges from 0 to the maximum number of tunnel interfaces supported by the device minus 1.)

Interfaces in an interface range must be of the same type, namely, FastEthernet or GigabitEthernet.

Configuring Macros of Interface Ranges

You can define macros to replace the interface ranges. Before using the **macro** parameter in the **interface range** command, first run the **define interface-range** command in global configuration mode to define these macros.

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

1.3.2 Interface Description and Administrative Status

You can configure the description for an interface to identify the interface, which helps you remember functions of the interface.

You can enter interface configuration mode to enable or disable an interface.

Working Principle

Interface Description

You can configure the description of an interface based on the purpose of the interface. For example, if you want to assign GigabitEthernet 0/1 for user A exclusively, you can configure the description of the interface as "Port for User A."

Interface Administrative Status

You can configure the administrative status of an interface to disable the interface as required. If the interface is disabled, no frame will be received or sent on this interface. You can enable a disabled interface by configuring the administrative status of the interface. Two types of interface administrative status are defined: Up and Down. The administrative status of an interface is Down when the interface is disabled, and Up when the interface is enabled.

1.3.3 MTU

You can configure the MTU of an interface to limit the length of a frame that can be received or sent over this interface.

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

Working Principle

When a large amount of data is exchanged over a interface, frames whose length is greater than that of standard Ethernet frames may exist. This type of frame is called jumbo frame. The MTU is the length of a valid data segment in a frame. It does not include the Ethernet encapsulation overhead.

If an interface receives or sends a frame with a length greater than its MTU, the frame will be discarded.

1.3.4 Bandwidth

Working Principle

The **bandwidth** command is mainly used by a routing protocol (for example, OSPF) to calculate the route metric and the Resource Reservation Protocol (RSVP) to calculate the reserved bandwidth. Changing the interface bandwidth will not affect the data transmission rate of the physical interface.

1.3.5 Load Interval

Working Principle

You can run the **load-interval** command to specify the interval for load calculation of an interface. Typically, the interval is 10s.

1.3.6 Carrier Delay

Working Principle

The carrier delay refers to the delay after which the data carrier detect (DCD) signal changes from Down to Up or from Up to Down. If the DCD status changes during the delay, the system will ignore this change to avoid negotiation at the upper data link layer. If a large carrier delay is used, nearly every DCD change is not detected. On the contrary, if the carrier delay is set to 0, every DCD signal change will be detected, resulting in poor stability.

If the DCD carrier is interrupted for a long time, a small carrier delay should be used to accelerate convergence of the topology or route. On the contrary, if the DCD carrier interruption time is shorter than the topology or route convergence time, a large carrier delay should be used to avoid topology or route flapping.

1.3.7 Link Trap Policy

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

Working Principle

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

1.3.8 Interface Index Persistence

Similar to an interface description, the interface index also identifies an interface. When an interface is created, the system automatically assigns a unique index to the interface. The index of an interface may change after the device is restarted. You can enable the interface index persistence function so that the interface index remains unchanged after the device is restarted.

Working Principle

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

1.3.9 Routed Interface

Working Principle

A physical interface on a Layer 3 device can be configured as a routed interface, which functions as the gateway interface for Layer 3 switching. The routed interface cannot be used for Layer 2 switching. You can run the **no switchport** command to change a switch interface to a routed interface and assign an IP address to this interface for routing. Running the **no switchport** command will delete all Layer 2 features of the interface.

1.3.10 Layer 3 Aggregate Interface

Working Principle

Similar to a Layer 3 routed interface, you can run the **no switchport** command to change a Layer 2 aggregate interface into a Layer 3 aggregate interface on a Layer 3 device, and then assign an IP address to this aggregate interface for routing. Running the **no switchport** command will delete all Layer 2 features of the aggregate interface.

A Layer 2 aggregate interface with one or more member interfaces cannot be configured as a Layer 3 aggregate interface. Similarly, a Layer 3 aggregate interface with one or more member interfaces cannot be changed to a Layer 2 aggregate interface.

1.3.11 Interface Speed, Duplex Mode, Flow Control Mode, and Auto-negotiation Factor

You can configure the interface speed, duplex mode, flow control mode, and auto-negotiation factor of an Ethernet physical interface or aggregate interface**.**

Working Principle

Speed

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

When you configure the speed 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.)

Flow Control

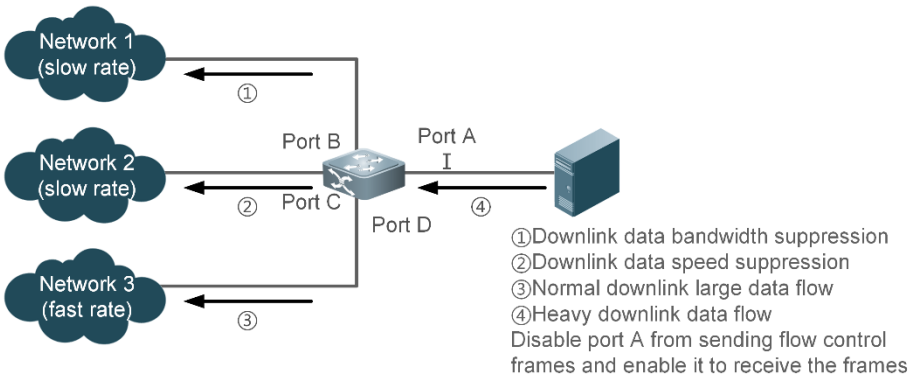
Flow control on an interface is performed in asymmetric or symmetrical mode:

- Symmetric mode: After flow control is enabled on an interface, the interface processes the received flow control frames, and sends flow control frames when the interface is congested. The incoming and outgoing flow control frames are processed in the same way.
- Asymmetric mode: In some cases, an interface on a device is expected to process the received flow control frames without packet loss due to congestion, and expected not to send flow control frames to avoid network speed decrease. In this case, you need to configure the asymmetric mode in which incoming and outgoing flow control frames are processed separately.

When you configure the flow control mode of an aggregate interface, the configuration takes effect on all of its member interfaces. (All these member interfaces are Ethernet physical interfaces.)

As shown in Figure 1-4, port A of the device is an uplink interface, ports B, C, and D are downlink interfaces, and port B and port C are connected to different networks. Assume that port A is enabled to send and receive flow control frames. If heavy data flow is sent on port B and port C, port B and port C will be congested, and consequently congestion occurs in the inbound direction of port A. Therefore, port A sends flow control frames. When the uplink device responds to the flow control frames, it reduces the data flow sent to port A, which causes the network speed to decrease on port D. In this case, you can disable the port A from sending flow control frames to ensure the bandwidth utilization of the entire network.

Figure 1-4



Auto-negotiation Mode

The auto-negotiation mode of an interface can be **on** or **off**. The auto-negotiation status of the interface is different from the auto-negotiation mode. The auto-negotiation status of the interface depends on the interface rate, duplex mode, flow control mode, and auto-negotiation mode.

Typically, if one of the interface rate, duplex mode, and flow control mode is set to **auto**, or the auto-negotiation mode of the interface is **on**, the auto-negotiation status of the interface is **on**, that is, the auto-negotiation function of the interface is enabled. If none of the interface rate, duplex mode, and flow control mode is set to **auto**, and the auto-negotiation mode of the interface is **off**, the auto-negotiation function of the interface is disabled.

1.3.12 Interface Errdisable Recovery

Some protocols support the interface errdisable recovery function to ensure security and stability of the network. For example, when you enable port security and configure the maximum number of security addresses on the interface, an interface violation event is generated if the number of addresses learned on this interface exceeds the maximum number of security addresses. For other protocols, such as the Spanning Tree Protocol (STP), 802.1X, Rapid Ethernet Uplink Protection Protocol (REUP), and frequent interface flapping, and an interface where a violation event occurs will be automatically shut down to ensure security.

Working Principle

When a interface is disabled due to setting violation of the REUP link state tracking group, the interface can be recovered by setting scheduled REUP recovery or by running the REUP errdisable recovery command in global configuration mode. In other cases, you can run the **errdisable recovery** command in global configuration mode to recovery all the interfaces in errdisable state and enable these interfaces. You can manually recover a interface, or automatically recover a interface at a scheduled time. For some products, you can run the **shutdown** and **no shutdown** commands in interface configuration mode to recover all the interfaces in errdisable state and enable the interfaces.

1.3.13 Interface Flapping Protection

An interface flapping causes a lot of hardware interruptions, consuming many CPU resources. Moreover, frequent interface flapping damages the interface. You can configure the interface flapping protection function to protect interfaces.

Principles

By default, the interface flapping protection function is enabled. You can disable this function as required. When an interface flapping occurs, the interface detects flapping every 2s or 10s. If the interface detect

six flappings in 2s, the device displays a prompt. If the device display 10 prompts continuously, that is, the interface detects flapping continuously within 20s, the interface is shut down (the violation cause is displayed as **Link Dither**). If the interface detects 10 flaps within 10s on an interface, the device displays a prompt without shutting down the interface.

1.3.14 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.

1.4 Configuration

Configuration	Description and Command	
Performing Basic Configurations	(Optional) It is used to manage interface configurations, for example, creating or deleting an interface, or configuring the interface description.	
	interface	Creates an interface and enters the configuration mode of the created interface or a specified interface.
	interface range	Enters an interface range, creates these interfaces (if not created), and enters the interface configuration mode.
	define interface-range	Creates a macro to specify an interface range.
	snmp-server if-index persist	Enables the interface index persistence function so that the interface index remains unchanged after the device is restarted.
	description	Configures the interface description of up to 80 characters in interface configuration mode.
	snmp trap link-status	Configures whether to send link traps of the interface.
	shutdown	Shuts down an interface in interface configuration mode.
	physical-port dither protect	Configures the interface flapping protection function in global configuration mode.
	logging [**link-updown** | **error-frame** | **link-dither**]	Configures the syslog function on an interface in global configuration mode.
Configuring Interface Attributes	(Optional) It is used to configure interface attributes.	
	bandwidth	Configures the bandwidth of an interface in interface configuration mode.
	carrier-delay	Configures the carrier delay of an interface in interface configuration mode.
	load-interval	Configures the interval for load calculation of an interface.
	duplex	Configures the duplex mode of an interface.
	flowcontrol	Enables or disables flow control on an interface.
	mtu	Configures the MTU of an interface.
	speed	Configures the speed of an interface.
	switchport	Configures an interface as a Layer 2 interface in interface configuration mode. (Run the **no switchport** command to configure an interface as a Layer 3 interface.)
	errdisable recovery	Recovers an interface in errdisable state in global configuration mode or privileged EXEC mode (errdisable recovery).

1.4.1 Performing Basic Configurations

Configuration Effect

- Create a specified logical interface and enter the configuration mode of this interface, or enter the configuration mode of an existing physical or logical interface.
- Create multiple specified logical interfaces and enter the interface configuration mode, or enter the configuration mode of multiple existing physical or logical interfaces.
- The interface indexes remain unchanged after the device is restarted.
- Configure the interface description, which helps to learn information about the interface.
- Enable or disable the link trap function of an interface.
- Enable or disable an interface.

Notes

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

Configuration Step

↘ Configuring a Specified Interface

- Optional.
- Run this command to create a logical interface or enter the configuration mode of a physical interface or an existing logical interface.

Command	**interface** *interface-type interface-number*
Parameter Description	*interface-type interface-number*: Indicates the type and number of the interface. The interface can be an Ethernet physical 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 this interface and enter the configuration mode of this interface. ● For a physical interface or an existing logical interface, run this command to enter the configuration mode of this interface. ● Use the **no** form of the command to delete a specified logical interface. ● Use the **default** form of the command to restore default settings of the interface in interface configuration mode.

↘ Configuring Interfaces Within a Range

- Optional.
- Run this command to create multiple logical interfaces or enter the configuration mode of multiple physical interface or existing logical interfaces.

Command	**interface range** { *port-range* | **macro** *macro_name* }
Parameter Description	*port-range*: Indicates the type and ID range of interfaces. These interfaces can be Ethernet physical interfaces, aggregate interfaces, SVIs, or loopback interfaces. *macro_name*: Indicates the name of the interface range macro.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	● If logical interfaces are not created yet, run this command to create these interfaces and enter the interface configuration mode. ● For multiple physical interfaces or existing logical interfaces, run this command to enter the interface configuration mode. ● Use the **default** form of the command to restore default settings of these

	interfaces in interface configuration mode. ● Before using a macro, run the **define interface-range** command to define the interface range as a macro name in global configuration mode, and then run the **interface range macro** *macro_name* command to apply the macro.

Configuring Interface Index Persistence

- Optional.
- Run this command when the interface indexes must remain unchanged after the device is restarted.

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

Configuring the Description of an Interface

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

Command	**description** *string*
Parameter Description	*string:* Indicates a string of up to 80 characters.
Defaults	By default, no description is configured.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the description of an interface. You can use the **no** or **default** form of the command to delete the description of an interface.

Configuring the Link Trap Function of an Interface

- Optional.
- Run this command to obtain link traps through SNMP.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, the link trap function is enabled.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the link trap function on an interface. When this function is enabled, the SNMP-enabled device sends link traps when the link status changes on the interface. You can use the **no** or **default** form of the command to disable the link trap function.

Configuring the Administrative Status of an Interface

- Optional.
- Run this command to enable or disable an interface.
- An interface that is disabled cannot send or receive packets.

Command	**Shutdown**
Parameter Description	N/A
Defaults	By default, the administrative status of an interface is Up.
Command Mode	Interface configuration mode
Usage Guide	You can run the **shutdown** command to disable an interface, or the **no shutdown** command to enable an interface. You can use the **no** or **default** form of the command to enable the interface. The following cases may occur for different devices: ● You cannot run the **no shutdown** command on the interface in errdisable state. ● You can run the **shutdown** and **no shutdown** commands to recover the interfaces in errdisable state.

Configuring Interface Flapping Protection

- Optional.
- Run this command to protect the interface where flapping occurs.

Command	physical-port dither protect
Parameter Description	N/A
Defaults	By default, interface 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 interface flapping information.
Defaults	By default, the syslog function is enabled on an interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Configuring a Specified Interface

- Run the **interface** command. If you can enter the interface configuration mode, the configuration is successful.
- For a logical interface, after the **no interface** command is executed, run the **show running** or **show interfaces** command to check whether the logical interface exists. If not, the logical interface is deleted.
- After the **default interface** command is executed, run the **show running** command to check whether the default settings of the corresponding interface are restored. If so, the operation is successful.

Configuring Interfaces Within a Range

- Run the **interface range** command. If you can enter the interface configuration mode, the configuration is successful.
- After the **default interface range** command is executed, run the **show running** command to check whether the default settings of the corresponding interfaces are restored. If so, the operation is successful.

Configuring Interface Index Persistence

- After the **snmp-server if-index persist** command is executed, run the **write** command to save the configuration, restart the device, and run the **show interface** command to check the interface index. If the index of an interface remains the same after the restart, interface index persistence is enabled.

Configuring the Link Trap Function of an Interface

- Remove and then install the network cable on a physical interface, and enable the SNMP server. If the SNMP server receives link traps, the link trap function is enabled.
- Run the **no** form of the **snmp trap link-status** command. Remove and then install the network cable on a physical interface. If the SNMP server does not receive link traps, the link trap function is disabled.

Configuring the Administrative Status of an Interface

- Insert the network cable on a physical interface, enable the interface, and run the **shutdown** command on this interface. If the syslog is displayed on the console indicating that the interface goes Down, and the LED on the interface is off, the interface is disabled. Run the **show interfaces** command, and verify that the interface status changes to Administratively Down. Then run the **no**

shutdown command to enable the interface. If the syslog is displayed on the console indicating that the interface goes Up, and the LED on the interface is on, the interface is enabled.

Configuring Interface Flapping Protection

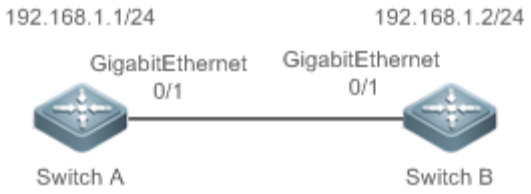
- Run the **physical-port dither protect** command in global configuration mode. Frequently remove and install the network cable on a physical interface to simulate interface flapping. Verify that a syslog indicating interface flapping is displayed on the console. After such a syslog is displayed for several times, the system displays a message indicating that the interface will be shut down. Run the **physical-port dither period** command in global configuration mode to configure parameters of flapping detection, such as the detection period, threshold for triggering flappings, and the number of consecutive periods for triggering violations.

Configuring the Syslog Function

- Run the **logging link-updown** command in global configuration mode to display interface status information. Remove and then install the network cable on a physical interface. The interface status will change twice. Verify that 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 install the network cable. Verify that related information is no longer displayed on the console. This indicates that the syslog function is normal.

Configuration Example

Configuring Basic Attributes of Interfaces

Scenario Figure 1-1	
Configuration Steps	● Connect two devices through the switch interfaces. ● Configure an SVI on two devices respectively, and assign IP addresses from the same network segment to the two SVIs. ● Enable interface index persistence on the two devices. ● Enable the link trap function on the two devices. ● Configure the interface administrative status on the two devices.

A	`A# configure terminal`
	`A(config)# snmp-server if-index persist`
	`A(config)# interface vlan 1`
	`A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0`
	`A(config-if-VLAN 1)# exit`
	`A(config)# interface gigabitethernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# snmp trap link-status`
	`A(config-if-GigabitEthernet 0/1)# shutdown`
	`A(config-if-GigabitEthernet 0/1)# end`
	`A# write`

B	`B# configure terminal`
	`B(config)# snmp-server if-index persist`
	`B(config)# interface vlan 1`
	`B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0`
	`B(config-if-VLAN 1)# exit`
	`B(config)# interface gigabitethernet 0/1`
	`B(config-if-GigabitEthernet 0/1)# snmp trap link-status`

	B(config-if-GigabitEthernet 0/1)# shutdown B(config-if-GigabitEthernet 0/1)# end B# write
Verification	Perform verification on Switch A and Switch B as follows: ● Run the **shutdown** command on GigabitEthernet 0/1, and check whether GigabitEthernet 0/1 and SVI 1 are Down. ● Run the **shutdown** command on GigabitEthernet 0/1, and check whether a trap indicating that this interface is Down is sent. ● Restart the device, and check whether the index of GigabitEthernet 0/1 is the same as that before the restart.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 **GigabitEthernet 0/1 is administratively down**, line protocol is DOWN Hardware is GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b) Interface address is: no ip address MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 1/255, Txload is 1/255 Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes 0 0 0 0 0 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0 4 0 0 0 0 5 0 0 0 0 6 0 0 0 0 7 4 440 0 0 Switchport attributes: interface's description:"" lastchange time:0 Day:20 Hour:15 Minute:22 Second Priority is 0 admin medium-type is Copper, oper medium-type is Copper admin duplex mode is AUTO, oper duplex is Unknown admin speed is AUTO, oper speed is Unknown flow control admin status is OFF, flow control oper status is Unknown admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is

	OFF Port-type: access Vlan id: 1 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 0 bits/sec, 0 packets/sec 4 packets input, 408 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 4 packets output, 408 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets A# show interfaces vlan 1 Index(dec):4097 (hex):1001 VLAN 1 is UP, line protocol is DOWN Hardware is VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af) **Interface address is: 192.168.1.1/24** ARP type: ARPA, ARP Timeout: 3600 seconds MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 0/255, Txload is 0/255
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 **GigabitEthernet 0/1 is administratively down**, line protocol is DOWN Hardware is GigabitEthernet Interface address is: no ip address, address is 00d0.f865.de9b (bia 00d0.f865.de9b) MTU 1500 bytes, BW 1000000 Kbit Encapsulation protocol is Bridge, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Rxload is 1/255, Txload is 1/255 Queue Transmitted packets Transmitted bytes Dropped packets Dropped bytes 0 0 0 0 0 1 0 0 0 0 2 0 0 0 0 3 0 0 0 0 4 0 0 0 0 5 0 0 0 0 6 0 0 0 0 7 4 440 0

```
0
  Switchport attributes:
    interface's description:""
    lastchange time:0 Day:20 Hour:15 Minute:22 Second
    Priority is 0
    admin medium-type is Copper, oper medium-type is Copper
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow control admin status is OFF, flow control oper status is
Unknown
    admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is
OFF
  Port-type: access
    Vlan id: 1
   10 seconds input rate 0 bits/sec, 0 packets/sec
   10 seconds output rate 0 bits/sec, 0 packets/sec
    4 packets input, 408 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    4 packets output, 408 bytes, 0 underruns, 0 dropped
    0 output errors, 0 collisions, 0 interface resets
B# show interfaces vlan 1
Index(dec):4097 (hex):1001
VLAN 1 is UP, line protocol is DOWN
Hardware is  VLAN, address is 00d0.f822.33af (bia 00d0.f822.33af)
Interface address is: 192.168.1.2/24
ARP type: ARPA, ARP Timeout: 3600 seconds
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec, set
  Carrier delay is 2 sec
  Rxload is 0/255, Txload is 0/255
```

1.4.2 Configuring Interface Attributes

Configuration Effect

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

Configuration Step

↘ Configuring a Routed Interface

- Optional.
- Run this command to configure an interface as a Layer 3 routed interface.

- After an interface is configured as a Layer 3 routed interface, Layer 2 protocols running on the interface do not take effect.
- This command is applicable to a Layer 2 switch interface.

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, an Ethernet physical interface is a Layer 2 switch interface.
Command Mode	Interface configuration mode
Usage Guide	On a Layer 3 device, you can run this command to configure a Layer 2 switch interface as a Layer 3 routed interface. You can run the **switchport** command to change a Layer 3 routed interface into a Layer 2 switch interface.

Configuring a Layer 3 Aggregate Interface

- Optional.
- Run the **no switchport** command in interface configuration mode to configure a Layer 2 aggregate interface as a Layer 3 aggregate interface. Run the **switchport** command to configure a Layer 3 aggregate interface as a Layer 2 aggregate interface.
- After an interface is configured as a Layer 3 routed interface, Layer 2 protocols running on the interface do not take effect.
- This command is applicable to a Layer 2 aggregate interface.

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, an aggregate interface is a Layer 2 aggregate interface.
Command Mode	Interface configuration mode
Usage Guide	After entering the configuration mode of a Layer 2 aggregate interface on a Layer 3 device, you can run this command to configure a Layer 2 aggregate interface as a Layer 3 aggregate interface. After entering the configuration mode of a Layer 3 aggregate interface, you can run the **switchport** command to change a Layer 3 aggregate interface into a Layer 2 aggregate interface.

Configuring the Speed of an Interface

- Optional.
- Interface flappings may occur if the configured speed of an interface changes.
- This command is applicable to an Ethernet physical interface or aggregate interface.
- The same speed mode must be configured on four consecutive 25 Gbps interfaces.

Command	**speed** [**10** | **100** | **1000** | **2500** | **5000** | **10G** | **auto**]
Parameter Description	**10**: Indicates that the speed of the interface is 10 Mbps. **100**: Indicates that the speed of the interface is 100 Mbps. **1000**: Indicates that the speed of the interface is 1000 Mbps. **2500**: Indicates that the speed of the interface is 2500 Mbps. **5000**: Indicates that the speed of the interface is 5000 Mbps. **10G**: Indicates that the speed of the interface is 10 Gbps. **auto**: Indicates that the speed of the interface is self-adaptative.
Defaults	By default, the speed of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	If an interface is a member interface of an aggregate interface, the speed of this interface is determined by the speed of the aggregate interface. When the interface is removed from the aggregate interface, it uses its own speed configuration. You can run **show interfaces** to display the speed configuration. The speed options available to an interface vary with the type of the interface. For example, you cannot set the speed of an SFP interface to 10 Mbps.

Configuring the Duplex Mode of an Interface

- Optional.
- Interface flappings may occur if the configured duplex mode of an interface changes.
- This command is applicable to an Ethernet physical interface or aggregate interface.

Command	**duplex** { **auto** | **full** | **half** }
Parameter Description	**auto**: Indicates automatic switching between full duplex and half duplex. **full**: Indicates full duplex. **half**: Indicates half duplex.
Defaults	By default, the duplex mode of an interface is auto.
Command Mode	Interface configuration mode
Usage Guide	The duplex mode of an interface is related to the interface type. You can run **show interfaces** to display the configuration of the duplex mode.

Configuring the Flow Control Mode of an Interface

- Optional.
- Typically, the default flow control mode of an interface is **off** by default. However, the default flow control mode is **on** for some devices.
- After the flow control mode is enabled on an interface, flow control frames will be received or sent to adjust the network data traffic in case of congestion on the interface.
- Interface flappings may occur if the configured duplex mode of an interface changes.
- This command is applicable to an Ethernet physical interface or aggregate interface.

Command	**flowcontrol** { **auto** | **off** | **on** }
Parameter Description	**auto**: Indicates auto-negotiation. **off**: Disables flow control. **on**: Enables flow control.
Defaults	By default, the flow control mode of an interface is **off**.
Command Mode	Interface configuration mode
Usage Guide	You can run the **show interfaces** command to display the flow control configuration and actual flow control information on interfaces.

Configuring the MTU of an Interface

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

Command	**mtu** *num*
Parameter Description	*num*: Indicates the MTU. The value range is from 64 to 2604.
Defaults	By default, the MTU of an interface is 1500 bytes.
Command Mode	Interface configuration mode
Usage Guide	This command is used to configure the interface's 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 that contains one or more member interfaces.

Configuring the Bandwidth of an Interface

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

Command	**bandwidth** *kilobits*
Parameter Description	*kilobits*: Indicates the bandwidth unit, in kilo bits. The value range is from 1 to 2147483647.
Defaults	Typically, the bandwidth of an interface matches the type of the interface. For example, the default bandwidth of a 1000M Ethernet physical interface is 1000000, and that of a 10GE Ethernet physical interface is 10000000.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Carrier Delay of an Interface

- Optional.

- If the configured carrier delay is long, it takes a long time to change the protocol status when the physical status of an interface changes. If the carrier delay is set to 0, the protocol status changes immediately after the physical status of an interface changes.

Command	**carrier-delay** *num*
Parameter Description	*num*: Indicates the carrier delay, in seconds. The value range is from 0 to 60.
Defaults	By default, the carrier delay of an interface is 2s.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Load Interval of an Interface

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

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

Configuring Interface Errdisable Recovery

- Optional.
- By default, an interface will be disabled and will not be recovered after a violation occurs. After interface errdisable recovery is configured, an interface in errdisable state will be recovered and enabled.

Command	**errdisable recovery** [**interval** *time*]
Parameter Description	*time*: Indicates the automatic recovery time, in seconds. The value range is from 30 to 86400.
Defaults	By default, interface errdisable recovery is disabled.
Command Mode	Global configuration mode or privileged EXEC mode (errdisable recovery)
Usage Guide	By default, an interface in errdisable state is not recovered. You can recover the interface manually or run this command to automatically recover the interface.

Verification

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

Command	**show interfaces** [*interface-type interface-number*] [**description | switchport | trunk**]
Parameter Description	*interface-type interface-number*: Indicates the type and number of an interface. **description**: Indicates the interface description, including the link status. **switchport**: Indicates Layer 2 interface information. This parameter is valid only for a Layer 2 interface. **trunk**: Indicates trunk interface 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 specified to display basic interface information.

	`SwitchA#show interfaces GigabitEthernet 0/1`
	`Index(dec):1 (hex):1`
	`GigabitEthernet 0/1 is DOWN, line protocol is DOWN`
	`  Hardware is Broadcom 5464 GigabitEthernet, address is 00d0.f865.de9b (bia 00d0.f865.de9b)`
	`  Interface address is: no ip address`

```
  Interface IPv6 address is:
    No IPv6 address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Ethernet-II, loopback not set
  Keepalive interval is 10 sec, set
  Carrier delay is 2 sec
  Ethernet attributes:
    Last link state change time: 2012-12-22 14:00:48
    Time duration since last link state change: 3 days, 2 hours, 50
minutes, 50 seconds
    Priority is 0
    Medium-type is Copper
    Admin duplex mode is AUTO, oper duplex is Unknown
    Admin speed is AUTO, oper speed is Unknown
    Flow receive control admin status is OFF,flow send control admin
status is OFF
    Flow receive control oper status is Unknown,flow send control oper
status is Unknown
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF
  Bridge attributes:
    Port-type: trunk
    Native vlan:1
    Allowed vlan lists:1-4094  //Allowed VLAN list of the Trunk port
    Active vlan lists:1, 3-4  //Active VLAN list (indicating that only
VLAN 1, VLAN 3, and VLAN 4 are created on the device)
  Rxload is 1/255,Txload is 1/255
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns, 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

- Run the **show 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 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.

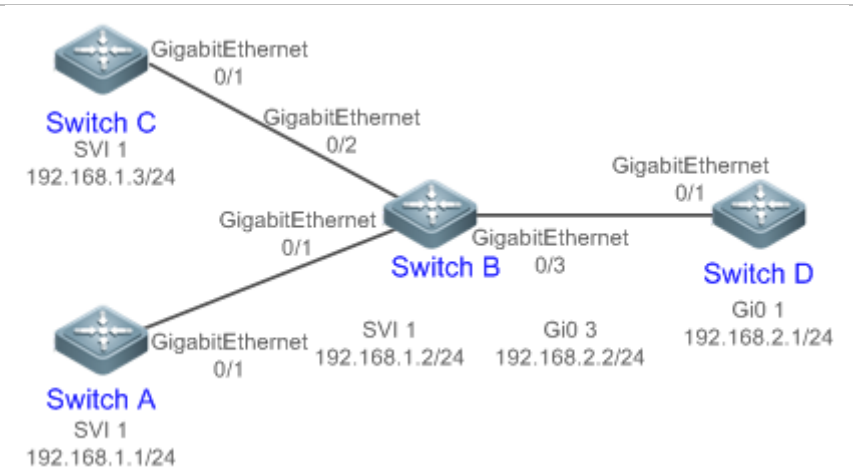
```
Hostname#show interfaces ethernet brief up
down: link down
*down: administratively down
disabled: err-disabled(Please reference to command [show interface status
err-disabled] for detail.)
Interface  Link Stat  Vlan  Auto-Neg  Duplex   Speed    Input Usage  Output
Usage   Description
---------  ---------  ----  --------  -------  -------  -----------
-------------  -----------
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
```

Configuration Example

Configuring Interface Attributes

Scenario Figure 1-5	
Configuration Steps	● On Switch A, configure GigabitEthernet 0/1 as an access interface, and use default VLAN 1. Assign an IP address to SVI 1 and create a route to Switch D. ● On Switch B, configure GigabitEthernet 0/1 and GigabitEthernet 0/2 as trunk interfaces, and use default VLAN 1. Assign an IP address to SVI 1. Configure GigabitEthernet 0/3 as a routed interface, and assign an IP address from another network segment to this interface. ● On Switch C, configure GigabitEthernet 0/1 as an access interface, and use default VLAN 1. Assign an IP address to SVI 1. ● On Switch D, configure GigabitEthernet 0/1 as a routed interface, assign an IP address to this interface, and create a route to Switch A.

A	`A# configure terminal`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# switchport mode access`
	`A(config-if-GigabitEthernet 0/1)# switchport access vlan 1`
	`A(config-if-GigabitEthernet 0/1)# exit`
	`A(config)# interface vlan 1`
	`A(config-if-VLAN 1)# ip address 192.168.1.1 255.255.255.0`
	`A(config-if-VLAN 1)# exit`
	`A(config)# ip route 192.168.2.0 255.255.255.0 VLAN 1 192.168.1.2`

B	`B# configure terminal`
	`B(config)# interface GigabitEthernet 0/1`
	`B(config-if-GigabitEthernet 0/1)# switchport mode trunk`
	`B(config-if-GigabitEthernet 0/1)# exit`
	`B(config)# interface GigabitEthernet 0/2`
	`B(config-if-GigabitEthernet 0/2)# switchport mode trunk`
	`B(config-if-GigabitEthernet 0/2)# exit`
	`B(config)# interface vlan 1`
	`B(config-if-VLAN 1)# ip address 192.168.1.2 255.255.255.0`
	`B(config-if-VLAN 1)# exit`
	`B(config)# interface GigabitEthernet 0/3`
	`B(config-if-GigabitEthernet 0/3)# no switchport`
	`B(config-if-GigabitEthernet 0/3)# ip address 192.168.2.2 255.255.255.0`

	B(config-if-GigabitEthernet 0/3)# exit
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# port-group 1 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface aggregateport 1 C(config-if-AggregatePort 1)# switchport mode access C(config-if-AggregatePort 1)# switchport access vlan 1 C(config-if-AggregatePort 1)# exit C(config)# interface vlan 1 C(config-if-VLAN 1)# ip address 192.168.1.3 255.255.255.0 C(config-if-VLAN 1)# exit
D	D# configure terminal D(config)# interface GigabitEthernet 0/1 D(config-if-GigabitEthernet 0/1)# no switchport D(config-if-GigabitEthernet 0/1)# ip address 192.168.2.1 255.255.255.0 D(config-if-GigabitEthernet 0/1)# exit A(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 0/1 192.168.2.2
Verification	Perform verification on Switch A, Switch B, Switch C, and Switch D as follows: ● On Switch A, ping IP addresses of interfaces of the other three switches. Verify that you can access the other three switches on Switch A. ● Verify that Switch B and Switch D can be pinged mutually. ● Verify that the interface status is correct.
A	A# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de90 (bia 00d0.f865.de90) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF

	Bridge attributes: **Port-type: access** **Vlan id: 1** Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
B	B# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de91 (bia 00d0.f865.de91) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Bridge attributes: **Port-type: trunk** **Native vlan: 1** **Allowed vlan lists: 1-4094** **Active vlan lists: 1** Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets

C	C# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de92 (bia 00d0.f865.de92) Interface address is: no ip address MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full Admin speed is AUTO, oper speed is 100M Flow control admin status is OFF, flow control oper status is OFF Admin negotiation mode is OFF, oper negotiation state is ON Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is OFF Rxload is 1/255, Txload is 1/255 10 seconds input rate 0 bits/sec, 0 packets/sec 10 seconds output rate 67 bits/sec, 0 packets/sec 362 packets input, 87760 bytes, 0 no buffer, 0 dropped Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort 363 packets output, 82260 bytes, 0 underruns, 0 dropped 0 output errors, 0 collisions, 0 interface resets
D	D# show interfaces gigabitEthernet 0/1 Index(dec):1 (hex):1 GigabitEthernet 0/1 is UP, line protocol is UP Hardware is GigabitEthernet, address is 00d0.f865.de93 (bia 00d0.f865.de93) **Interface address is: 192.168.2.1/24** MTU 1500 bytes, BW 100000 Kbit Encapsulation protocol is Ethernet-II, loopback not set Keepalive interval is 10 sec, set Carrier delay is 2 sec Ethernet attributes: Last link state change time: 2012-12-22 14:00:48 Time duration since last link state change: 3 days, 2 hours, 50 minutes, 50 seconds Priority is 0 Admin medium-type is Copper, oper medium-type is Copper Admin duplex mode is AUTO, oper duplex is Full

```
    Admin speed is AUTO, oper speed is 100M
    Flow control admin status is OFF, flow control oper status is
OFF
    Admin negotiation mode is OFF, oper negotiation state is ON
    Storm Control: Broadcast is OFF, Multicast is OFF, Unicast is
OFF
  Rxload is 1/255, Txload is 1/255
  10 seconds input rate 0 bits/sec, 0 packets/sec
  10 seconds output rate 67 bits/sec, 0 packets/sec
    362 packets input, 87760 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    363 packets output, 82260 bytes, 0 underruns, 0 dropped
    0 output errors, 0 collisions, 0 interface resets
```

1.5 Monitoring

Clearing

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

Command	Description
clear counters [*interface-type interface-number*]	Clears the counters of a specified interface.
clear interface *interface-type interface-number*	Resets the interface hardware.

Displaying

Displaying the Interface Configuration and Status

Command	Description
show interfaces [*interface-type interface-number*]	Displays all the status and configuration of a specified interface.
show interfaces [*interface-type interface-number*] **status**	Displays the interface status.
show interfaces [*interface-type interface-number*] **status err-disable**	Displays the interface errdisable status.
show interfaces [*interface-type interface-number*] **link-state-change statistics**	Displays the link status change time and count of a specified interface.
show interfaces [*interface-type interface-number*] **switchport**	Displays the administrative and operational states of switch interfaces (non-routed interfaces).
show interfaces [*interface-type interface-number*] **description** [**up** | **down**]	Displays the description and status of a specified interface.
show interfaces [*interface-type interface-number*] **counters** [**up | down**]	Displays the counters of a specified interface, among which the displayed speed may have an error of ±0.5%.
show interfaces [*interface-type interface-number*] **counters increment** [**up** | **down**]	Displays the number of packets increased in a load interval.
show interfaces [*interface-type interface-number*] **counters error** [**up** | **down**] [**nozero**]	Displays statistics about error packets.
show interfaces [*interface-type interface-number*] **counters rate** [**up | down**] **nozero**]	Displays the packet sending or receiving rate of an interface.

Command	Description
show interfaces [*interface-type interface-number*] **counters summary** [**up** | **down**] [**nozero**]	Displays a summary of interface information.
show interfaces [*interface-type interface-number*] **counters drops** [**up** | **down**]	Displays statistics on discarded packets on an interface.
show interfaces [*interface-type interface-number*] **usage** [**up** | **down**]	Displays the bandwidth usage of an interface.
show interfaces [*interface-type interface-number*] **brief** [**up** | **down**]	Displays brief information about an interface, including the interface status, transmit bandwidth usage, receive bandwidth usage, and numbers of transmitted and received error packets.
show interfaces [*interface-type interface-number*] **ethernet brief** [**up** | **down**] **usage**	Displays brief Ethernet information of an interface, including the link status, VLAN, auto-negotiation mode, duplex mode, interface rates and bandwidth usage, and description (alias). Displays the bandwidth usage of an interface.

1 Configuring Aggregate Interface

1.1 Overview

An aggregate interface is used to bundle multiple physical links into one logical link to increase the link bandwidth and improve connection reliability.

An aggregate interface supports load balancing, namely, distributes load evenly among member links. Besides, an aggregate interface realizes link backup. When a member link of the aggregate interface is disconnected, the load carried by the link is automatically allocated to other functional member links. A member link does not forward broadcast or multicast packets to other member links.

For example, the link between two devices supports a maximum bandwidth of 1000 Mbps. When service traffic carried by the link exceeds 1000 Mbps, excess traffic will be discarded. Interface 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 with the bandwidth of *N* multiplied by 1000 Mbps, where *N* refers to the number of links.

For example, there are two devices connected by a network cable. When the link between the two interfaces of the devices is disconnected, services carried by the link will be interrupted. After the connected interfaces are aggregated, the services will not be affected as long as one link remains connected.

Protocols and Standards

IEEE 802.3ad

1.2 Applications

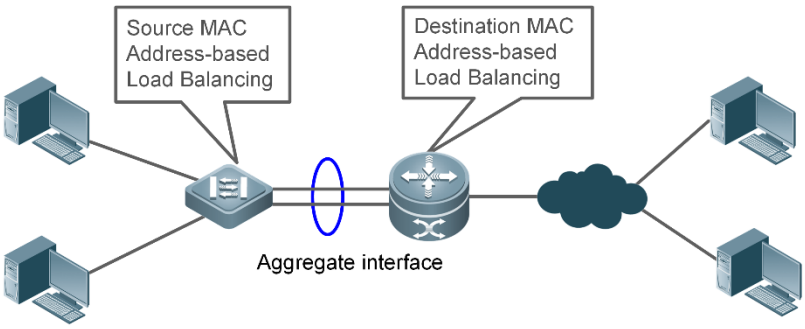
Applications	Description
Link Aggregation and Load Balancing	A large number of packets are transmitted between an aggregation device and a core device, which requires higher bandwidth. To meet this requirement, you can bundle the physical links between the devices into one logical link to increase the link bandwidth, and configure a proper load balancing algorithm to distribute the work load evenly to each physical link, thus improving bandwidth utilization.

1.2.1 Link Aggregation and Load Balancing of the Aggregate Interface

Scenario

In Figure 1-1, the switch communicates with the router through an aggregate interface. All the devices on the intranet (such as the two PCs on the left) use the router as a gateway. All the devices on the extranet (such as the two PCs on the right) send packets to the internet devices through the router, with the gateway's MAC address as its source MAC address. To distribute the load between the router and other hosts to other links, configure destination MAC address-based load balancing. On the switch, configure source MAC address-based load balancing.

Figure 1-1 Link Aggregation and Load Balancing of the Aggregate Interface



Deployment

- Configure the directly connected interfaces between the switch and router to form an aggregate interface in static or Link Aggregation Control Protocol (LACP) mode.
- On the switch, configure a source MAC address-based load balancing algorithm.
- On the router, configure a destination MAC address-based load balancing algorithm.

1.3 Features

Basic Concepts

Static Aggregate Interface

In static mode, physical interfaces are directly added to an aggregate interface through manual configuration and can forward packets when their link status and protocol status are Up.

An aggregate interface in static mode is called a static aggregate interface, and its member interfaces are called static member interfaces.

LACP

LACP enables the local device to exchange information with the connected device through LACP data units (LACPDUs).

An aggregate interface in LACP mode is called an LACP aggregate interface, and its member interfaces are called LACP member interfaces.

AP Member Port Mode

There are three aggregation modes available, namely, active, passive, and static.

AP member interfaces in active mode initiate LACP negotiation. AP member interfaces in passive mode only respond to received LACPDUs. AP member interfaces in static mode do not send LACPDUs for negotiation. The following table lists the requirements for peer interface mode.

Local Interface Mode	Remote Interface Mode
Active mode	Active or passive mode
Passive mode	Active mode
Static mode	Static mode

Member Interface Status

A static member interface has the following states:

- When a member interface is Down, the interface cannot forward packets. The Down state is displayed.
- When a member interface is Up and the link protocol is ready, the interface can forward packets. The Up state is displayed.

An LACP member interface has the following states:

- When the link of an interface is Down, the interface cannot forward packets. The Down state is displayed.
- When the link of an interface is Up and the interface is added to an aggregation group, the bndl state is displayed.
- When the link of an interface is Up but the interface is suspended because the peer end is not enabled with LACP or the attributes of the interface are inconsistent with those of the active interface, the susp state is displayed. (The interface in susp state does not forward packets.)

Only full-duplex interfaces support LACP aggregation.

LACP aggregation can be implemented only when the rates, flow control status, medium types, and Layer 2 or Layer 3 attributes of member interfaces are consistent.

If you change the preceding attributes of a member interface in the aggregation group, LACP aggregation will fail.

The interfaces which are prohibited from joining or exiting an aggregate interface cannot be added to or removed from a static aggregate interface or an LACP aggregate interface.

LACP System ID

One device can be configured with only one LACP aggregation system. The system is identified by a system ID and each system has a priority, which is a configurable value. The system ID consists of the LACP system priority and MAC address of the device. A lower system priority indicates a higher priority of the system ID. If the system priorities are the same, a smaller MAC address of the device indicates a higher priority of the system ID. The system with the system ID of a higher priority determines the interface status. The interface status of a system with an ID of a lower priority keeps consistent with that of a higher priority.

LACP Interface ID

Each interface has an independent LACP interface priority, which is a configurable value. The interface ID consists of the LACP interface priority and interface number. A smaller interface priority indicates a higher priority of the interface ID. If the interface priorities are the same, a smaller interface number indicates a higher priority of the interface ID.

LACP Active Interface

When dynamic member interfaces are Up, LACP selects one of those interfaces to be the active interface based on the rates and duplex modes, ID priorities of the interfaces in the aggregation group, and bundling status of the member interfaces in Up state. Only the interfaces that have the same attributes as the active interface are in bundle state and participate in data forwarding. When the attributes of interfaces are changed, LACP reselects an active interface.

Overview

Overview	Description

Link Aggregation	Aggregates physical links statically or dynamically to increase link bandwidth and achieves link backup.
Load Balancing	Balances the load within an aggregation group flexibly by using different load balancing methods.

1.3.1 Link Aggregation

Working Principle

There are two link aggregation modes: static and LACP modes.

- Static Mode

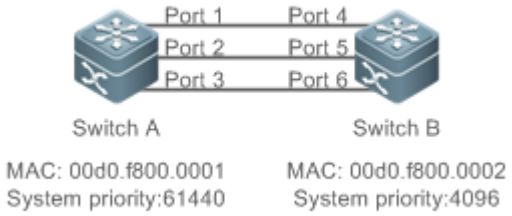
The static aggregate interface configuration is simple. You only need to add the specified physical interface to the aggregate interface through a command. After joining the aggregation group, a member interface can receive and transmit data and participate in load balancing.

- LACP Mode

An LACP-enabled interface sends LACPDUs to advertise its system priority, system MAC address, interface priority, interface number, and operation key. When receiving the LACPDU from the peer end, the device compares the system priorities of both ends based on the system ID in the LACPDU. The end with a higher system ID priority sets the interfaces in the aggregation group to bundle state based on the interface ID priorities in descending order, and sends an updated LACPDU. When receiving the LACPDU, the peer end sets corresponding interfaces to bundle state so that both ends maintain consistency when an interface is removed from or added to the aggregation group. The physical link can forward packets only after the interfaces at both ends are bundled dynamically.

After link aggregation, LACP member interfaces periodically exchange LACPDUs. When an interface does not receive an LACPDU in a given period of time, timeout occurs and the links are unbundled. In this case, the member interfaces cannot forward packets. There are two timeout modes: long and short timeout. In long timeout mode, an interface sends an LACPDU every 30s. If it does not receive an LACPDU from the peer end in 90s, timeout occurs. In short timeout mode, an interface sends an LACPDU every 1s. If it does not receive an LACPDU from the peer end in 3s, timeout occurs.

Figure 1-2 LACP Negotiation



In Figure 1-2, Switch A is connected to Switch B through three interfaces. System priorities of Switch A and Switch B are set to 61440 and 4096 respectively. LACP is enabled on ports 1–6, the aggregation mode of the three interfaces are set to the active mode, and the interface priority is set to the default value 32768.

When receiving an LACPDU from Switch A, Switch B finds that it has a higher system ID priority than Switch A (the system priority of Switch B is higher than that of Switch A). Switch B sets Port 4, Port 5, and Port 6 to bundle state based on the order of interface ID priorities (or in ascending order of interface numbers if the interface priorities are the

same). When receiving an updated LACPDU from Switch B, Switch A finds that Switch B has a higher system ID priority and has set Port 4, Port 5, and Port 6 to bundle state. Then Switch A also sets Port 1, Port 2, and Port 3 to bundle state.

1.3.2 Load Balancing

Working Principle

An aggregate interface identifies packet flows by using load balancing algorithms based on packet characteristics, such as the source and destination MAC addresses, source and destination IP addresses, and Layer 4 source and destination interface numbers. The same packet flow 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 member links based on 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.

The device supports the following load balancing modes:

- Source or destination MAC address
- Source and destination MAC addresses
- Source or destination IP address
- Source and destination IP addresses
- Layer 4 source or destination interface number
- Layer 4 source and destination interface numbers
- Source IP address + Layer 4 source interface number
- Source IP address + Layer 4 destination interface number
- Destination IP address + Layer 4 source interface number
- Destination IP address + Layer 4 destination interface number
- Source IP address + Layer 4 source interface number + Layer 4 destination interface number
- Destination IP address + Layer 4 source interface number + Layer 4 destination interface number
- Source IP address + destination IP address + Layer 4 source interface number
- Source IP address + destination IP address + Layer 4 destination interface number
- Source IP address + destination IP address + Layer 4 source interface number + Layer 4 destination interface number

Load balancing based on IP addresses or interface numbers is applicable only to Layer 3 packets. When a device enabled with this load balancing mode 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 modes. The input parameters include the source MAC address, destination MAC address, source and destination MAC addresses, source IP address, destination IP address, source and destination IP addresses, source and destination IP addresses + Layer 4 interface number, and so on. The algorithm ensures that packets with different input parameters are evenly distributed to member links. It does not indicate that these packets are always distributed to different member links. For example, in IP address-based load balancing, two

packets with different source and destination IP addresses may be distributed to the same member link through calculation.

1.4 Configuration

Configuration	Description and Command	
Configuring a Static Aggregate Interface	(Mandatory) It is used to configure link aggregation manually.	
	interface aggregateport	Creates an Ethernet aggregate interface.
	port-group	Configures static member interfaces.
Configuring an LACP Aggregate Interface	(Mandatory) It is used to configure link aggregation dynamically.	
	port-group mode	Configures LACP member interfaces.
	lacp system-priority	Configures the LACP system priority.
	lacp port-priority	Configures the interface priority.
	lacp short-timeout	Configures the short timeout mode on an interface.
Enabling LinkTrap	(Optional) It is used to enable LinkTrap.	
	snmp trap link-status	Enables LinkTrap advertisement for an aggregate interface.
	aggregateport member linktrap	Enables LinkTrap t for member interfaces.
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 aggregate interface or its member interfaces.
Configuring Aggregate Interface Configuration Delivery from the AC	**ap-interface wire** *portnumber* **-group** *apnumber*	Configures aggregate interface configuration delivery from the AC.

1.4.1 Configuring a Static Aggregate Interface

Configuration Effect

- Manually configure multiple physical interfaces as member interfaces of an aggregate interface to realize link aggregation.
- The bandwidth of the aggregated link is equal to the sum of bandwidth of member links.
- When a member link of the aggregate interface is disconnected, the load carried by the link is automatically allocated to other functional member links.

Notes

- Only physical interfaces can be added to an aggregate interface.
- The interfaces of different media types or interface modes cannot be added to the same aggregate interface.

- Layer 2 interfaces can be added to only a Layer 2 aggregate interface, and Layer 3 interfaces can be added to only a Layer 3 aggregate interface. The Layer 2 or Layer 3 attributes of an aggregate interface that contains member interfaces cannot be modified.
- After an interface is added to an aggregate interface, attributes of the interface are replaced by those of the aggregate interface.
- After an interface is removed from an aggregate interface, attributes of the interface are restored.

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

Static aggregation has no error detection. Member interfaces are bound if links are connected, so you must ensure topology accuracy and consistency among member interfaces' negotiation attributes.

Configuration Step

Creating an Ethernet Aggregate Interface

- Mandatory.
- Perform this configuration on a device that supports the aggregate interface.

Command	**interface aggregateport** *ap-number*
Parameter Description	*ap-number*: Indicates the number of an aggregate interface. The value range is from 1 to 4.
Defaults	By default, no aggregate interface is created.
Command Mode	Global configuration mode
Usage Guide	To create an Ethernet aggregate interface, run **interfaces aggregate** in global configuration mode. To delete the specified Ethernet aggregate interface, run **no interfaces aggregateport** *ap-number* in global configuration mode.

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

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

The aggregate interface must be configured on the devices at both ends of a link and the aggregate interface mode must be the same (static or LACP mode).

Configuring Static AP Member Ports

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

Command	**port-group** *ap-number*
Parameter	**port-group** *ap-number*: Indicates the number of an aggregate interface. The value range is from 1

Description	to 4.
Defaults	By default, no interfaces are added to any static aggregate interface.
Command Mode	Interface configuration mode of the specified Ethernet interface
Usage Guide	To add member interfaces to an aggregate interface, run **port-group** in interface configuration mode. To remove member interfaces from an aggregate interface, run **no port-group** in interface configuration mode.

The static member interfaces configured on the devices at both ends of a link must be consistent.

After a member interface is removed from the aggregate interface, the default settings of member interface are restored. The original configuration of member interfaces may be processed by different functional modules differently, so check the interface settings after a member interface is removed from an aggregate interface.

After a member interface is removed from an aggregate interface, the interface 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 interface again.

Converting a Layer 2 Aggregate Interface to a Layer 3 Aggregate Interface

- Optional.
- To enable Layer 3 routing on an aggregate interface, for example, configure IP addresses or static routing entries, convert the Layer 2 aggregate interface to a Layer-3 aggregate interface and enable routing on the Layer 3 aggregate interface.
- Perform this configuration on the device that supports Layer 2 and Layer 3 features, and the aggregate interface, such as Layer 3 switches or access controllers (ACs).

Command	**no switchport**
Parameter Description	N/A
Defaults	By default, aggregate interfaces are Layer 2 aggregate interfaces.
Command Mode	Aggregate interface configuration mode
Usage Guide	The Layer 3 aggregate interface is supported by only Layer 3 devices.

The aggregate interface created on a Layer 3 device that does not support Layer 2 features is a Layer 3 aggregate interface. Otherwise, the aggregate interface is a Layer 2 aggregate interface.

Verification

- Run **show running-config** to display the configuration.
- Run **show aggregateport summary** to display the aggregate interface configuration.

Command	**show aggregateport** *aggregate-port-number* [**load-balance** | **summary**]
Parameter Description	*aggregate-port-number*: Indicates the number of an aggregate interface. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode

Usage Guide	Information about all aggregate interfaces is displayed if you do not specify the aggregate interface number.

	`Hostname# show aggregateport 1 summary`
	`AggregatePort MaxPorts SwitchPort Mode Ports`
	`------------ -------- ---------- ------`
	`-----------------------------------`
	`Ag1` `32 Enabled TRUNK` **`Gi0/1 ,Gi0/2`**

Configuration Example

Configuring a Static Aggregate Interface

Scenario **Figure 1-3**	
Configuration Steps	● Add GigabitEthernet 0/1 and GigabitEthernet 0/2 on Switch A to static aggregate interface 1. ● Add GigabitEthernet 0/1 and GigabitEthernet 0/2 on Switch B to static aggregate interface 1.

Switch A	`SwitchA# configure terminal`
	`SwitchA(config)# interface range GigabitEthernet 0/1-2`
	`SwitchA(config-if-range)# port-group 1`

Switch B	`SwitchB# configure terminal`
	`SwitchB(config)# interface range GigabitEthernet 0/1-2`
	`SwitchB(config-if-range)# port-group 1`

Verification	● Run **show aggregateport summary** to check whether aggregate interface 3 contains member interfaces GigabitEthernet 1/1 and GigabitEthernet 1/2.

Switch A	`SwitchA# show aggregateport summary`
	`AggregatePort MaxPorts SwitchPort Mode Ports`
	`------------ -------- ---------- ------ -----------------------------------`
	`Ag1` `32 Enabled ACCESS` **`Gi0/1,Gi0/2`**

Switch B	`SwitchB# show aggregateport summary`
	`AggregatePort MaxPorts SwitchPort Mode Ports`
	`------------ -------- ---------- ------ -----------------------------------`
	`Ag1` `32 Enabled ACCESS` **`Gi0/1,Gi0/2`**

1.4.2 Configuring an LACP Aggregate Interface

Configuration Effect

- Connected devices realize dynamic link aggregation through LACP auto-negotiation.

- The bandwidth of the aggregated link is equal to the sum of bandwidth of member links.
- When a member link of the aggregate interface is disconnected, the load carried by the link is automatically allocated to other functional member links.
- It takes LACP 90s to detect a link failure in long timeout mode and 3s in short timeout mode.

Notes

- After a member interface is removed from the LACP aggregate interface, the default settings of member interface are restored. The original configuration of member interfaces may be processed by different functional modules differently, so check the interface settings after a member interface is removed from an LACP aggregate interface.
- Changing the LACP system priority may cause LACP member interfaces to be disaggregated and aggregated again.
- Changing the priority of an LACP member interface may cause the other member interfaces to be disaggregated and aggregated again.

Configuration Step

Configuring LACP Member Interfaces

- Mandatory.
- Perform this configuration on the LACP-enabled device.

Command	**port-group** *key-number* **mode** { **active | passive** }
Parameter Description	*Key-number*: Indicates the management key of an aggregate interface, that is, LACP aggregate interface number. The value range is from 1 to 4. **active**: Indicates that interfaces are added to a dynamic aggregate interface actively. **passive**: Indicates that interfaces are added to a dynamic aggregate interface passively.
Defaults	By default, no physical interfaces are added to any LACP aggregate interface.
Command Mode	Physical interface configuration mode
Usage Guide	Use this command in interface configuration mode to add member interfaces to an LACP aggregate interface.

The LACP member interface configuration at both ends of a link must be consistent.

Configuring the LACP System Priority

- Optional.
- Perform this configuration when you need to adjust the system ID priority. A smaller value indicates a higher system ID priority. The device with a higher system ID priority selects an aggregate interface.
- Perform this configuration on the LACP-enabled device.

Command	**lacp system-priority** *system-priority*
Parameter Description	*system-priority*: Indicates the LACP system priority. The value range is from 0 to 65535.
Defaults	By default, the LACP system priority is 32768.
Command	Global configuration mode

Mode	
Usage Guide	Use this command in global configuration mode to configure the LACP system priority. All the dynamic member links share one LACP system priority. Changing the LACP system priority will affect all member links. To restore the default settings, run **no lacp system-priority** in interface configuration mode.

Configuring the Priority of an LACP Member Interface

- Optional.
- Perform this configuration when you need to specify the interface ID priority. A smaller value indicates a higher interface ID priority. The interface with the highest interface ID priority will be selected as the active interface.
- Perform this configuration on the LACP-enabled device.

Command	**lacp port-priority** *port-priority*
Parameter Description	*port-priority*: Indicates the priority of an LACP member interface. The value range is from 0 to 65535.
Defaults	By default, the priority of an LACP member interface is 32768.
Command Mode	Physical interface configuration mode
Usage Guide	Use this command in global configuration mode to configure the priority of an LACP member interface. To restore the settings, run **no lacp port-priority** in interface configuration mode.

Configuring the Timeout Mode of LACP Member Interfaces

- Optional.
- To implement real-time link failure detection, configure the short timeout mode. It takes LACP 90s to detect a link failure in long timeout mode and 3s in short timeout mode.
- Perform this configuration on the LACP-enabled device, such as switch.

Command	**lacp short-timeout**
Parameter Description	N/A
Defaults	By default, the timeout mode of LACP member interfaces is long.
Command Mode	Interface configuration mode
Usage Guide	The timeout mode is supported only by physical interfaces. To restore the default settings, run **no lacp short-timeout** in interface configuration mode.

Verification

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

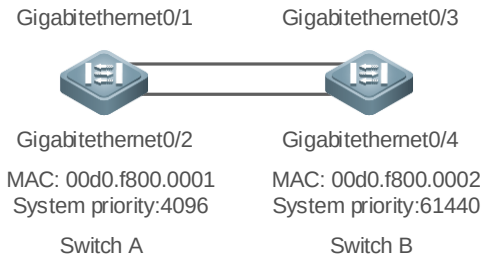
Command	**show lacp summary** [*key-number*]
Parameter Description	*key-name*: Indicates the number of an LACP aggregate interface.
Command	Any mode

Mode	
Usage Guide	Information about all LACP aggregate interfaces is displayed if you do not specify *key-name*.

```
Hostname(config)# show lacp summary 1
System Id:32768, 00d0.f8fb.0002
Flags:  S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs.
A - Device is in active mode.       P - Device is in passive mode.
Aggregated port 1:
Local information:
LACP port      Oper    Port     Port
Port     Flags     State     Priority       Key     Number  State
---------------------------------------------------------------------
Gi0/1     SA       bndl       4096        0x3     0x1      0x3d
Gi0/2     SA       bndl       4096        0x3     0x2      0x3d
Gi0/3     SA       bndl       4096        0x3     0x3      0x3d
Partner information:
                LACP port               Oper    Port     Port
Port     Flags     Priority     Dev ID       Key     Number   State
---------------------------------------------------------------------
Gi0/1     SA       61440     00d0.f800.0001   0x3     0x1     0x3d
Gi0/2     SA       61440     00d0.f800.0001   0x3     0x2     0x3d
Gi0/3     SA       61440     00d0.f800.0001   0x3     0x3     0x3d
```

Configuration Example

Configuring LACP

Scenario Figure 1-4	
Configuration Steps	● On Switch A, set the LACP system priority to 4096. ● Enable dynamic link aggregation on GigabitEthernet0/1 and GigabitEthernet0/2 of Switch A and add the interfaces to LACP aggregate interface 1. ● On Switch B, set the LACP system priority to 61440.

	● Enable dynamic link aggregation on GigabitEthernet0/3 and GigabitEthernet0/4 on Switch B and add the interfaces to LACP aggregate interface 1.
Switch A	SwitchA# configure terminal SwitchA(config)# lacp system-priority 4096 SwitchA(config)# interface range GigabitEthernet 0/1-2 SwitchA(config-if-range)# port-group 1 mode active SwitchA(config-if-range)# end
Switch B	SwitchB# configure terminal SwitchB(config)# lacp system-priority 61440 SwitchB(config)# interface range GigabitEthernet 0/3-4 SwitchB(config-if-range)# port-group 1 mode active SwitchB(config-if-range)# end
Verification	● Run **show lacp summary 1** to check whether LACP aggregate interface 1 contains member interfaces GigabitEthernet2/1 and GigabitEthernet2/2.
Switch A	SwitchA# show LACP summary 1 System Id:32768, 00d0.f8fb.0001 Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs. A - Device is in active mode. P - Device is in passive mode. Aggregated port 1: Local information: LACP port Oper Port Port Port Flags State Priority Key Number State --- Gi0/1 SA bndl 32768 0x3 0x1 0x3d Gi0/2 SA bndl 32768 0x3 0x2 0x3d Partner information: LACP port Oper Port Port Port Flags Priority Dev ID Key Number State --- Gi0/1 SA 32768 00d0.f800.0002 0x3 0x1 0x3d Gi0/2 SA 32768 00d0.f800.0002 0x3 0x2 0x3d
Switch B	SwitchB# show LACP summary 1

```
System Id:32768, 00d0.f8fb.0002

Flags:  S - Device is requesting Slow LACPDUs

 F - Device is requesting Fast LACPDUs.

A - Device is in active mode.       P - Device is in passive mode.

Aggregated port 1:

Local information:

LACP port      Oper    Port     Port

Port     Flags     State     Priority       Key     Number    State

---------------------------------------------------------------------------

Gi0/3     SA       bndl       32768        0x3     0x1      0x3d

Gi0/4     SA       bndl       32768        0x3     0x2      0x3d

Partner information:

                LACP port                Oper    Port    Port

Port     Flags     Priority     Dev ID      Key     Number  State

---------------------------------------------------------------------

Gi0/3     SA       32768     00d0.f800.0001   0x3     0x1     0x3d

Gi0/4     SA       32768     00d0.f800.0001   0x3     0x2     0x3d
```

1.4.3 Enabling LinkTrap

Configuration Effect

Enable the system with LinkTrap to send LinkTrap messages when aggregation links are changed.

Configuration Step

Enabling LinkTrap for an Aggregate Interface

- Optional.
- Enable LinkTrap in interface configuration mode. By default, LinkTrap is enabled. LinkTrap messages are sent when the link status or protocol status of the aggregate interface is changed.
- Perform this configuration on the AP-enabled device.

Command	**snmp trap link-status**
Parameter Description	N/A
Defaults	By default, LinkTrap is enabled.
Command Mode	Aggregate interface configuration mode
Usage Guide	Use this command in interface configuration mode to enable LinkTrap for the specified aggregate interface. After LinkTrap is enabled, LinkTrap messages are sent when the link status of the aggregate interface is changed. Otherwise, LinkTrap messages are not sent. By default, LinkTrap is enabled. To disable LinkTrap for an aggregate interface, run **no snmp trap link-status** in interface configuration mode. LinkTrap cannot be enabled for a specific member interface. To enable LinkTrap for all member interfaces, run **aggregateport member linktrap** in global configuration mode.

Enabling LinkTrap for Member Interfaces

- Optional.
- By default, LinkTrap is disabled for member interfaces.
- Perform this configuration on the AP-enabled device.

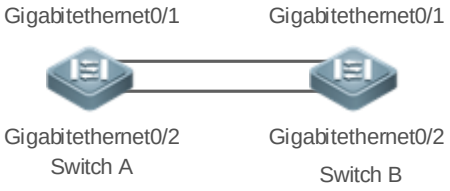
Command	**aggregateport member linktrap**
Parameter Description	N/A
Defaults	By default, LinkTrap is disabled for member interfaces.
Command Mode	Global configuration mode
Usage Guide	Use this command in global configuration mode to enable LinkTrap for all member interfaces. By default, LinkTrap messages are not sent when the link status of member interfaces is changed. To disable LinkTrap for all member interfaces, run **no aggregateport member linktrap** in global configuration mode.

Verification

- Run **show running-config** to display the configuration.
- After LinkTrap is enabled, you can monitor this feature on aggregate interfaces or their member interfaces by using the MIB software.

Configuration Example

Enabling LinkTrap for Member Interfaces

Scenario **Figure 1-5**	
Configuration Steps	● Add GigabitEthernet 0/1 and GigabitEthernet 0/2 on Switch A to static aggregate interface 1. ● Add GigabitEthernet 0/1 and GigabitEthernet 0/2 on Switch B to static aggregate interface 1. ● On Switch A, disable LinkTrap for aggregate interface 1 and enable LinkTrap for its member interfaces. ● On Switch B, disable LinkTrap for aggregate interface 1 and enable LinkTrap its AP member interfaces.

Switch A	`SwitchA# configure terminal`
	`SwitchA(config)# interface range GigabitEthernet 0/1-2`
	`SwitchA(config-if-range)# port-group 1`
	`SwitchA(config-if-range)# exit`
	`SwitchA(config)# aggregateport member linktrap`
	`SwitchA(config)# interface Aggregateport 1`
	`SwitchA(config-if-AggregatePort 3)# no snmp trap link-status`

Switch B	`SwitchB# configure terminal`
	`SwitchB(config)# interface range GigabitEthernet 0/1-2`
	`SwitchB(config-if-range)# port-group 1`
	`SwitchB(config-if-range)# exit`
	`SwitchB(config)# aggregateport member linktrap`
	`SwitchB(config)# interface Aggregateport 1`
	`SwitchB(config-if-AggregatePort 3)# no snmp trap link-status`

Verification	● Run **show running-config** to check whether LinkTrap is enabled for aggregate interface 3 and its member interfaces.
Switch A	`SwitchA# show run interface AggregatePort 1` `Building configuration...`

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

1.4.4 Configuring a Load Balancing Mode

Configuration Effect

The system distributes incoming packets among member links by using the specified load balancing algorithm. The same packet flow is transmitted by one member link, whereas different packet flows are evenly distributed to various links.

Notes

N/A

Configuration Step

↘ Configuring the Global Load Balancing Algorithm of an Aggregate Interface

- Optional. Perform this configuration when you need to optimize load balancing.
- Perform this configuration on the AP-enabled device.

Command	**aggregateport load-balance** { **dst-mac** | **src-mac** | **src-dst-mac** | **dst-ip** | **src-ip** | **src-dst-ip** | **src-dst-ip-l4port** | **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** }
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 interface numbers. **src- l4port**: Indicates that load is distributed based on Layer 4 source interface numbers. **dst- l4port**: Indicates that load is distributed based on Layer 4 destination interface numbers. **src-dst-l4port**: Indicates that load is distributed based on Layer 4 source and destination interface numbers. **src-ip-src-l4port**: Indicates that load is distributed based on source IP addresses and Layer 4 source interface numbers. **src-ip-dst-l4port**: Indicates that load is distributed based on source IP addresses and Layer 4 destination interface numbers. **dst-ip-src-l4port**: Indicates that load is distributed based on destination IP addresses and Layer 4 source interface numbers. **dst-ip-dst-l4port**: Indicates that load is distributed based on destination IP addresses and Layer 4 destination interface numbers. **src-ip-src-dst-l4port:** Indicates that load is distributed based on source IP addresses as well as Layer 4 source and destination interface numbers. **dst-ip-src-dst-l4port**: Indicates that load is distributed based on destination IP addresses as well as Layer 4 source and destination interface numbers. **src-dst-ip-src-l4port**: Indicates that load is distributed based on source and destination IP addresses as well as Layer 4 source interface 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.
Defaults	Load balancing can be based on source and destination MAC addresses or source and destination IP addresses.
Command Mode	Global configuration mode
Usage Guide	-

Verification

- Run **show running-config** to display the configuration.
- Run **show aggregateport load-balance** to display the load balancing configuration.
- Run **show aggregateport summary** to display the configuration.

Command	**show aggregateport** [*aggregate-port-number*] { **load-balance | summary** }
Parameter Description	*aggregate-port-number*: Indicates the number of an aggregate interface. **load-balance**: Displays the load balancing algorithm. **summary**: Displays the summary of each link.
Command Mode	Any mode
Usage Guide	Information about all aggregate interfaces is displayed if you do not specify the aggregate interface number.

	Hostname# show aggregateport 1 summary AggregatePort MaxPorts SwitchPort Mode Ports ---------- -------- ---------- ------ ---------- **Ag1** 32 Enabled TRUNK **Gi0/1 ,Gi0/2**

Configuration Example

Configuring a Load Balancing Mode

Scenario **Figure 1-6**	
Configuration Steps	● Add GigabitEthernet 0/1 and GigabitEthernet 0/2 on Switch A to static aggregate interface 1. ● Add GigabitEthernet 0/1 and GigabitEthernet 0/2 on Switch B to static aggregate interface 1. ● On Switch A, configure source MAC address-based load balancing for aggregate interface 1 in global configuration mode. ● On Switch B, configure destination MAC address-based load balancing for aggregate interface 1 in global configuration mode.
Switch A	SwitchA# configure terminal SwitchA(config)# interface range GigabitEthernet 0/1-2 SwitchA(config-if-range)# port-group 1 SwitchA(config-if-range)# exit SwitchA(config)# aggregateport load-balance src-mac
Switch B	SwitchB# configure terminal SwitchB(config)# interface range GigabitEthernet 0/1-2 SwitchB(config-if-range)# port-group 1 SwitchB(config-if-range)# exit SwitchB(config)# aggregateport load-balance dst-mac
Verification	● Run **show aggregateport load-balance** to display the load balancing algorithm configuration.
Switch A	SwitchA# show aggregatePort load-balance Load-balance : **Source MAC**
Switch B	SwitchB# show aggregatePort load-balance Load-balance : **Destination MAC**

1.4.5 Configuring Aggregate Interface Configuration Delivery from the AC

Configuration Effect

- After the AC delivers the aggregate interface configuration to the AP, the corresponding wired interface on the AP will be added to or removed from the corresponding aggregate interface.

Notes

- To ensure normal link aggregation, static member interfaces need to be configured consistently on the two devices of a link.
- After a member interface is added to an aggregate interface, the member interface cannot be added to other aggregate interfaces. The member interface can be added to another aggregate interface only after it is removed from the original aggregate interface.

Configuration Step

↘ Configuring Aggregate Interface Configuration Delivery from the AC

- Optional
- Perform this operation when a wired interface of a specific AP, AP group, or all APs needs to be added to the aggregate interface.

Command	**ap-interface wireport** *port-number* **port-group** *ap-number*
Parameter Description	**port-number**: Indicates the ID of the wired interface on the AP. **ap-number**: Indicates the ID of the aggregate interface.
Defaults	By default, the AC does not deliver the aggregate interface configuration.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	In AP configuration mode or AP group configuration mode, run **ap-interface wireport** *port-number* **port-group** *ap-number* to deliver the aggregate interface configuration to enable a wired interface on the AP to be added to the aggregate interface, and run **no ap-interface wireport** *port-number* **port-group** to remove a wired interface from the aggregate interface

Verification

- Run **show running-config** to display the corresponding configuration.
- Run **show aggregateport summary** to display the relationship between the aggregate interface and member interfaces.

Command	**show aggregateport summary**
Parameter Description	**ap-num**: Indicates the AP number.
Command Mode	All modes
Usage Guide	-

Command Presentation	`Hostname# show aggregateport summary`
	
	`AggregatePort MaxPorts  Ports`

	``` ------------- -------- --------------------------------- Ag1 8 Gi0/1,Gi0/2 ```

1.5 Monitoring

Displaying

Command	Description
show lacp summary [*key-number*]	Displays the LACP aggregation status. You can check information about a specific LACP aggregation group by specifying ***key*-number**.
show aggregateport { **load-balance** | [*aggregate-port-number*] **summary** }	Displays the summary or load balancing algorithm of an aggregate interface.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug lsm ap	Debugs an aggregate interface.

Configuring Ethernet Switching

1. Configuring MAC Address
2. Configuring VLAN
3. Configuring MAC VLAN
4. Configuring Super VLAN
5. Configuring VLAN Group
6. Configuring MSTP

1 Configuring MAC Address

1.1 Overview

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

When a device forwards a packet, it looks up an outbound interface from its MAC address table according to the destination MAC address and VLAN ID of the packet. Then the packet is unicast, multicast, or broadcast.

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

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 Applications

Application	Description
MAC Address Learning	Forward unicast packets through MAC addresses learning.
MAC Address Change Notification	Monitor change of user devices connected to a network device through MAC address change notification.

1.2.1 MAC Address Learning

Scenario

Typically, a device maintains a MAC address table by learning MAC addresses dynamically.

As shown in Figure 1-1, the MAC address table of the device is empty. When User A communicates with User B, it sends a packet to GigabitEthernet 0/2 of the device, and the device learns the MAC address of User A and stores it in the table.

Because the table does not contain the MAC address of User B, the device broadcasts the packet to interfaces of all connected devices (User B and User C) except User A.

Figure 1-1 Step 1 of MAC Address Learning

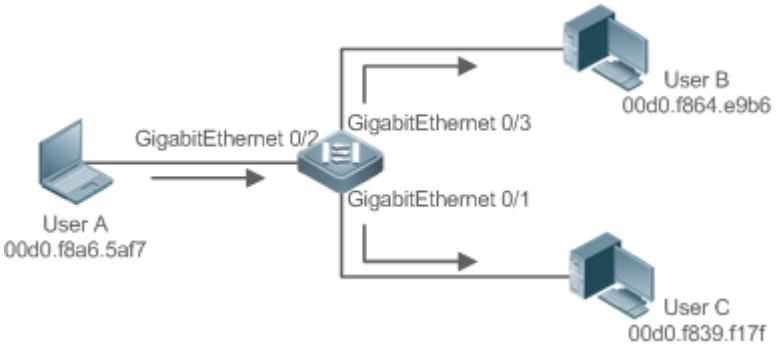


Figure 1-2 MAC Address Table 1

Status	VLAN ID	MAC Address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2

When User B receives the packet, it sends a reply packet to User A through GigabitEthernet 0/3 on the switch. Because the MAC address of User A is already in the MAC address table, the switch sends the reply unicast packet to GigabitEthernet 0/2 and learns the MAC address of User B. User C does not receive the reply packet from User B to User A.

Figure 1-3 Step 2 of MAC Address Learning

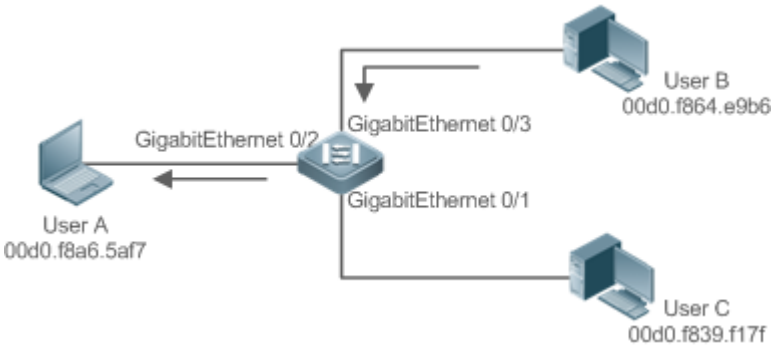


Figure 1-4 MAC Address Table 2

Status	VLAN ID	MAC Address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2
Dynamic	1	00d0.f8a4.e9b6	GigabitEthernet 0/3

Through interaction between User A and User B, the switch learns the MAC addresses of User A and User B. Then packets between User A and User B will be unicast without being received by User C.

Deployment

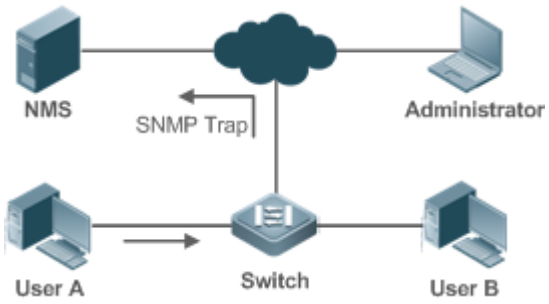
- With MAC address learning, a Layer 2 switch unicasts packets, reducing broadcast packets and network load.

1.2.2 MAC Address Change Notification

MAC address change notification provides a mechanism for the network management system (NMS) to monitor the change of user devices connected to a network device.

Scenario

Figure 1-5 MAC Address Change Notification



With MAC address change notification enabled, the device generates a notification message when the device learns a new MAC address or finishes aging a learned MAC address, and sends the message in an SNMP trap message to a specified NMS.

A notification of adding a MAC address indicates that a new user accesses a network, and a notification of deleting a MAC address indicates that a user sends no new packet within an aging time and usually the user exits the network.

When a network device is connected to a large number of devices, many MAC address changes may occur in a short time, resulting in an increase in traffic. To reduce traffic, you may configure an interval for sending MAC address change notifications. When the interval expires, all notifications generated during the interval are encapsulated into a message. When a notification is generated, it is stored in the table of historical MAC address change notifications. The administrator may know recent MAC address changes by checking the table even without the NMS.

A MAC address change notification is generated only for dynamic MAC addresses.

Deployment

- Enable MAC address change notification on a Layer 2 switch to monitor the change of devices connected to a network device.

1.3 Features

Basic Concepts

Dynamic MAC Address

A dynamic MAC address is generated through MAC address learning on 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 learning the MAC address. 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.

Unicast Forwarding

If a device finds the MAC address that matches the destination MAC address and VLAN ID of packets in its MAC address table and the outbound interface is unique, it will send the packet through the interface directly.

Broadcast Forwarding

If a device receives a packet with the destination address of ffff.ffff.ffff or no MAC address entry in the MAC address table matches the packet, it will send the packet through all the interfaces in the VLAN where the packet is from, except the inbound interface.

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.

1.3.1 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 greater 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.

1.3.2 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 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 greater 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.

1.4 Configuration

Configuration	Description and Command	
Configuring a Dynamic MAC Address	⚠ (Optional) It is used to enable MAC address learning.	
	mac-address-learning	Configures MAC address learning globally or on an interface.
	mac-address-table aging-time	Configures an aging time for a dynamic MAC address.
Configuring a Static MAC Address	⚠ (Optional) It is used to bind the MAC address of a device to an interface of a switch.	
	mac-address-table static	Configures a static MAC address.
Configuring a MAC Address for Packet Filtering	⚠ (Optional) It is used to filter packets.	
	mac-address-table filtering	Configures a MAC address for packet filtering.
Configuring MAC Address Change Notification	⚠ (Optional) It is used to monitor change of user devices connected to a network device.	
	mac-address-table notification	Configures MAC address change notification globally.
	snmp trap mac-notification	Configures MAC address change notification on an interface.

1.4.1 Configuring a Dynamic MAC Address

Configuration Effect

Learn MAC addresses dynamically and forward packets in unicast mode.

Notes

- N/A

Configuration Step

↘ Configuring MAC Address Learning on Interface

- Optional.
- You can perform this configuration to disable MAC address learning on an interface.

Command	**mac-address-learning**
Parameter Description	N/A
Defaults	MAC address learning is enabled by default.
Command Mode	Interface configuration mode
Usage Guide	Perform this configuration on a Layer 2 interface, for example, a switch interface or an aggregate interface. If you run the **default interface** command in global configuration mode and Layer 2 sub-interfaces

	are configured on an interface, the default configuration of MAC address learning on the interface cannot be restored.

By default, MAC address learning is enabled. If 802.1X, IP source guard, or port security is configured on an interface, MAC address learning cannot be enabled. Access control cannot be enabled on an interface with MAC address learning disabled.

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 0 or in the range from 10 to 630. 0 indicates that the MAC address aging is disabled.
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 twice 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 of dynamic MAC addresses.

Command	**show mac-address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: Displays the information about a specific dynamic MAC address. **interface** *interface-id*: Specifies a physical interface or an aggregate interface. **vlan** *vlan-id*: Displays 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	VLAN where the MAC address resides.
	MAC Address	-
	Type	MAC address type
	Interface	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 1-6	
Configuration Steps	● Enable MAC address learning on an interface. ● Set the aging time for dynamic MAC addresses to 180s. ● Delete all dynamic MAC addresses in VLAN 1 on GigabitEthernet 0/1.

	`Hostname# configure terminal`
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# mac-address-learning`
	`Hostname(config-if-GigabitEthernet 0/1)# exit`
	`Hostname(config)# mac aging-time 180`
	`Hostname# clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan 1`

Verification	● Check MAC address learning on an interface. ● Display the aging time of dynamic MAC addresses. ● Display all dynamic MAC addresses in VLAN 1 on 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 interface or aggregate interface.

1.4.2 Configuring a Static MAC Address

Configuration Effect

- Bind the MAC address of a network device to an interface of a switch.

Notes

- N/A

Configuration Step

↘ Configuring a Static MAC address

- Optional.
- Bind the MAC address of a network device to an interface of a switch.

Command	**mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*
Parameter Description	**address** *mac-address*: Specifies a MAC address. **vlan** *vlan-id*: Specifies a VLAN where the MAC address resides. **interface** *interface-id*: Specifies a physical interface or an aggregate interface.
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 in a specified VLAN, the packet is forwarded to the bound interface.

Verification

- Run the **show mac-address-table static** command to check whether the configuration takes effect.

Command	**show mac-address-table static** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]
Parameter Description	**address** *mac-address*: Specifies a MAC address. **interface** *interface-id*: Specifies a physical interface or an aggregate interface. **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

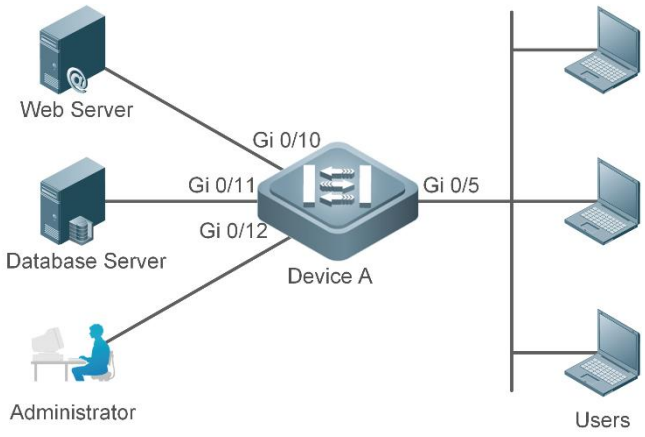
	`Hostname# show mac-address-table static`
	`Vlan MAC Address Type Interface`
	`----- ----------- -------- ------------------`
	`1 00d0.f800.1001 STATIC GigabitEthernet 0/1`
	`1 00d0.f800.1002 STATIC GigabitEthernet 0/1`
	`1 00d0.f800.1003 STATIC GigabitEthernet 0/1`

Configuration Example

Configuring a Static MAC address

The following table lists the mapping between the MAC addresses, VLAN IDs, and interface numbers.

Role	MAC Address	VLAN ID	Interface Number
Web server	00d0.3232.0001	VLAN2	Gi0/10
Database server	00d0.3232.0002	VLAN2	Gi0/11
Administrator	00d0.3232.1000	VLAN2	Gi0/12

Scenario **Figure 1-7**	
Configuration Steps	● Specify the destination MAC address (*mac-address*). ● Specify the VLAN (*vlan-id*) where the MAC addresses reside. ● Specify the interface number (*interface-id*).

Device A	`Hostname# configure terminal`
	`Hostname(config)# mac-address-table static 00d0.f800.3232.0001 vlan 2 interface gigabitEthernet 0/10`
	`Hostname(config)# mac-address-table static 00d0.f800.3232.0002 vlan 2 interface gigabitEthernet 0/11`
	`Hostname(config)# mac-address-table static 00d0.f800.3232.1000 vlan 2 interface gigabitEthernet 0/12`

Verification	Display the static MAC address configuration on a device.

Device A	`Hostname# show mac-address-table static`
	`Vlan MAC Address Type Interface`
	`---------- -------------------- -------- -------------------`
	`2 00d0.f800.3232.0001 STATIC GigabitEthernet 0/10`
	`2 00d0.f800.3232.0002 STATIC GigabitEthernet 0/11`
	`2 00d0.f800.3232.1000 STATIC GigabitEthernet 0/12`

Common Errors

- Configure a static MAC address before configuring the specific interface as a Layer 2 interface, for example, a switch interface or an aggregate interface.

1.4.3 Configuring a MAC Address for Packet Filtering

Configuration Effect

- If a device receives packets containing a source MAC address or destination MAC address specified as the filtered MAC address, the packets are discarded.

Notes

- N/A

Configuration Step

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 filtering** [**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, or 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

1.4.4 Configuring MAC Address Change Notification

Configuration Effect

- Monitor change of user devices connected to a network device.

Notes

- N/A

Configuration Step

Configuring the NMS

- Optional.
- Perform this configuration to enable an NMS to receive MAC address change notifications.

Command	**snmp-server host** *host-addr* **traps** [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }] *community-string*
Parameter Description	**host** *host-addr*: Specifies the IP address of a receiver. **version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**] }: Specifies the version of SNMP trap messages. You can also specify authentication and a security level for packets of Version 3. *community-string*: Indicates an authentication name.
Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling SNMP Trap

- Optional.
- Perform this configuration to send SNMP trap messages.

Command	**snmp-server enable traps**
Parameter Description	N/A
Defaults	By default, the function is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Global MAC Address Change Notification

- Optional.
- If MAC address change notification is disabled globally, it is disabled on all interfaces.

Command	**mac-address-table notification**
Parameter Description	N/A

Defaults	By default, MAC address change notification is disabled globally.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring MAC Address Change Notification on an Interface

- Optional.
- Perform this configuration to enable MAC address change notification on an interface.

Command	**snmp trap mac-notification** { **added** | **removed** }
Parameter Description	**added**: Generates a notification when an MAC address is added. **removed**: Generates a notification when an MAC address is deleted.
Defaults	By default, MAC address change notification is disabled on an interface.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Interval for Generating MAC Address Change Notifications and the Maximum Number of Entries in the Notification History Table

- Optional.
- Perform this configuration to modify the interval for generating MAC address change notifications and the maximum number of entries in the notification history table.

Command	**mac-address-table notification** { **interval** *value* | **history-size** *value* }
Parameter Description	**interval** *value*: Indicates the interval for generating MAC address change notifications, in seconds. The value range is from 1 to 3600. **history-size** *value*: Indicates the maximum number of entries in the notification history table. The value range is from 1 to 200.
Defaults	The default interval is 1 second and the default maximum number of entries in the notification history table is 50.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show mac-address-table notification** command to check whether the NMS receives MAC address change notifications.

Command	**show mac-address-table notification** [**interface** [*interface-id*] | **history**]
Parameter Description	**interface**: Displays the configuration of MAC address change notification on all interfaces. *interface-id*: Displays the configuration of MAC address change notification on a specified interface. **history**: Displays the history of MAC address change notifications.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	N/A

Usage Guide

Display the configuration of global MAC address change notification.

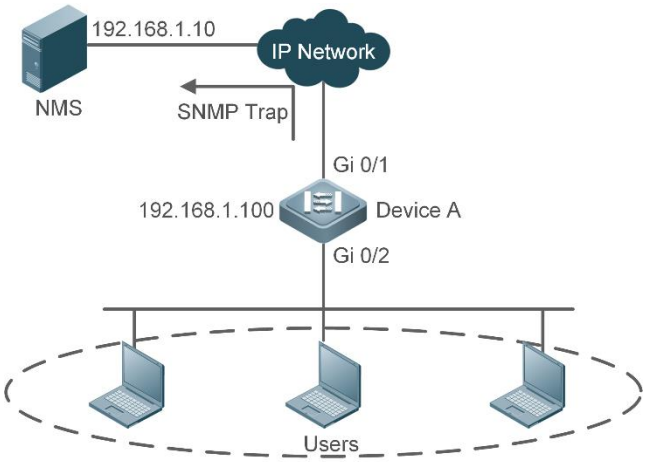
```
Hostname#show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 300
Maximum History Size : 50
Current History Size : 0
```

Field	Description
Interval(Sec)	Interval for generating MAC address change notifications
Maximum History Size	Maximum number of entries in the notification history table
Current History Size	Current number of entries in the notification history table

Configuration Example

Scenario

Figure 1-8



The figure shows an intranet of an enterprise. Users are connected to A through Gi0/2.

Perform the configuration to achieve the following effects:

- When Gi0/2 learns a new MAC address or finishes aging a learned MAC address, a MAC address change notification is generated.
- A sends the MAC address change notification in an SNMP trap message to a specified NMS.
- In a scenario where A is connected to a number of users, the configuration can prevent MAC address change notification burst in a short time so as to reduce the network load.

Configuration Steps

- Enable global MAC address change notification on A, and configure MAC address change notification on Gi0/2.
- Configure the IP address of the NMS host, and enable A to send SNMP trap messages. A communicates with the NMS through routing.
- Configure the interval for sending MAC address change notifications to 300s (1s by default).

Device A

```
Hostname# configure terminal
Hostname(config)# mac-address-table notification
Hostname(config)# interface gigabitEthernet 0/2
Hostname(config-if-GigabitEthernet 0/2)# snmp trap mac-notification added
Hostname(config-if-GigabitEthernet 0/2)# snmp trap mac-notification removed
Hostname(config-if-GigabitEthernet 0/2)# exit
```

	Hostname(config)# snmp-server host 192.168.1.10 traps version 2c comefrom2 Hostname(config)# snmp-server enable traps Hostname(config)# mac-address-table notification interval 300
Verification	● Check whether MAC address change notification is enabled globally. ● Check whether MAC address change notification is configured on the interface. ● Display MAC addresses of interfaces, and run the **clear mac-address-table dynamic** command to simulate aging dynamic MAC addresses. ● Check whether global MAC address change notification is enabled globally. ● Display the history of MAC address change notifications.
Device A	Hostname# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 0 Hostname# show mac-address-table notification interface GigabitEthernet 0/2 Interface MAC Added Trap MAC Removed Trap ---------- ---------- ---------- GigabitEthernet 0/2 Enabled Enabled Hostname# show mac-address-table interface GigabitEthernet 0/2 Vlan MAC Address Type Interface ---------- ---------- -------- ---------- 1 00d0.3232.0001 DYNAMIC GigabitEthernet 0/2 Hostname# show mac-address-table notification MAC Notification Feature : Enabled Interval(Sec): 300 Maximum History Size : 50 Current History Size : 1 Hostname# show mac-address-table notification history History Index : 0 Entry Timestamp: 221683 MAC Changed Message : Operation:DEL Vlan:1 MAC Addr: 00d0.3232.0003 GigabitEthernet 0/2

Common Errors

None

1.5 Monitoring

Clearing

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

Command	Description

clear mac-address-table dynamic [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]	Clears dynamic MAC addresses.

Displaying

Command	Description
show mac-address-table { **dynamic** | **static** | **filter** } [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]	Displays the MAC address table.
show mac-address-learning	Displays MAC address learning on an interface.
show mac-address-table count [**interface** *interface-id* | **vlan** *vlan-id*]	Displays the number of address entries in the address table.
show mac-address-table aging-time	Displays the aging time for dynamic MAC addresses.
show mac-address-table notification [**interface** [*interface-id*] | **history**]	Displays the configuration and history of MAC address change notifications.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug bridge mac	Debugs MAC address operation.

1 Configuring VLAN

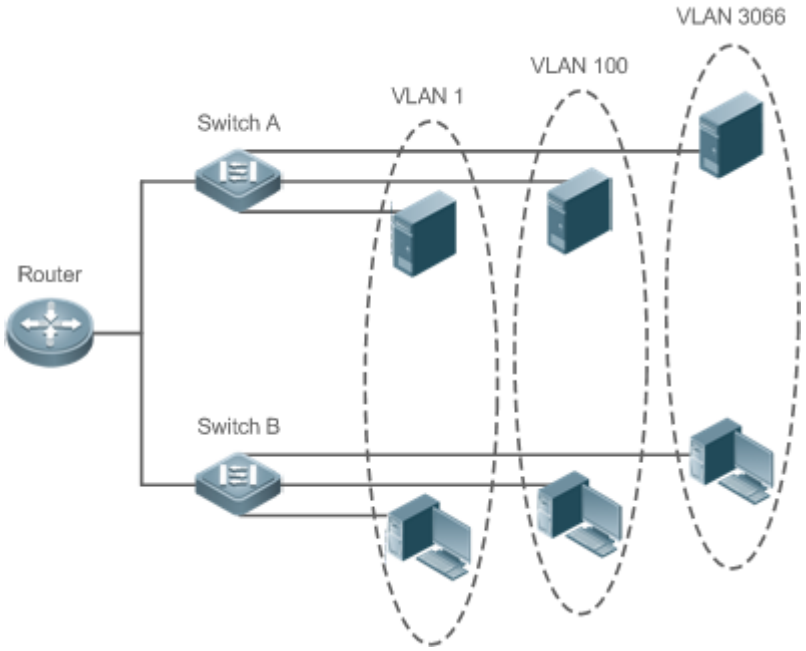
1.1 Overview

A Virtual Local Area Network (VLAN) is a logical network created based on a physical network. A VLAN can be categorized into Layer 2 networks of the OSI model.

A VLAN has the same attributes as a common LAN, except for limitation on the physical location. Layer 2 unicast, broadcast, and multicast frames are forwarded and transmitted within a VLAN.

An interface can be defined as a member of a VLAN, and all terminals connected to this interface are parts of a virtual network that supports multiple VLANs. You do not need to adjust the network physically when adding, removing, and modifying users. Communication among VLANs is realized through Layer 3 devices, as shown in the following figure.

Figure 1-1



Protocols and Standards

- IEEE 802.1Q

1.2 Applications

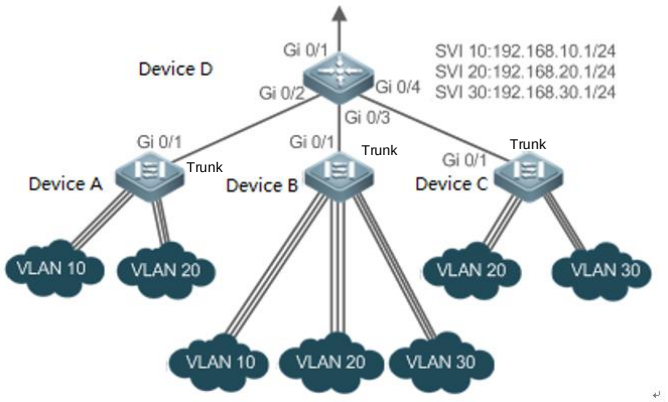
Application	Description
Layer 2 Isolation and Layer 3 Interconnection Between VLANs	A user intranet is divided into multiple VLANs to realize Layer 2 isolation. These VLANs realize subnet interconnection based on the IP forwarding capability of the Layer 3 core switch.

1.2.1 Layer 2 Isolation and Layer 3 Interconnection Between VLANs

Scenario

The LAN of a user needs to be divided into VLAN 10, VLAN 20, and VLAN 30 to realize Layer 2 isolation. The three VLANs correspond to subnets 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24, respectively, and these VLANs implement subnet interconnection based on the IP forwarding capability of the Layer 3 core switch.

Figure 1-2



Remarks	Device A, Device B, and Device C are access switches. On the Layer 3 core switch Device D, configure the three VLANs, configure the interfaces for connecting the access switches as trunk interfaces, and specify an allowed VLAN list to realize Layer 2 isolation. Create the VLANs separately on the three access switches, assign an access interface for each VLAN, and configure the interfaces for connecting the core switch as trunk interfaces. Configure three SVIs on Device D as the gateway interfaces of the IP subnets corresponding to the three VLANs. Configure IP addresses for these SVIs.

Deployment

- Divide the LAN into multiple VLANs to realize Layer 2 isolation.
- Configure the SVIs on the Layer 3 switch for Layer 3 communication between VLANs.

1.3 Features

Basic Concepts

VLAN

A VLAN is a logical network created based on a physical network. A VLAN has the same attributes as a common LAN, except for limitation on the physical location. Layer 2 unicast, broadcast, and multicast frames are forwarded and transmitted within a VLAN.

The VLANs supported by Ruijie products comply with IEEE 802.1Q. A maximum of 4094 VLANs 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 failures.

Interface Mode

You can determine the frames allowed on an interface and the VLANs which the interface belongs to by configuring the interface mode.

Interface Mode	Description
Access interface	An access interface belongs to only one VLAN, which is specified manually.
Trunk interface (802.1Q)	A trunk interface belongs to all the VLANs of an access switch by default, and can forward the frames of all the VLANs or the frames of allowed VLANs.
Uplink interface	An uplink interface belongs to all the VLANs of an access switch by default, and can forward the frames of all the VLANs and frames from the native VLAN in tagged mode.
Hybrid interface	A hybrid interface belongs to all the VLANs of an access switch by default, and can forward frames of all the VLANs and send frames of VLANs in untagged mode. It can also transmit frames of allowed VLANs.

Overview

Feature	Description
VLAN	VLAN helps realize Layer 2 isolation.

1.3.1 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.

Layer 2 isolation: If no SVIs are configured for VLANs, VLANs are isolated at Layer 2. That is, users in the VLANs cannot communicate with each other.

Layer 3 interconnection: If SVIs are configured on a Layer 3 switch for VLANs, these VLANs can communicate with each other at Layer 3.

1.4 Configuration

Configuration	Description and Command	
Configuring a VLAN	(Mandatory) It is used to create a VLAN.	
	vlan	Enters a VLAN ID.
	Optional.	
	interface vlan	Creates a Layer 3 virtual interface for a VLAN.
	(Optional) It is used to rename a VLAN.	
	name	Names a VLAN.

Configuration	Description and Command	
Configuring an Access Interface	(Optional) It is used to configure an access interface to transmit flows from a single VLAN.	
	switchport mode access	Defines an interface as a Layer 2 access interface.
	switchport access vlan	Assigns an interface to a VLAN.
	add interface	Adds one access interface or a group of such interface s to the VLAN.
Configuring a Trunk Port	(Mandatory) It is used to configure the interface as a trunk interface.	
	switchport mode trunk	Defines an interface as a Layer 2 trunk interface.
	(Optional) It is used to configure trunk interfaces to transmit flows from multiple VLANs.	
	switchport trunk allowed vlan	Configures allowed VLANs for a trunk interface.
	switchport trunk native vlan	Specifies a native VLAN for a trunk interface.
Configuring an Uplink Interface	(Mandatory) It is used to configure the interface as an uplink interface.	
	switchport mode uplink	Configures an interface as an uplink interface.
	(Optional) It is used to restore the interface mode.	
	no switchport mode	Restores the interface mode.
	switchport trunk allowed vlan	Configures an allowed VLAN list for an uplink interface.
	switchport trunk native vlan	Configures a native VLAN for an uplink interface.
Configuring a Hybrid Interface	(Mandatory) It is used to configure an interface as a hybrid interface.	
	switchport mode hybrid	Configures an interface as a hybrid interface.
	(Optional) It is used to transmit frames of multiple VLANs in untagged mode.	
	no switchport mode	Restores the interface mode.
	switchport hybrid allowed vlan	Configures allowed VLANs for a hybrid interface.
	switchport hybrid native vlan	Configures a default VLAN for a hybrid interface.

1.4.1 Configuring a 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 Step

Creating and Modifying a VLAN

- Mandatory.
- In case of insufficient hardware resources, the system returns information on VLAN creation failures.
- Use the **vlan** *vlan-id* command to create a VLAN or enter the VLAN configuration mode.

Command	**vlan** { *vlan-id* | **range** *vlan-range* }
Parameter Description	*vlan-id*: Indicates the VLAN ID. The value range is from 1 to 4094.
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 can use the **no vlan** *vlan-id* command to delete a VLAN. VLAN 1, VLANs where SVIs are configured, and sub-VLANs cannot be deleted.

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 VLAN 4 is VLAN 0004.
Command Mode	VLAN configuration mode
Usage Guide	To restore the default VLAN name, use the **no name** command.

Configuring an SVI

- Optional.
- Create a Layer 3 SVI for a VLAN, enter the SVI configuration mode, and assign an IP address to the SVI so that devices in the VLAN can communicate at Layer 3.

Command	**interface vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates the VLAN ID.
Defaults	No SVI exists in a VLAN by default.
Command Mode	Global 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 description** command to check the created SVI.
- Run the **show interface vlan** *vlan-id* command to check detailed SVI 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 SVI

Configuration Steps	• Create an SVI for VLAN 1 and assign an IP address to the SVI.

	`Hostname# configure terminal`
	`Hostname(config)# interface vlan 1`
	`Hostname(config-if-VLAN 1)# ip address 10.10.29.1/24`
	`Hostname(config-if-VLAN 1)# end`

Verification	• Run the **show interface description** command to check the created SVI.

	`Hostname#show interface description`
	`Interface Status Administrative`
	`Description`
	`---------- -------- --------------`
	`VLAN 1 up up`

	• Run the **show interface vlan** *vlan-id* command to check detailed SVI configuration.

	`Hostname# show interface vlan 1`
	`Index(dec):4097 (hex):1001`
	`VLAN 1 is UP , line protocol is UP`
	`Hardware is VLAN, address is 00d0.f822.3719 (bia 00d0.f822.3719)`
	`Interface address is: 10.10.29.1/24`
	`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

1.4.2 Configuring an Access Interface

Configuration Effect

Configure a Layer 2 interface as an access interface and add it to a VLAN.

Configuration Step

Assigning an Access Interface to a Specified VLAN

- Optional.
- Use the **switchport mode access** command in interface configuration mode to specify Layer 2 interfaces (switch interfaces) as access interfaces.
- Use the **switchport access vlan** *vlan-id* command in interface configuration mode to add an access interface to a specified VLAN.

Command	**switchport mode access**
Parameter Description	N/A
Defaults	A switch interface is an access interface by default.
Command Mode	Interface configuration mode
Usage Guide	N/A

Command	**switchport access vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates a VLAN ID.
Defaults	An access interface is added to VLAN 1 by default.
Command Mode	Interface configuration mode
Usage Guide	This command is valid for only the access interface. If an interface is assigned to a nonexistent VLAN, this VLAN will be automatically created. The **no switchport access vlan** command can be used to restore the access interface to VLAN 1.

Adding an Access Interface to a VLAN

- Optional.
- This command is executed in VLAN configuration mode and takes effect only on an access interface. After an access interface is added to a VLAN, traffic of the VLAN can be transmitted through the interface.

Command	**add interface** { *interface-type interface-number* | **range** *interface-type interface-range* }
Parameter Description	*interface-type interface-number*: Indicates a single interface. *interface-type interface-range*: Indicates multiple interface s.

Defaults	By default, all Layer 2 Ethernet interface s belong to VLAN 1.
Command Mode	VLAN configuration mode
Usage Guide	In VLAN configuration mode, add a specific access interface to a VLAN. This command is valid for only the access interface. This command has the same effect as the **switchport access vlan** *vlan-id* command. The **no add interface** { *interface-type interface-number* | **range** *interface-type interface-range* } command can be used to add the access interface specified in a VLAN (except VLAN 1) to VLAN 1.

For the two commands of adding an interface to a VLAN, the command configured later will overwrite the other one.

Verification

- Send untagged packets to an access interface. The packets are broadcast within the VLAN.
- Use **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id*: Indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A

Command Display	`Hostname(config-vlan)#show vlan id 20`
	`VLAN Name Status Ports`
	`---- -------------------------------- --------- ----------`
	`20 VLAN0020 STATIC Gi0/1`

Configuration Example

Adding an Access Interface to a VLAN

Configuration Steps	• Add an access interface to the VLAN. There are two approaches.

	`Hostname# configure terminal`
	`Hostname(config)# interface gigabitethernet 0/3`
	`Hostname(config-if-GigabitEthernet 0/3)# switchport`
	`Hostname(config-if-GigabitEthernet 0/3)# switchport mode access`
	`Hostname(config-if-GigabitEthernet 0/3)# switchport access vlan 20`
	• Add GigabitEthernet 0/3 to VLAN 20.
	`Hostname# configure terminal`
	`SwitchA(config)#vlan 20`
	`SwitchA(config-vlan)#add interface gigabitethernet 0/3`

Verification	• Run the **show vlan** and **show interface switchport** commands to check whether the configuration takes effect.
	`Hostname(config-vlan)#show vlan` `VLAN Name Status Ports`

```
---- -------------------------------- ---------
-----------------------------------
   1 VLAN0001                         STATIC
  20 VLAN0020                         STATIC    Gi0/3

Hostname# show interface GigabitEthernet 0/3 switchport
Interface                        Switchport Mode      Access Native
Protected VLAN lists
-------------------------------- ---------- --------- ------ ------
--------- --------------
GigabitEthernet 0/3              enabled    ACCESS    20     1
Disabled  ALL
```

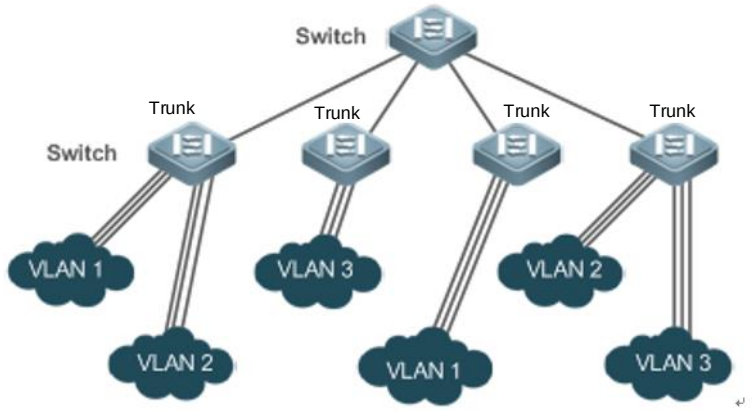
1.4.3 Configuring a Trunk Port

Configuration Effect

A trunk is a point-to-point link connecting one or more Ethernet interfaces to other network devices and can transmit traffic from multiple VLANs.

The trunk of Ruijie devices conforms to 802.1Q. The following figure displays a network adopting trunk connections.

Figure 1-3



You may configure an Ethernet interface or aggregate interface (See *Configuring Aggregate Interface*) as a trunk interface.

You should specify a native VLAN for a trunk interface. The untagged packets received by and sent from the trunk interface are considered to belong to the native VLAN. The default VLAN ID (PVID in IEEE 802.1Q) of this trunk interface is the native VLAN ID. Frames of the native VLAN sent through the trunk are untagged. The default native VLAN of a trunk interface is VLAN 1.

When configuring a trunk, make sure that the trunk interfaces at the two ends of the link adopt the same native VLAN.

Configuration Step

↘ **Configuring a Trunk Interface**

- Mandatory.
- Configure a trunk interface to transmit traffic from multiple VLANs.

Command	**switchport mode trunk**
Parameter Description	N/A
Defaults	The default mode is access, which can be modified to trunk.
Command Mode	Interface configuration mode
Usage Guide	To restore all properties of a trunk interface to default settings, use the **no switchport mode** command.

Defining Allowed VLANs for a Trunk Interface

- Optional.
- By default, a trunk interface transmits traffic from all the VLANs (VLANs 1 to 4094). You may configure a list of allowed VLANs to prohibit traffic of some VLANs from passing through a trunk interface.

Command	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Parameter Description	*vlan-list*: Indicates a VLAN or a list of VLANs. VLAN IDs are connected by the hyphen (-) in order. For example: 10–20. **all**: Indicates allowed VLANs, including all VLANs. **add**: Indicates that a specific VLAN is added to the list of allowed VLANs. **remove**: Indicates that a specific VLAN is removed from the list of allowed VLANs. **except**: Indicates that all VLANs except those in the listed VLAN are added to the list of allowed VLANs. **only**: Indicates that listed VLANs are added to the list of allowed VLANs, and that other VLANs are removed from the list.
Defaults	The trunk interface and the uplink interface belong to all VLANs.
Command Mode	Interface configuration mode
Usage Guide	To restore the default allowed VLAN list of a trunk interface, use the **no switchport trunk allowed vlan** command.

Configuring a Native VLAN

- Optional.
- A trunk interface receives and sends tagged or untagged 802.1Q frames. Traffic from the native VLAN are forwarded in untagged mode. The default native VLAN is VLAN 1.
- If a frame carries the VLAN ID of a native VLAN, its tag will be stripped automatically when it passes a trunk interface.

Command	**switchport trunk native vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates a VLAN ID.
Defaults	The default VALN for a trunk or uplink interface is VLAN 1.
Command	Interface configuration mode

Mode	
Usage Guide	To restore the default native VLAN of a trunk interface, use the **no switchport trunk native vlan** command.

When you set the native VLAN of an interface to a nonexistent VLAN, this VLAN will not be created automatically. Besides, the native VLAN can be out of the list of allowed VLANs for this interface. In this case, traffic from the native VLAN cannot pass through the interface.

Verification

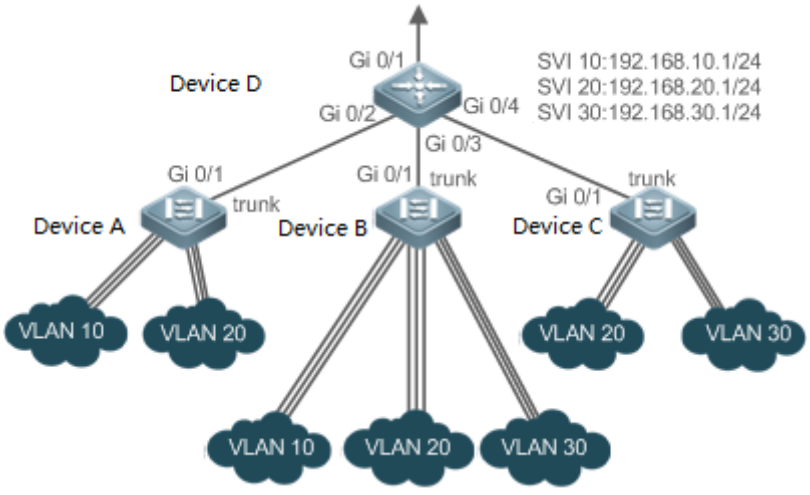
- Send tagged packets to a trunk interface. Packets are broadcast within the specified VLANs.
- Use **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id*: Indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A

Command Display	`Hostname(config-vlan)#show vlan id 20`
	`VLAN Name Status Ports`
	`---- -------------------------------- ---------`
	`----------`
	`20 VLAN0020 STATIC Gi0/1`

Configuration Example

Configuring Basic VLANs for Layer 2 Isolation and Layer 3 Interconnection

Scenario Figure 1-4	
Configuration Steps	Networking requirements: The LAN of a user is divided into VLAN 10, VLAN 20, and VLAN 30 to realize Layer 2 isolation. The three VLANs correspond to the IP subnets 192.168.10.0/24, 192.168.20.0/24, and 192.168.30.0/24, respectively, and these VLANs implement subnet interconnection based on the IP forwarding capability of the Layer 3 core switch. This example uses the core switch and one access switch to describe the configuration process.

	Configuration key points: ● On the Layer 3 core switch, configure the three VLANs, configure the interfaces for connecting the access switches as trunk interfaces, and specify an allowed VLAN list to realize Layer 2 isolation. ● Configure three SVIs on the core switch as the gateway interfaces of the IP subnets corresponding to the three VLANs. Configure IP addresses for these SVIs. ● Create the VLANs separately on the three access switches, assign an access interface to each VLAN, and configure the interfaces for connecting the core switch as trunk interfaces. In this example, Device A (an access switch) is used.
Device D	DeviceD#configure terminal DeviceD(config)#vlan 10 DeviceD(config-vlan)#vlan 20 DeviceD(config-vlan)#vlan 30 DeviceD(config-vlan)#exit DeviceD(config)#interface range GigabitEthernet 0/2-4 DeviceD(config-if-range)#switchport mode trunk DeviceD(config-if-range)#exit DeviceD(config)#interface GigabitEthernet 0/2 DeviceD(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan remove 1-4094 DeviceD(config-if-GigabitEthernet 0/2)#switchport trunk allowed vlan add 10,20 DeviceD(config-if-GigabitEthernet 0/2)#interface GigabitEthernet 0/3 DeviceD(config-if-GigabitEthernet 0/3)#switchport trunk allowed vlan remove 1-4094 DeviceD(config-if-GigabitEthernet 0/3)#switchport trunk allowed vlan add 10,20,30 DeviceD(config-if-GigabitEthernet 0/3)#interface GigabitEthernet 0/4 DeviceD(config-if-GigabitEthernet 0/4)#switchport trunk allowed vlan remove 1-4094 DeviceD(config-if-GigabitEthernet 0/4)#switchport trunk allowed vlan add 20,30 DeviceD#configure terminal DeviceD(config)#interface vlan 10 DeviceD(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0 DeviceD(config-if-VLAN 10)#interface vlan 20 DeviceD(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0 DeviceD(config-if-VLAN 20)#interface vlan 30 DeviceD(config-if-VLAN 30)#ip address 192.168.30.1 255.255.255.0 DeviceD(config-if-VLAN 30)#exit
Device A	DeviceA#configure terminal DeviceA(config)#vlan 10 DeviceA(config-vlan)#vlan 20 DeviceA(config-vlan)#exit

```
DeviceA(config)#interface range GigabitEthernet 0/2-12
DeviceA(config-if-range)#switchport mode access
DeviceA(config-if-range)#switchport access vlan 10
DeviceA(config-if-range)#interface range GigabitEthernet 0/13-24
DeviceA(config-if-range)#switchport mode access
DeviceA(config-if-range)#switchport access vlan 20
DeviceA(config-if-range)#exit
DeviceA(config)#interface GigabitEthernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)#switchport mode trunk
```

Verification

Check VLAN configuration on the core switch.

- Check VLAN information, including VLAN IDs, names, statuses, and interfaces included in the VLANs.
- Check the VLAN status on Gi 0/2, Gi 0/3, and Gi 0/4.

Device D

```
DeviceD#show vlan
VLAN  Name       Status                Ports
---- --------  --------   --------------------------------
   1 VLAN0001   STATIC     Gi0/1, Gi0/5, Gi0/6, Gi0/7
                           Gi0/8, Gi0/9, Gi0/10, Gi0/11
                           Gi0/12, Gi0/13, Gi0/14, Gi0/15
                           Gi0/16, Gi0/17, Gi0/18, Gi0/19
                           Gi0/20, Gi0/21, Gi0/22, Gi0/23
                           Gi0/24
  10 VLAN0010  STATIC      Gi0/2, Gi0/3
  20 VLAN0020  STATIC      Gi0/2, Gi0/3, Gi0/4
  30 VLAN0030  STATIC      Gi0/3, Gi0/4
DeviceD#show interface GigabitEthernet 0/2 switchport
Interface                        Switchport Mode      Access Native
Protected VLAN lists
-------------------------------- ---------- --------- ------ ------
--------- --------------
GigabitEthernet 0/2              enabled    TRUNK     1      1
Disabled  10,20
DeviceD#show interface GigabitEthernet 0/3 switchport
Interface                        Switchport Mode      Access Native
Protected VLAN lists
-------------------------------- ---------- --------- ------ ------
--------- --------------
GigabitEthernet 0/3              enabled    TRUNK     1      1
Disabled  10,20,30
DeviceD#show interface GigabitEthernet 0/4 switchport
Interface                        Switchport Mode      Access Native
Protected VLAN lists
-------------------------------- ---------- --------- ------ ------
--------- --------------
```

	GigabitEthernet 0/4 enabled TRUNK 1 1 Disabled 20,30

Common Errors

- N/A

1.4.4 Configuring an Uplink Interface

Configuration Effect

- An uplink interface is similar to a trunk interface. Their difference is that an uplink interface only transmits tagged frames while a trunk interface sends untagged frames of the native VLAN.

Configuration Step

Configuring an Uplink Interface

- Mandatory.
- Configure an uplink interface to transmit traffic from multiple VLANs. Only tagged frames can be transmitted.

Command	**switchport mode uplink**
Parameter Description	N/A
Defaults	The default mode is access, which can be modified to uplink.
Command Mode	Interface configuration mode
Usage Guide	To restore all default properties of an uplink interface, use the **no switchport mode** command.

Defining Allowed VLANs for a Trunk Interface

- Optional.
- You may configure a list of allowed VLANs to prohibit traffic of some VLANs from passing through an uplink interface.

Command	**switchport trunk allowed vlan** { **all** | [**add** | **remove** | **except** | **only**] } *vlan-list*
Parameter Description	*vlan-list*: Indicates a VLAN or a list of VLANs. VLAN IDs are connected by the hyphen (-) in order. For example: 10–20. **all**: Indicates allowed VLANs, including all VLANs. **add**: Indicates that a specific VLAN is added to the list of allowed VLANs. **remove**: Indicates that a specific VLAN is removed from the list of allowed VLANs. **except**: Indicates that all VLANs except those in the listed VLAN are added to the list of allowed VLANs. **only**: Indicates that listed VLANs are added to the list of allowed VLANs, and that other VLANs are removed from the list.
Command Mode	Interface configuration mode
Usage Guide	To restore default allowed VLANs, use the **no switchport trunk allowed vlan** command.

Configuring a Native VLAN

- Optional.
- If a frame carries the VLAN ID of a native VLAN, its tag will not be stripped when it passes an uplink interface. This is contrary to a trunk interface.

Command	**switchport trunk native vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates a VLAN ID.
Command Mode	Interface configuration mode
Usage Guide	To restore the default native VLAN of an uplink interface, use the **no switchport trunk native vlan** command.

Verification

- Send tagged packets to an uplink interface. Packets are broadcast within the specified VLANs.
- Use **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id*: Indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A

Command Display	`Hostname(config-vlan)#show vlan id 20`
	`VLAN Name Status Ports`
	`---- -------------------------------- ---------`
	`-----------------------------------`
	`20 VLAN0020 STATIC Gi0/1`

Configuration Example

Configuring an Uplink Interface

Configuration Steps	● The following is an example of configuring Gi0/1 as an uplink interface.

	`Hostname# configure terminal`
	`Hostname(config)# interface gi 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# switchport mode uplink`
	`Hostname(config-if-GigabitEthernet 0/1)# end`

Verification	● Check whether the configuration is correct.

	`Hostname# show interfaces GigabitEthernet 0/1 switchport`
	`Interface Switchport Mode Access Native`
	`Protected VLAN lists`
	`-------------------------------- ---------- --------- ------ ------`
	`--------- -----------------`

	GigabitEthernet 0/1 enabled **UPLINK** 1 1 disabled ALL

1.4.5 Configuring a Hybrid Interface

Configuration Effect

- A hybrid interface is usually used in the shared VLAN environment. By default, a hybrid interface is the same as a trunk interface. Their difference is that a hybrid interface can send frames from the VLANs except the default VLAN in untagged mode.

Configuration Step

Configuring a Hybrid Interface

- Mandatory.
- Configure a hybrid interface to transmit traffic from multiple VLANs.

Command	**switchport mode hybrid**
Parameter Description	N/A
Defaults	The default mode is access, which can be modified to hybrid.
Command Mode	Interface configuration mode
Usage Guide	To restore all default properties of a hybrid interface, use the **no switchport mode** command.

Defining Allowed VLANs for a Hybrid Interface

- Optional.
- By default, a hybrid interface transmits traffic from all the VLANs (VLANs 1 to 4094). You can configure a list of allowed VLANs to prohibit traffic of some VLANs from passing through a hybrid interface.

Command	**switchport hybrid allowed vlan** [[**add** | **only**] **tagged** | [**add**] **untaged** | **remove**] *vlan_list*
Parameter Description	*vlan-id*: Indicates a VLAN ID.
Defaults	By default, a hybrid interface belongs to all VLANs. The interface is added to the default VLAN in untagged mode and to the other VLANs in tagged mode.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring a Native VLAN

- Optional.
- If a frame carries the VLAN ID of a native VLAN, its tag will be stripped automatically when it passes a hybrid interface.

Command	**switchport hybrid native vlan** *vlan_id*
Parameter	*vlan-id*: Indicates a VLAN ID.

Description	
Defaults	The default native VLAN is VLAN 1.
Command Mode	Interface configuration mode
Usage Guide	To restore the default native VLAN of a hybrid interface, use the **no switchport hybrid native vlan** command.

Verification

- Send tagged packets to a hybrid interface. Packets are broadcast within the specified VLANs.
- Use **show vlan** and **show interface switchport** to check whether the configuration takes effect.

Command	**show vlan** [**id** *vlan-id*]
Parameter Description	*vlan-id*: Indicates a VLAN ID.
Command Mode	Any mode
Usage Guide	N/A

Command Display	`Hostname(config-vlan)#show vlan id 20`
	`VLAN Name Status Ports`
	`---- -------------------------------- ---------`
	`----------------------------------`
	`20 VLAN0020 STATIC Gi0/1`

Configuration Example

Configuring a Hybrid Interface

Configuration Steps	The following is an example of configuring Gi0/1 as a hybrid interface.

	`Hostname# configure terminal`
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# switchport mode hybrid`
	`Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid native vlan 3`
	`Hostname(config-if-GigabitEthernet 0/1)# switchport hybrid allowed vlan untagged 20-30`
	`Hostname(config-if-GigabitEthernet 0/1)# end`

Verification	Check whether the configuration is correct.

	`Hostname(config-if-GigabitEthernet 0/1)#show run interface gigabitEthernet 0/1`
	
	`Building configuration...`
	`Current configuration : 166 bytes`
	
	`interface GigabitEthernet 0/1`
	` switchport`
	`switchport mode hybrid`

```
switchport hybrid native vlan 3
switchport hybrid allowed vlan add untagged 20-30
```

1.5 Monitoring

Displaying

Command	Description
show vlan [**id** *vlan-id*]	Displays the VLAN configuration.
show interface [*interface-type interface-number*] **switchport**	Displays configuration of switch interfaces.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug bridge vlan	Debugs VLANs.

1 Configuring MAC VLAN

1.1 Overview

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

Protocols

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

1.2 Applications

Application	Description
Configuring a MAC VLAN	The MAC VLAN function is used to assign VLANs based on users' MAC addresses. When the physical location of a user device changes, for example, switching from one switch to another, you do not need to reconfigure the VLAN of the interface connected to the user device.

1.2.1 Configuring a MAC VLAN

Scenario

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

With the MAC VLAN function configured, when the physical location of a user device changes, for example, switching from one switch to another, you do not need to reconfigure the VLAN of the interface connected to the user device.

Deployment

- Push MAC VLAN entries on a Layer 2 switch or wireless device to assign VLANs based on users' MAC addresses.

1.3 Overview

Feature

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

1.3.1 Configuring MAC VLAN

Working Principle

When a switch receives a packet, the switch compares the source MAC address of the packet with the MAC address specified in a MAC VLAN entry. If they match, the switch forwards the packet to the VLAN specified in the MAC VLAN entry. If they do not match, the VLAN to which the packet belongs is still determined by the VLAN assignment rule of the interface.

To ensure that a PC is assigned to a specified VLAN regardless of the switch connected to the PC, you can perform the configuration by using an authentication server (dynamic VLAN assignment of 802.1X): After a user passes authentication, a switch dynamically creates an association between the MAC address and a VLAN based on the information provided by the authentication server. When the user goes offline, the switch automatically deletes the association. This approach requires that the MAC-VLAN association be configured on the authentication server. For details about dynamic VLAN assignment of 802.1X, see *Configuring 802.1X*.

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

- MAC VLAN entries are effective only for untagged packets, but ineffective for tagged packets.
- For MAC VLAN entries dynamically generated, the specified VLANs must exist.
- VLANs specified in MAC VLAN entries cannot be super-VLANs (but can be sub-VLANs), remote VLANs, or primary VLANs (but can be secondary VLANs).
- MAC addresses specified in MAC VLAN entries must be unicast addresses.

1.4 Monitoring

Displaying

Command	Description
show mac-vlan all	Displays all the MAC VLAN entries.
show mac-vlan vlan *vlan-id*	Displays MAC VLAN entries of a specified VLAN.
show mac-vlan mac-address *mac-address*	Displays MAC VLAN entries of a specified MAC address.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug bridge mvlan	Debugs the MAC VLAN function.

1 Configuring Super-VLAN

1.1 Overview

The super-VLAN is used to allocate Virtual Local Area Networks (VLANs). Super-VLAN, also called VLAN aggregation, is a management technology tailored for IP address optimization.

Using super-VLAN can greatly save IP addresses. Only one IP address needs to be assigned to the super-VLAN that consists of multiple sub-VLANs, which greatly saves IP addresses and facilitates network management.

1.2 Application

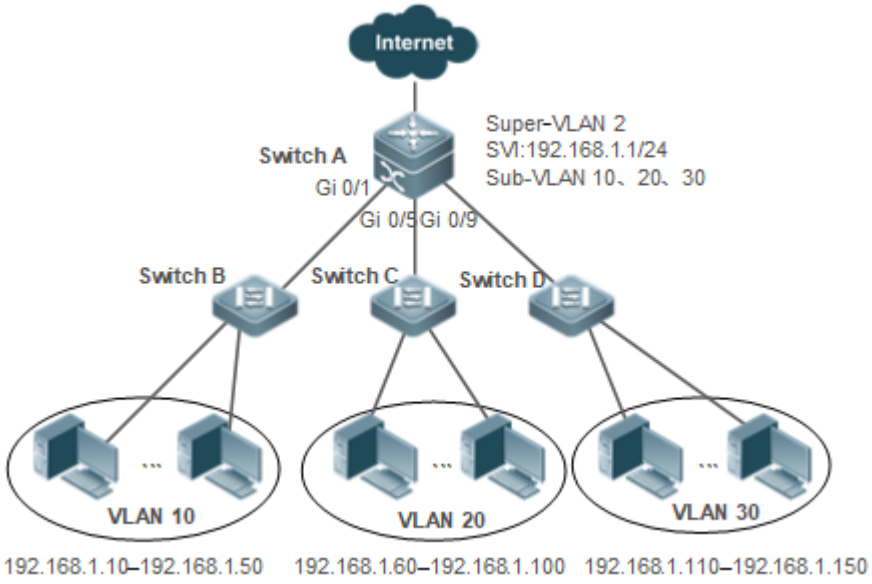
Application	Description
Sharing One IP Gateway Among Multiple VLANs	VLANs are assigned to implement Layer 2 isolation of access users. All VLAN users share one IP gateway to implement Layer 3 communication and communication with external networks.

1.2.1 Sharing One IP Gateway Among Multiple VLANs

Scenario

Multiple VLANs are isolated at Layer 2 on a Layer 3 device, but users of these VLANs can perform Layer 3 communication with each other in the same network segment.

Figure 1-1



Remarks	Switch A functions as the gateway or core switch. Switch B, Switch C, and Switch D function as access switches. On Switch A, configure a super-VLAN and sub-VLANs, and configure a Layer 3 interface for the

	super-VLAN and an IP address for the Layer 3 interface. On Switch B, Switch C, and Switch D, configure VLAN 10, VLAN 20, and VLAN 30, respectively, and allocate these VLANs to different departments of the company.

Deployment

On the intranet, use the super-VLAN so that multiple sub-VLANs can share one IP gateway and VLANs are mutually isolated at Layer 2.

Users in sub-VLANs can perform Layer 3 communication through the gateway of the super-VLAN.

1.3 Features

Basic Concepts

Super-VLAN

Super-VLAN, also called VLAN aggregation, is a management technology tailored for IP address optimization. It aggregates multiple VLANs to one IP network segment. No physical port can be added to a super-VLAN. The switch virtual interface (SVI) is used to manage the cross-VLAN communication of sub-VLANs. The super-VLAN cannot be used as a common 802.1Q VLAN, and is considered as the primary VLAN of sub-VLANs.

Sub-VLAN

A sub-VLAN is an independent broadcast domain. Sub-VLANs are isolated at Layer 2. Users of sub-VLANs of the same or different super-VLANs communicate with each other through Layer 3 SVIs of their own super-VLANs.

Proxy ARP

A Layer 3 SVI can be created only for a super-VLAN. Users in a sub-VLAN communicate with users in other sub-VLANs of the same super-VLAN or users in other network segments through proxy ARP and the Layer 3 SVI of the super-VLAN. When a user of a sub-VLAN sends an ARP Request packet to a user of another sub-VLAN, the gateway of the super-VLAN uses its own MAC address to send or respond to the ARP Request packet. The process is called proxy ARP.

IP Address Range of a Sub-VLAN

Based on the gateway IP address configured for the super-VLAN, an IP address range can be configured for each sub-VLAN.

Overview

Feature	Description
Super-VLAN	Create a Layer 3 interface as an SVI to allow all sub-VLANs to share the same IP network segment through proxy ARP.

1.3.1 Super-VLAN

Users of all sub-VLANs of a super-VLAN can be allocated IP addresses in the same IP address range, and share the same IP gateway. Users can implement cross-VLAN communication through this gateway. In this case, there is no need to allocate a gateway for each VLAN, which saves IP addresses.

Working Principle

IP addresses in a network segment are allocated to different sub-VLANs that belong to the same super-VLAN. Each sub-VLAN has an independent broadcast domain of the VLAN, and different sub-VLANs are isolated from each other at Layer 2. When users in sub-VLANs need to perform Layer 3 communication, the IP address of the SVI of the super-VLAN is used as the gateway address. In this way, multiple VLANs share the same IP gateway, without configuring a gateway for each VLAN. In addition, to implement Layer 3 communication between sub-VLANs and between sub-VLANs and other network segments, proxy ARP is used to forward and process ARP Request and Reply packets.

Layer 2 communication of sub-VLANs: If the SVI is not configured for the super-VLAN, sub-VLANs of the super-VLAN are isolated at Layer 2. That is, users in different sub-VLANs cannot communicate with each other. If the SVI is configured for the super-VLAN and the gateway of the super-VLAN can function as the ARP proxy, users in different sub-VLANs of the same super-VLAN can communicate with each other. This is because IP addresses of users in different sub-VLANs belong to the same network segment, and communication between these users is Layer 2 communication.

Layer 3 communication of sub-VLANs: If users in sub-VLANs of a super-VLAN need to perform Layer 3 communication across network segments, the gateway of this super-VLAN functions as the ARP proxy to respond to ARP Request packets in place of sub-VLANs.

1.4 Configuration

Configuration Item	Description and Command	
Configuring Basic Functions of the	Mandatory.	
	supervlan	Configures a super-VLAN.
	subvlan	Configures a sub-VLAN.
	proxy-arp	Enables the proxy ARP function.
	interface vlan	Creates a virtual interface for a super-VLAN.
	ip address	Configures the IP address of the virtual interface of a super-VLAN.
	Optional.	
	subvlan-address-range	Specifies the IP address range in a sub-VLAN.

1.4.1 Configuring Basic Functions of the Super-VLAN

Configuration Effect

Enable the super-VLAN function and configure an SVI for the super-VLAN to implement Layer 2 or Layer 3 communication between sub-VLANs across VLANs.

Users in all sub-VLANs of a super-VLAN share the same IP gateway. There is no need to specify a network segment for each VLAN, which saves IP addresses.

Notes

A super-VLAN does not belong to any physical interface. Therefore, the device configured with the super-VLAN cannot process packets tagged with the super-VLAN ID.

Both the super-VLAN function and the proxy ARP function of each sub-VLAN must be enabled.

An SVI and an IP address must be configured for a super-VLAN. The SVI is a virtual interface used for communication of users in all sub-VLANs.

Configuration Step

Configuring a Super-VLAN

- Mandatory.
- No physical interface exists in a super-VLAN.
- The proxy ARP function must be enabled. This function is enabled by default.
- Run the **supervlan** command to change a common VLAN into a super-VLAN.
- A super-VLAN cannot contain any physical interface. Therefore, after a common VLAN is changed into a super-VLAN, all interfaces in the VLAN exit the VLAN.

A super-VLAN is valid only after you configure sub-VLANs for this super-VLAN.

VLAN 1 cannot be configured as a super-VLAN.

A super-VLAN cannot be configured as a sub-VLAN of another super-VLAN. A sub-VLAN of a super-VLAN cannot be configured as a super-VLAN.

Command	**supervlan**
Parameter Description	N/A
Defaults	N/A
Command Mode	VLAN configuration mode
Usage Guide	By default, the super-VLAN function is disabled. No physical interface can be added to a super-VLAN. Once a VLAN is not a super-VLAN, all its sub-VLANs become common static VLANs.

Configuring a Sub-VLAN

- Mandatory.
- Physical interfaces can be added to sub-VLANs. Sub-VLANs of a super-VLAN share the gateway address of the super-VLAN and reside in the same network segment.
- The proxy ARP function must be enabled. This function is enabled by default.
- Run the **subvlan** *vlan-id-list* command to change common VLANs into sub-VLANs of a super-VLAN. These sub-VLANs can contain physical interfaces.
- The super-VLAN manages user communication in the sub-VLANs.

You must change a sub-VLAN into a common VLAN before you can delete this sub-VLAN by running the **no vlan** command.

One sub-VLAN belongs to only one super-VLAN.

Command	**subvlan** *vlan-id-list*
Parameter Description	*vlan-id-list*: Specifies multiple VLANs as sub-VLANs of a super-VLAN.
Defaults	All VLANs are common VLANs by default.
Command Mode	VLAN configuration mode
Usage Guide	Interfaces connected to user devices can be added to a sub-VLAN. You must change a sub-VLAN into a common VLAN before you can delete this sub-VLAN by running the **no vlan** [*id*] command. You cannot configure a Layer 3 SVI of the VLAN for a sub-VLAN. If you have configured a Layer 3 SVI for a super-VLAN, adding more sub-VLANs may fail due to insufficient resources. If you configure sub-VLANs for a super-VLAN, and then configure a Layer 3 SVI of the VLAN for a super-VLAN, some sub-VLANs may become common VLANs again due to insufficient resources y.

Configuring Proxy ARP

- Mandatory.
- Proxy ARP is enabled by default.
- Users in sub-VLANs can implement Layer 2 or Layer 3 communication across VLANs through the gateway proxy only after the proxy ARP function is enabled in both the super-VLAN and sub-VLANs.
- Users in sub-VLANs can communicate with users in other VLANs only after the proxy ARP function is enabled in both the super-VLAN and sub-VLANs.

The proxy ARP function must be enabled in both the super-VLAN and sub-VLANs. Otherwise, this function does not take effect.

Command	**proxy-arp**
Parameter Description	N/A
Defaults	The proxy ARP function is enabled by default.
Command Mode	VLAN configuration mode
Usage Guide	By default, the proxy ARP function is enabled. Run this command to enable the proxy ARP function in both the super-VLAN and sub-VLANs. Users in sub-VLANs can implement Layer 2 or Layer 3 communication across VLANs only after the proxy ARP function is enabled in both the super-VLAN and sub-VLANs.

Configuring a Virtual Interface for a Super-VLAN

- Mandatory.
- No physical interface can be added to a super-VLAN. You can configure the Layer 3 SVI for a VLAN.

When a super-VLAN is configure with an SVI, it allocates a Layer 3 interface to each sub-VLAN. If a sub-VLAN is not allocated a Layer 3 interface due to insufficient resources, the sub-VLAN becomes a common VLAN again.

Command	**interface vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates the ID of the super-VLAN.
Defaults	No virtual interface is configured for a super-VLAN by default.
Command Mode	Global configuration mode
Usage Guide	A Layer 3 interface must be configured as the virtual interface of a super-VLAN. For details, see *VLAN Command Reference*.

Configuring the Gateway of a Super-VLAN

- Mandatory.
- The IP gateway on the Layer 3 SVI is configured as the proxy for all users in sub-VLANs to respond to ARP Request packets.

Command	**ip address** *ip-address mask*
Parameter Description	*ip-address*: Indicates the IP address of the gateway on the virtual interface of a super-VLAN. *mask*: Indicates the mask.
Defaults	No gateway is configured for a super-VLAN by default.
Command Mode	Interface configuration mode
Usage Guide	Run this command to configure the gateway for a super-VLAN. Users of all sub-VLANs of the super-VLAN share this gateway.

Configuring the IP Address Range of the Sub-VLAN

- You can allocate an IP address range to each sub-VLAN. Users in a sub-VLAN can communicate with users of other VLANs only when their IP addresses are in the specified range.
- Unless otherwise specified, you do not need to configure the IP address range.

IP addresses dynamically allocated to users through DHCP may be not in the allocated IP address range. If the IP addresses allocated through DHCP are not in the specified range, users in a sub-VLAN cannot communicate with users of other VLANs. Therefore, exercise caution when you run the **subvlan-address-range** *start-ip end-ip* command.

The IP address range of a sub-VLAN must be within the IP address range of the super-VLAN to which the sub-VLAN belongs. Otherwise, users in sub-VLANs cannot communicate with each other.

IP addresses of users in a sub-VLAN must be within the IP address range of the sub-VLAN. Otherwise, users in the sub-VLAN cannot communicate with each other.

Command	**subvlan-address-range** *start-ip-address end-ip-address*
Parameter Description	*start-ip-address*: Indicates the start IP address of a sub-VLAN. *end-ip-address*: Indicates the end IP address of a sub-VLAN.
Defaults	No IP address range is configured for a sub-VLAN by default.
Command	VLAN configuration mode

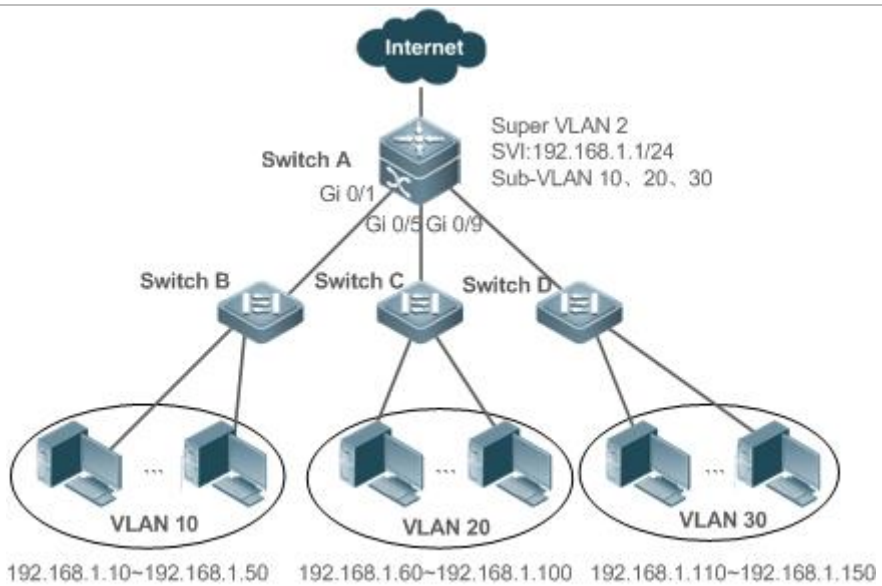
Mode	
Usage Guide	Optional. Run this command to configure the IP address range of users in a sub-VLAN. IP address ranges of different sub-VLANs of a super-VLAN cannot overlap with each other. IP address ranges of sub-VLANs of different super-VLANs can overlap each other. ⚠ The IP address range of a sub-VLAN must be within the IP address range of the super-VLAN to which the sub-VLAN belongs. Otherwise, users in sub-VLANs cannot communicate with each other. ⚠ Users in a sub-VLAN can communicate with users of other VLANs only when their IP addresses (either dynamically allocated through DHCP or statically configured) are in the configured IP address range. ⚠ IP addresses allocated through DHCP may not be in the configured IP address range. In this case, users in a sub-VLAN cannot communicate with users of other VLANs. Therefore, be cautious when using this command.

Verification

After each sub-VLAN is correlated with the gateway of the super-VLAN, users in sub-VLANs can ping each other.

Configuration Example

Configure a super-VLAN on the network to enable users in sub-VLANs of the super-VLAN to share the same network segment and the same IP gateway, so as to save IP addresses.

Scenario **Figure 1-2**	
Configuration Steps	● Configure a super-VLAN on the core switch. The configuration details are not mentioned here. ● On the access switch, configure common VLANs corresponding to sub-VLANs on the core switch.

A	`SwitchA#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`SwitchA(config)#vlan 2`

	SwitchA(config-vlan)#exit SwitchA(config)#vlan 10 SwitchA(config-vlan)#exit SwitchA(config)#vlan 20 SwitchA(config-vlan)#exit SwitchA(config)#vlan 30 SwitchA(config-vlan)#exit SwitchA(config)#vlan 2 SwitchA(config-vlan)#supervlan SwitchA(config-vlan)#subvlan 10,20,30 SwitchA(config-vlan)#exit SwitchA(config)#interface vlan 2 SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0 SwitchA(config)#vlan 10 SwitchA(config-vlan)#subvlan-address-range 192.168.1.10 192.168.1.50 SwitchA(config-vlan)#exit SwitchA(config)#vlan 20 SwitchA(config-vlan)#subvlan-address-range 192.168.1.60 192.168.1.100 SwitchA(config-vlan)#exit SwitchA(config)#vlan 30 SwitchA(config-vlan)#subvlan-address-range 192.168.1.110 192.168.1.150 SwitchA(config)#interface range gigabitEthernet 0/1,0/5,0/9 SwitchA(config-if-range)#switchport mode trunk
Verification	● Check whether the source device (192.168.1.10) and the destination device (192.168.1.60) can ping each other successfully.
A	SwitchA# show supervlan supervlan id supervlan arp-proxy subvlan id subvlan arp-proxy subvlan ip range ------------ ------------------- ---------- ----------------- ---------
	2 ON 10 ON 192.168.1.10 - 192.168.1.50
	20 ON 192.168.1.60 - 192.168.1.100
	30 ON 192.168.1.110 - 192.168.1.150

Common Errors

The SVI and IP gateway are not configured for the super-VLAN. Consequently, communication fails between sub-VLANs and between sub-VLANs and other VLANs.

The proxy ARP function is disabled in the super-VLAN or sub-VLANs. Consequently, users in sub-VLANs cannot communicate with users of other VLANs.

The IP address range of the sub-VLAN is configured, but IP addresses allocated to users are not in this range.

1.5 Monitoring

Displaying

Command	Description	
show supervlan [**id** *super-vlan-id*]	**Command**	**Description**

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug bridge svlan	Debugs the super-VLAN002E

1 Configuring VLAN Group

1.1 Overview

Each virtual LAN (VLAN) group contains multiple VLANs. A wireless LAN (WLAN) can be associated with a VLAN group to achieve 1:N mapping, which assigns VLANs flexibly to stations (STAs).

There are two VLAN assignment modes:

- After STAs pass 802.1X authentication, the authentication server assigns VLANs to STAs.
- The Dynamic Host Configuration Protocol (DHCP) server assigns VLANs to STAs based on the address pool.

Protocols and Standards

- N/A

1.2 Applications

Application	Description
VLAN Assignment	The VLAN group assigns VLANs to STAs.

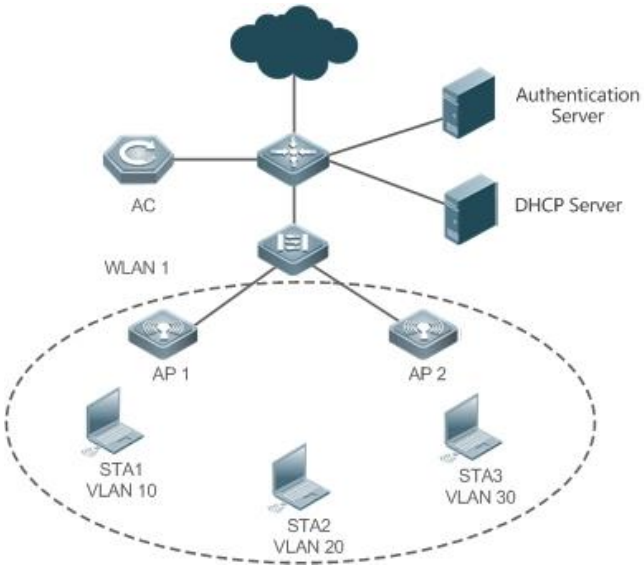
1.2.1 VLAN Assignment

Scenario

Multiple STAs connect to the same WLAN. VLANs are assigned to STAs based on the VLAN assignment mode of the VLAN group mapped to the WLAN.

As shown in Figure 1-1, the VLAN group assigns VLANs to STA 1, STA 2, and STA 3 connected to WLAN 1.

Figure 1-1



Remarks	STAs connect to the wired network through AP 1 and AP 2. The access controller (AC) connects to APs through the wired network to manage APs in a unified manner.

1.3 Features

Basic Concepts

VLAN Group

Multiple VLANs are added to a VLAN group. When STAs connect to a WLAN, VLANs are assigned to the STAs based on the VLAN assignment mode of the VLAN group mapped to the WLAN.

VLAN Assignment Mode

Each VLAN group can assign VLANs based on VLAN delivery of 802.1X or the DHCP server address pool.

Overview

Feature	Description
802.1X-based VLAN Assignment	You can plan VLANs to be assigned after STAs pass 802.1X authentication.
DHCP-based VLAN Assignment	VLANs are assigned flexibly to STAs based on the load of each address pool.

1.3.1 802.1X-based VLAN Assignment

Working Principle

Before authentication, a STA belongs to the default VLAN of a VLAN group mapped to the connected WLAN.

The STA will be authenticated in the default VLAN. After authentication succeeds, the authentication server determines whether to assign a VLAN. If so, the packets subsequently sent by the STA will be automatically redirected to the assigned VLAN. If not, the packets will be transmitted in the default VLAN of the default VLAN group.

1.3.2 DHCP-based VLAN Assignment

Working Principle

The device checks and records the assignment status of the DHCP servers corresponding to members of VLAN groups. If a STA in a VLAN sends multiple consecutive DHCP Request packets but receives no Reply packets, the DHCP server assignment status of the VLAN will be marked as "not assignable".

When a STA connects to a WLAN, it checks whether any VLAN with its DHCP server assignment status being "assignable" exists in the VLAN group.

If so, a VLAN with its DHCP server assignment status being "assignable" is randomly assigned to the STA. Then, the STA requests an IP address from the DHCP server. After the IP address is successfully obtained, the packets subsequently sent by the STA will be automatically redirected to the VLAN.

If not, the DHCP server assignment status of all VLANs in the VLAN group will be marked as "not assignable".

1.4 Configuration

Configuration	Description and Command	
Configuring a VLAN Group	(Mandatory) It is used to create a VLAN group and configure a VLAN list, the VLAN assignment mode, and default VLAN.	
	vlan-group *group-id*	Creates a VLAN group.
	vlan-list *vlan-list*	Configures a VLAN list for a VLAN group.
	vlan-assign-mode XX	Specifies the VLAN assignment mode for a VLAN group.
	default-vlan XX	Configures the default VLAN for a VLAN group.
	(Optional) It is used to configure the VLAN group name.	
	name *vlan-group-name*	Configures the VLAN group name.
Configuring Mapping Between a WLAN and a VLAN Group Supported functions vary depending on the product version. The WS7204 and WS6812 support this function; the settled AP (AP880), wall plate AP (AP180V2), and outdoor AP (AP680(CD)) do not support this function.	(Mandatory) It is used to configure the mapping between a WLAN and a VLAN group.	
	ap-group { *ap-group-name* | **default** }	Configures the AP group of an AP.
	interface-mapping	Configures WLAN-VLAN group mapping on ACs.

1.4.1 Configuring a VLAN Group

Configuration Effect

- Create a VLAN group and complete configurations related to the VLAN group.

Notes

- N/A

Configuration Step

Creating a VLAN Group

- Mandatory.
- Create a VLAN group so as to assign VLANs to STAs in its associated WLAN.

Command	**vlan-group** *group-id*
Parameter Description	*group-id*: Indicates the ID of a VLAN group. The value range is from 1 to 128.

Defaults	No VLAN group is created.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a VLAN List for a VLAN Group

- Mandatory. Ensure that VLANs have been created.
- Add multiple VLANs to the same VLAN group if a WLAN needs to map to multiple VLANs.
- Perform the configuration on the AC.

Command	**vlan-list** *vlan-list*
Parameter Description	*vlan-list*: Indicates a VLAN list. It contains a maximum of 128 VLANs.
Defaults	No VLAN list is configured.
Command Mode	VLAN group configuration mode
Usage Guide	N/A

Configuring the VLAN Assignment Mode for a VLAN Group

- Mandatory.
- Use this command to implement the VLAN assignment policy of a VLAN group.
- Perform the configuration on the AC.

Command	**vlan-assign-mode** { **dot1x** | **mac-hash** }
Parameter Description	**dot1x**: Indicates that the authentication server assigns VLANs to STAs after 802.1X authentication succeeds. **mac-hash**: Indicates the assignment of VLANs to user terminals based on the MAC address hashing.
Defaults	No VLAN assignment mode is configured.
Command Mode	VLAN group configuration mode or global configuration mode
Usage Guide	In global configuration mode, the configurations apply to all VLAN groups. In VLAN group configuration mode, the configurations apply to the VLAN group only. Configurations in VLAN group configuration mode take precedence over those in global configuration mode. There are two VLAN assignment modes: 802.1X-based and DHCP-based. DHCP –based assignment mode is not supported.

Configuring the Default VLAN for a VLAN Group

- Mandatory.
- Perform the configuration on the AC.
- The default VLAN takes effect when the WLAN is in 802.1X-based assignment mode, that is, when the authentication server assigns the default VLAN before 802.1X authentication succeeds.

- Configure it on ACs.

Command	**default-vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates the ID of a VLAN in the VLAN list of the VLAN group.
Defaults	No default VLAN is specified.
Command Mode	VLAN group configuration mode
Usage Guide	Before configuring the default VLAN, you must add this VLAN to the destination VLAN group.

Configuring the VLAN Group Name

- Optional.
- Configure this function on the AC.

Command	**name** *vlan-group-name*
Parameter Description	*vlan-group-name*: Indicates the VLAN group name, with a maximum length of 64 bytes.
Defaults	No VLAN group name is configured by default.
Command Mode	VLAN group configuration mode
Usage Guide	It is used to configure the VLAN group name. In the case of 802.1X VLAN assignment, the authentication service is matched against the VLAN group delivered by the authentication server and selects a VLAN from the matched VLAN group through the 802.1X policy. The authentication user is redirected from the default VLAN to the VLAN. If the VLAN group name is deleted or not configured on the device, the authentication server will not deliver VLANs. The packets from the client are transmitted over the default VLAN in the default VLAN group. Do not configure the same name for different VLAN groups.

Verification

- Check the configurations of the VLAN group.

Configuration Example

Configuring a VLAN Group

Configuration Steps	• Create VLAN Group 10. • Set the VLAN assignment mode to 802.1X-based mode. • Configure a VLAN list that contains VLAN 1 to VLAN 10. • Set the default VLAN to VLAN 1. • Configure the name as **vg10**.

	`Hostname# configure terminal`
	`Hostname(config)# vlan-group 10`
	`Hostname(config-vlan-group)# vlan-assign-mode dot1x`
	`Hostname(config-vlan-group)# vlan-list 1-10`
	`Hostname(config-vlan-group)# default-vlan 1`

	Hostname(config-vlan-group)# name vg10 Hostname(config-vlan-group)# end
Verification	● Check whether the configurations of VLAN Group 10 are correct.
	Hostname# show vlan-group 10 vlan-group id mode default-vlan vlan-list ------------ ---------- ---------- ---------- 10 dot1x 1 1-10

Common Errors

- A VLAN configured in a VLAN list does not exist.
- The default VLAN configured does not exist in the VLAN list.

1.4.2 Configuring Mapping Between a WLAN and a VLAN Group

Supported functions vary depending on the product version. The WS7204 and WS6812 support this function; the settled AP (AP880), wall plate AP (AP180V2), and outdoor AP (AP680(CD)) do not support this function.

Configuration Effect

- The mapping between a WLAN and a VLAN group so that STAs can be associated with the WLAN.

Notes

- N/A

Configuration Step

Configuring the AP Group of an AP

- Mandatory.

Command	**ap-group** { *ap-group-name* | **default** }
Parameter Description	*ap-group-name*: Creates an AP group and enters the AP group configuration mode. The name of the AP group contains a maximum of 63 bytes and spaces are not allowed. **default**: Enters the default AP group configuration mode.
Defaults	An AP group named **default** is automatically created by default after the system is started. This group cannot be created or deleted.
Command Mode	Global configuration mode
Usage Guide	When the **no** form of the command is used to delete an AP group, APs of this group are automatically moved to the default group.

Configuring Mapping Between a WLAN and a VLAN Group

- Mandatory.

Command	**interface-mapping** *wlan-id* [*vlan-id* I **group** *vlan-group-id* I **list** *vlan-list* [**def-vlan** *def-vlan-id*]] [**radio** { *radio-id* | **6GHz** | **802.11b** | **802.11a** }] [**ap-wlan-id** *ap-wlan-id*]
Parameter	*wlan-id*: Indicates the ID of the specified WLAN. This WLAN must have been created. The value

Description	range of the settled AP (AP880) is from 1 to 16; the value range of the wall plate AP (AP180V2) is from 1 to 8; the value range of the outdoor AP (AP680(CD)) is from 1 to 16. *vlan-id*: Indicates the ID of the specified VLAN. The VLAN ID range is from 1 to 4094. vlan-group-id: Indicates the ID of the specified VLAN group. The VLAN group ID range is from 1 to 128. *vlan-list*: Indicates the specified VLAN list. The value range is from 1 to 4094. The number of VLANs allowed in the list is 1 to 32. *def-vlan-id*: Indicates the default VLAN in the VLAN list. The value ranges from 1 to 4094. r*adio-id*: Indicates the ID of the radio of a specified AP. If radio-id is not specified, the mapping is applied to all radios of all APs in the AP group. The radio ID range is from 1 to 96. **6GHz**: Indicates that the mapping is applied to all 6 GHz radios of all APs in the AP group. **802.11b**: Indicates that the mapping is applied to all 2.4 GHz radios of all APs in the AP group. **802.11a**: Indicates that the mapping is applied to all 5.8 GHz radios of all APs in the AP group. *ap-wlan-id*: Specifies the WLAN ID that is used on the AP through interface mapping. The value range is from 1 to 64.
Defaults	By default, a WLAN is not associated with any VLAN group.
Command Mode	AP group configuration mode
Usage Guide	Only the AC supports this command. ● In local forwarding mode, if the VLAN ID assigned to a terminal by using the **interface-mapping** command is the same as the VLAN ID specified by using the **ap-vlan** command, the service VLAN for data forwarding by the terminal will be determined by the access switch connected to the AP. In particular, if the VLAN ID configured by using the **interface-mapping** command is 1 (when the **ap-vlan** command is not configured, the default VLAN ID of **ap-vlan** is 1), the VLAN of the terminal for data forwarding will be determined by the access switch. ● When the **interface-mapping** command is used to configure the list mapping mode, a single VLAN ID can be added, but the VLAN ID specified in the VLAN list cannot be deleted. ● When the i**nterface-mapping** command is used to configure the list mapping mode, the VLAN members in the VLAN list must be configured with corresponding VLANs on the AC. Otherwise, the 802.1X authenticated users cannot be connected.

Verification

- Run the **show running** command to check configurations of all AP groups.

Configuration Example

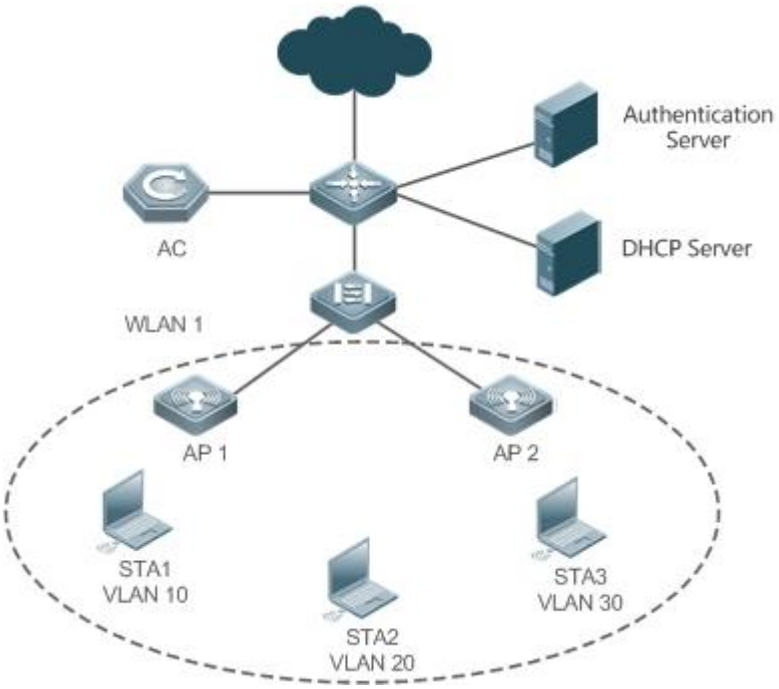
Configuring Mapping Between a WLAN and a VLAN Group

Configuration Steps	● Enter the AP group configuration mode. ● Configure the mapping between a WLAN and a VLAN group.
	`Hostname(config)# ap-group default` `Hostname(config-ap-group)# interface-mapping 1 vlan-group 1`
Verification	● Run the **show running** command to check whether the configuration is correct.

Configuring 802.1X-based VLAN Assignment

In the WLAN scenario shown in Figure 1-2, leaders, employees, and guests are differentiated to access the WLAN with different privilege levels. The following configurations are required:

- Create VLAN group 100, including VLAN 10, VLAN 20, and VLAN 30.
- Map WLAN 1 to VLAN group 100. When STAs access WLAN 1, the authentication server performs 802.1X authentication for the STAs. After the authentication is complete, the authentication server assigns VLAN 10 to leaders, VLAN 20 to employees, and VLAN 30 to guests.

Scenario **Figure 1-2**	
Configuration Steps	● If 1:N mapping between a WLAN and a VLAN group is used, different VLANs can be assigned to STAs in the same WLAN. ● Set the WLAN authentication mode to 802.1X authentication so that different VLANs can be assigned to different STAs.
AP1 & AP2	APs apply the centralized forwarding in fit AP architecture by default, and are managed by the AC in a unified manner.

AC	Step 1: Create VLANs respectively for different types of users.
	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# vlan range 10,20,30`
	`Hostname(config-vlan-range)# exit`
	Step 2: Create a VLAN group, add VLAN 10, VLAN 20, and VLAN 30 to the group, and configure VLAN 30 as the default VLAN for guests.
	`Hostname(config)# vlan-group 100`
	`Hostname(config-vlan-group)# vlan-assign-mode dot1x`
	`Hostname(config-vlan-group)# vlan-list 10,20,30`
	`Hostname(config-vlan-group)# default-vlan 30`
	`Hostname(config-vlan-group)# exit`
	Step 3: Create WLAN 1, with the WLAN authentication mode set to 802.1X authentication and the encryption mode set to Advanced Encryption Standard (AES).

	Hostname(config)# wlan-config 1 office_wifi Hostname(config-wlan)# exit Hostname(config)# wlansec 1 Hostname(wlansec)# security wpa enable Hostname(wlansec)# security wpa akm 802.1x enable Hostname(wlansec)# security wpa ciphers aes enable Step 4: Configure the mapping between WLAN 1 and VLAN group 100. Hostname(config)# ap-group default Hostname(config-ap-group)# interface-mapping 1 vlan-group 100
Authentication Server	● Before establishing a new STA type on the authentication server, configure a specific VLAN.
Verification	● Check the VLAN group configuration on the AC.
AC	Hostname# show vlan-group VLAN-Group ID Default VLAN Assign-Mode VLAN-List ---------- ---------- ---------- ---------- 100 30 dot1x 10,20,30

Common Errors

- N/A

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show vlan-group [*group-id*]	Displays VLAN group information.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug bridge vgoup	Debugs the VLAN group status.

1 Configuring MSTP

1.1 Overview

The Spanning Tree Protocol (STP) is a Layer 2 management protocol. It can selectively block redundant links to eliminate Layer 2 loops and back up links.

STP is continuously updated from the Rapid Spanning Tree Protocol (RSTP) to the Multiple Spanning Tree Protocol (MSTP) as the network develops.

For the Layer 2 Ethernet, only one active link can exist between two local area networks (LANs). Otherwise, a broadcast storm will occur. To enhance reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. Manual control is infeasible in this situation. Therefore, STP needs to automatically complete this work. STP enables devices on a LAN to provide the following functions:

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by an administrator. The best topology tree can be obtained by properly configuring these parameters.

RSTP is compatible with 802.1D STP. Similar to traditional STP, RSTP provides loop-free topology and link redundancy. It is characterized by rapid speed. If all bridges on a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds for traditional STP) to re-generate a topology tree after the network topology changes.

STP and RSTP have the following defects:

- STP migration is slow. Even on point-to-point links or edge ports, it still takes twice the forward delay for ports to switch to the forwarding state.
- RSTP can rapidly converge but has the same defect with STP. Since all VLANs on a LAN share the same spanning tree, packets of all VLANs are forwarded along this spanning tree. Therefore, redundant links cannot be blocked according to specific VLANs and data traffic cannot be load balanced among VLANs.

MSTP, defined by IEEE 802.1s, resolves defects of STP and RSTP. It can rapidly converge and enable traffic of different VLANs to be forwarded along respective paths, thereby providing a better load balancing mechanism for redundant links.

Typically, STP/RSTP works based on ports, while MSTP works based on instances. An instance is a set of multiple VLANs. Binding multiple VLANs to one instance can reduce the communication overhead and resource utilization.

Ruijie devices support STP, RSTP, and MSTP, and comply with IEEE 802.1d, IEEE 802.1w, and IEEE 802.1s.

Protocols and Standards

- IEEE 802.1D: Media Access Control (MAC) Bridges
- IEEE 802.1w: Part 3: Media Access Control (MAC) Bridges—Amendment 2: Rapid Reconfiguration

- IEEE 802.1s: Virtual Bridged Local Area Networks—Amendment 3: Multiple Spanning Trees

1.2 Applications

Application	Description
Configuring MSTP	With the hierarchical network architecture, MSTP and the Virtual Router Redundancy Protocol (VRRP) are used to implement redundancy and load balancing to improve system availability of the network.

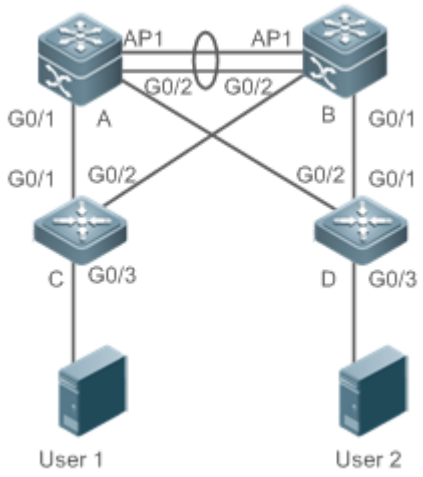
1.2.1 MSTP+VRRP Dual-Core Topology

Scenario

The MSTP+VRRP dual-core solution is often used. This solution improves system availability of a network. It uses the hierarchical network architecture composed of three layers (core layer, aggregation layer, and access layer) or two layers (core layer and access layer), forming the switching network system to provide data exchange service.

In the hierarchical network architecture, all capacity indicators, characteristics, and functions of network devices at each layer are optimized based on their network locations and roles, enhancing their stability and availability.

Figure 1-1 MSTP+VRRP Dual-Core Topology



Remarks	The topology is divided into two layers: core layer (Devices A and B) and access layer (Devices C and D).

Deployment

- Core layer: Multiple Spanning Tree instances (MSTIs) are configured to realize load balancing. For example, two MSTIs are created: MSTI 1 and MSTI 2. MSTI 1 maps VLAN 10, while MSTI 2 maps VLAN 20. Device A is the root bridge of MSTIs 0 and 1. MSTI 0 is the Common and Internal Spanning Tree (CIST), which exists by default. Device B is the root bridge of MSTI 2.
- Core layer: Devices A and B are VRRP master devices in VLAN 10 and VLAN 20, respectively.
- Access layer: Configure the port directly connected to the terminal (PC or server) as an edge port, and enable BPDU guard to prevent users from accessing unauthorized devices.

1.3 Features

Basic Concepts

BPDU

To generate a stable tree topology network, ensure that the following conditions are met:

- Each bridge has a unique ID consisting of the bridge priority and MAC address.
- The overhead of the path from the bridge to the root bridge is called the root path cost.
- A port ID consists of the port priority and port number.

Bridges exchange Bridge Protocol Data Units (BPDUs) to obtain information required for establishing the best tree topology. The BPDUs use the multicast address 01-80-C2-00-00-00 (hexadecimal notation) as the destination address.

A BPDU consists of the following elements:

- Root bridge ID assumed by the local bridge
- Root path cost of the local bridge
- Bridge ID of the local bridge
- Message Age (lifetime of the BPDU)
- Port ID (ID of the port sending the BPDU)
- Forward Delay, Hello Time, Max Age are specified in MSTP.
- Other flags, such as flags indicating network topology changes and local port status

If a port of a bridge receives a BPDU with a higher priority (smaller bridge ID and lower root path cost), the bridge saves BPDU information and transmits the information to all other ports. If the bridge receives a BPDU with a lower priority, it discards the information.

Such a mechanism allows information with higher priorities to be transmitted across the entire network. BPDU exchange results are as follows:

- A bridge is selected as the root bridge.
- Except the root bridge, each bridge has a root port, that is, a port providing the shortest path to the root bridge.
- Each bridge calculates the shortest path to the root bridge.
- Each LAN has a designated bridge located in the shortest path between the LAN and the root bridge. A port designated to connect the bridge and the LAN is called designated port.
- The root port and designated port enter the forwarding state.

Bridge ID

According to IEEE 802.1w, each bridge has a unique ID. The spanning tree algorithm selects the root bridge based on the bridge ID. The bridge ID consists of 8 bytes, of which the last 6 bytes are the MAC address of the bridge. In its first 2 bytes (as listed in the following table), the first 4 bits indicate the priority; the last 8 bits indicate the system ID and is reserved. In RSTP, the system ID is 0. Therefore, the bridge priority should be an integral multiple of 4096.

-	Priority				System ID											
bit	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
-	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1
-	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0

Spanning Tree Timers

The following three timers affect the performance of the entire spanning tree:

- Hello timer: Interval for periodically sending a BPDU.
- Forward Delay timer: Interval for changing the port status, that is, interval for a port to change from the listening state to the learning state or from the learning state to the forwarding state when RSTP runs in STP-compatible mode.
- Max Age timer: Maximum time-to-live (TTL) of a BPDU. When this timer elapses, the BPDU is discarded.

Port Roles and States

Each port plays a role on a network to reflect different functions in the network topology.

- Root port: Provides the shortest path to the root bridge.
- Designated port: Is used by each LAN to connect the root bridge.
- Alternate port: Is the alternative port of the root port. Once the root port loses its role, the alternate port immediately changes to the root port.
- Backup port: Is the backup of the designated port. When a bridge has two ports connected to a LAN, the port with the higher priority is the designated port while the port with the lower priority is the backup port.
- Disabled port: Is in inactive state. The port with the operation state being Down plays this role.

The following uppercase letters represent roles of different ports:

- R: root port
- D: designated port
- A: alternate port
- B: backup port

Unless otherwise specified, the ports are prioritized in descending order: R > D > A > B.

Figure 1-2

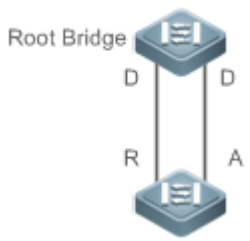


Figure 1-3

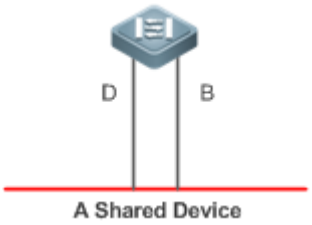
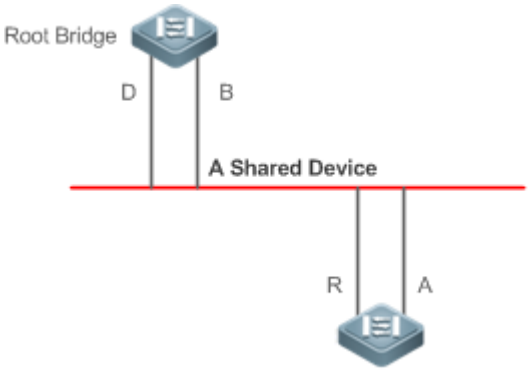


Figure 1-4



Each port has three states indicating whether to forward data packets so as to control the entire spanning tree topology:

- Discarding: Does not forward received packets or learn the source MAC address.
- Learning: Does not forward received packets but learns the source MAC address, which is a transitive state.
- Forwarding: Forwards received packets and learns the source MAC address.

For a stable network topology, only the root port and designated port can enter the forwarding state while other ports are always in discarding state.

Hop Count

Internal spanning trees (ISTs) and MSTIs calculate whether the BPDU time expires based on the hop count that is similar to the IP TTL, but not Message Age and Max Age.

You are advised to run the **spanning-tree max-hops** command in global configuration mode to configure the hop count. In a region, every time a BPDU passes through a device from the root bridge, the hop count decreases by 1. When the hop count becomes 0, the BPDU time expires and the device discards the BPDU.

To be compatible with STP and RSTP outside the region, MSTP retains Message Age and Max Age mechanisms.

Overview

Feature	Description
STP	STP, defined by IEEE 802.1D, is used to eliminate physical loops at the data link layer on a LAN.
RSTP	RSTP, defined by IEEE 802.1w, is optimized based on STP to rapidly converge the network topology.
MSTP	MSTP, defined by IEEE 802.1s, resolves defects of STP, RSTP, and Per-VLAN Spanning Tree (PVST). It can rapidly converge and forward traffic of different VLANs along respective paths, thereby providing a better load balancing mechanism for redundant links.

MSTP Optional Features	MSTP optional features include the edge port, BPDU guard, BPDU filter, TC protection, TC guard, TC filter, BPDU source MAC address check, BPDU filter, Auto Edge, root guard, and loop guard.

1.3.1 STP

STP is used to prevent broadcast storms incurred by loops and provide link redundancy.

Working Principle

For the Layer 2 Ethernet, only one active link can exist between two LANs. Otherwise, a broadcast storm will occur. To enhance reliability of a LAN, it is necessary to establish a redundant link and keep some paths in backup state. If the network is faulty and a link fails, you must switch the redundant link to the active state. Manual control is infeasible in this situation. Therefore, STP needs to automatically complete this work. STP enables devices on a LAN to provide the following functions

- Discover and start the best tree topology on the LAN.
- Troubleshoot a fault and automatically update the network topology so that the possible best tree topology is always selected.

The LAN topology is automatically calculated based on a set of bridge parameters configured by the administrator. The best topology tree can be obtained by properly configuring these parameters.

1.3.2 RSTP

RSTP is compatible with 802.1D STP. Similar to traditional STP, RSTP provides loop-free and redundancy services. It is characterized by rapid speed. If all bridges on a LAN support RSTP and are properly configured by the administrator, it takes less than 1 second (about 50 seconds for traditional STP) to re-generate a topology tree after the network topology changes.

Working Principle

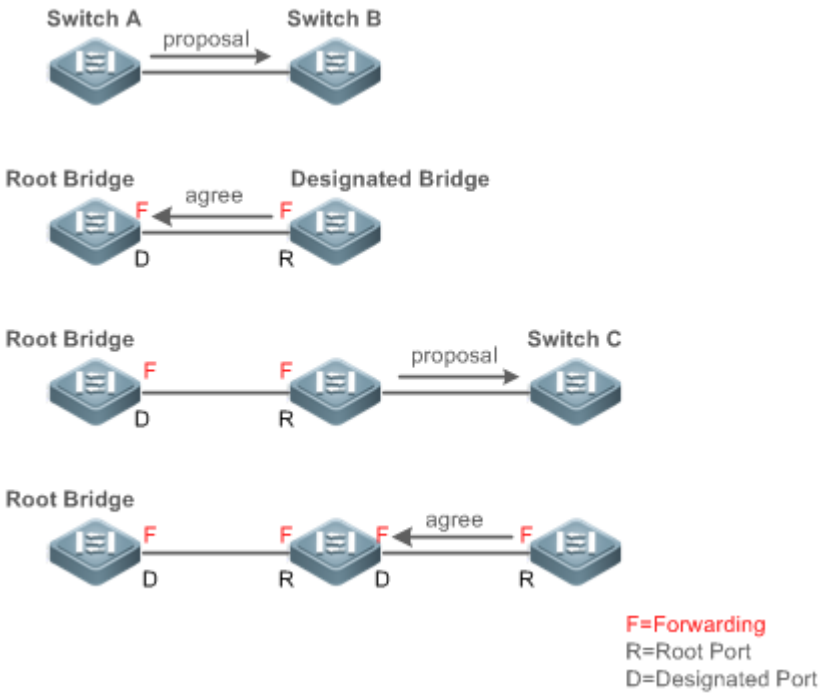
↘ Fast Convergence of RSTP

RSTP can make ports quickly enter the forwarding state.

STP enables a port to enter the forwarding state 30 seconds (twice the value of the Forward Delay, which can be configured and has the default value of 15 seconds) after selecting a port role. Each time the topology changes, the root port and designated port reselected by each bridge enter the forwarding state 30 seconds later. Therefore, it takes about 50 seconds for the entire network topology to become the tree topology.

RSTP differs greatly from STP in the forwarding process. As shown in Figure 1-5, Switch A sends an RSTP Proposal packet to Switch B. If Switch B finds that the priority of Switch A is higher, it selects Switch A as the root bridge. In addition, the port receiving the packet is used as the root port and enters the forwarding state immediately. Then, Switch B sends an Agree packet from the root port to Switch A. If the designated port of Switch A is agreed, the port enters the forwarding state. Switch B's designated port resends a Proposal packet to extend the spanning tree by sequence. RSTP can recover the network tree topology to rapidly converge once the network topology changes.

Figure 1-5



The preceding handshake process is implemented only when ports are connected in point-to-point mode. To give the devices their full play, do not use non-P2P connections between devices.

Figure 1-6 and **Figure 1-7** show the examples of non-point-to-point connection.

Example of non-P2P connection:

Figure 1-6

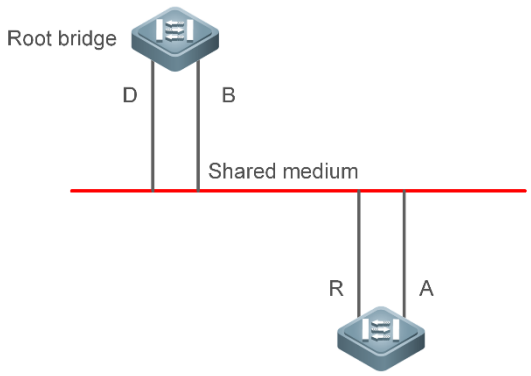


Figure 1-7

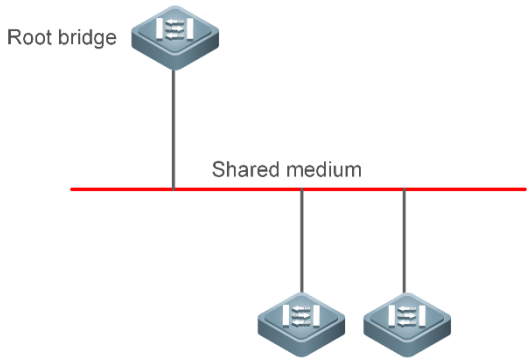
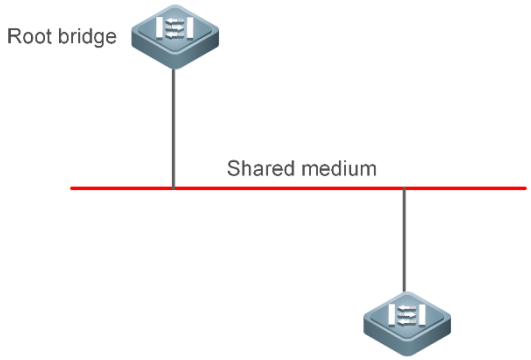


Figure 1-8 shows an example of point-to-point connection.

Figure 1-8



Compatibility Between RSTP and STP

RSTP is compatible with STP. RSTP automatically checks whether the connected bridge supports STP or RSTP based on the received BPDU version number. If the port connects to an STP bridge, the port enters the forwarding state 30s later.

Another problem may occur when RSTP and STP are used together. As shown in the following figures, Switch A (RSTP) connects to Switch B (STP). If Switch A finds itself connected to an STP bridge, it sends an STP BPDU. However, if Switch B is replaced with Switch C (RSTP) but Switch A still sends STP BPDUs, Switch C will assume itself connected to the STP bridge. As a result, two RSTP devices work in STP mode, reducing the efficiency.

RSTP provides the protocol migration feature to forcibly send RSTP BPDUs (the peer bridge must support RSTP). In this case, Switch A is enforced to send an RSTP BPDU and Switch C then finds itself connected to the RSTP bridge. As a result, two RSTP devices work in RSTP mode, as shown in Figure 1-9.

Figure 1-9

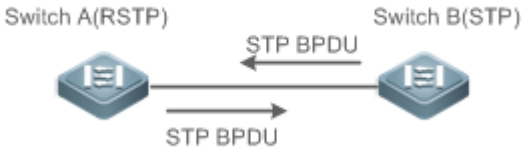
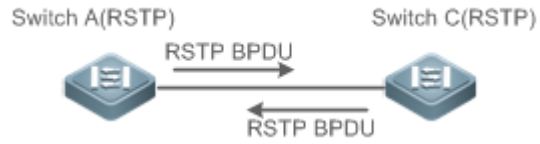


Figure 1-10



1.3.3 MSTP

MSTP resolves defects of STP and RSTP. It can rapidly converge and forward traffic of different VLANs along respective paths, thereby providing a better load balancing mechanism for redundant links.

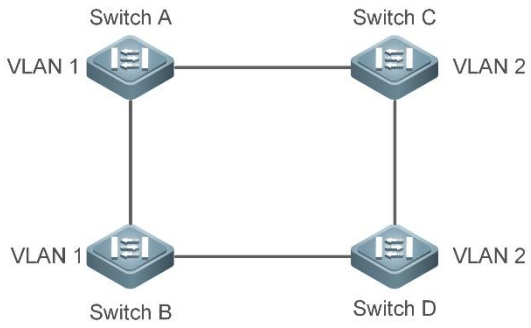
Working Principle

Ruijie devices support MSTP. MSTP is developed based on traditional STP and RSTP, and also provides the fast RSTP forwarding mechanism.

Since traditional spanning tree protocols are irrelevant to VLANs, problems may occur in specific network topologies.

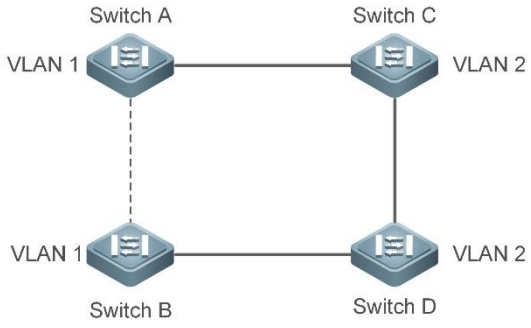
As shown in Figure 1-11, Devices A and B are in VLAN 1, while Devices C and D are in VLAN 2, forming a loop.

Figure 1-11



If the cost of the link from Device A to Device B through Devices C and D is less than that of the link from Device A to Device B, the link between Device A and Device B enters the discarding state (as shown in Figure 1-12). Because Devices C and D are not added to VLAN 1 and cannot forward data packets of VLAN 1, VLAN 1 of Device A fails to communicate with VLAN 1 of Device B.

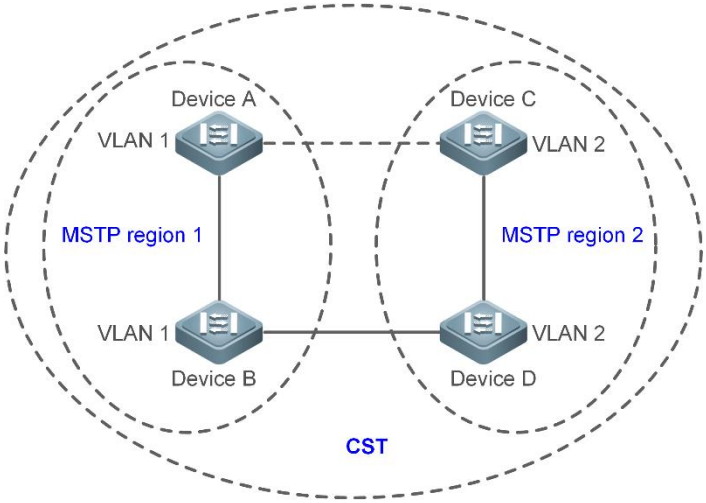
Figure 1-12



MSTP is developed to resolve this problem. It divides one or more VLANs of a device into an MSTI. Devices configured with the same MSTI form an MST region to run an independent spanning tree (called IST). The MST region implements the spanning tree algorithm with other MST regions to generate a complete spanning tree, which is called common spanning tree (CST).

Based on this algorithm, the network topology is formed shown in Figure 1-13. Devices A and B are in MSTP region 1 where no loop occurs, and therefore no link enters the discarding state. This also applies to MSTP region 2. Loops exist between MST region 1 and region 2, so a link is selected to enter the discarding state.

Figure 1-13



This prevents loops to ensure proper communication between devices in the same VLAN.

MSTP Region Division

For MSTP, you must properly divide MSTP regions and configure the same MST configuration for devices in the same MSTP region.

MST configuration includes the following items:

- MST configuration name: Consists of at most 32 bytes to identify an MSTP region.
- MST revision number: Consists of 16 bits to identify an MSTP region.
- MSTI-VLAN mapping table: A maximum of 64 MSTIs (with their IDs ranging from 1 to 64) are created for each device and MSTI 0 exists by default. Therefore, the system supports a maximum of 65 MSTIs. You can assign 1 to 4,994 VLANs belonging to different MSTIs (ranging from 0 to 64) as required. Unassigned VLANs belong to MSTI 0 by default. In this case, each MSTI is a VLAN group and implements the spanning tree algorithm of the MSTI specified in the BPDU, which is not affected by CIST and other MSTIs.

Run the **spanning-tree mst configuration** command in global configuration mode to enter the MST configuration mode to configure the preceding information.

MSTP BPDUs carry the preceding information. If the BPDU received by a device carries the same MST configuration with that on the device, it regards that the connected device belongs to the same MST region with itself. Otherwise, it regards the connected device originated from another MST region.

You are advised to configure the MSTI-VLAN mapping table after disabling MSTP. Then, re-enable MSTP to ensure stability and convergence of the network topology.

IST (Spanning Tree in an MST Region)

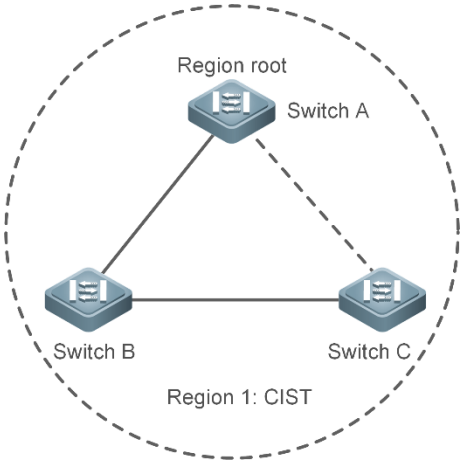
After MSTP regions are divided, each region selects an independent root bridge for each MSTI based on the corresponding parameters such as the bridge priority and port priority, assigns roles to each port on each device, and specifies whether the port is in forwarding or discarding state in the MSTI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

Through MSTP BPDU exchange, an IST is generated and each MSTI has their own spanning tree, in which the spanning tree corresponding to MSTI 0 and CST are uniformly called Common Instance Spanning Tree (CIST). That is, each MSTI provides a single and loop-free network topology for their own VLAN groups.

As shown in Figure 1-14, Devices A, B, and C form a loop in Region 1.

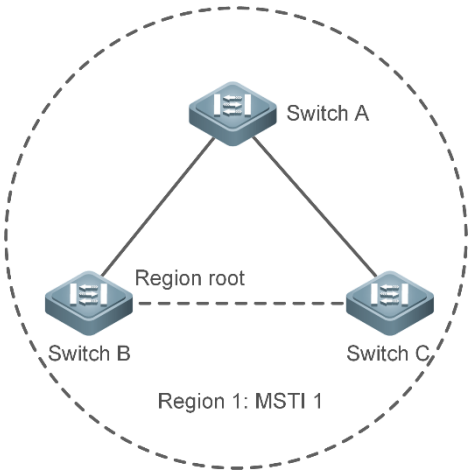
As shown in Figure 1-14, Device A has the highest priority in the CIST (MSTI 0) and thereby is selected as the region root. Then the link between A and C is enabled to enter the discarding state based on other parameters. Therefore, for the VLAN group of MSTI 0, only links from A to B and from B to C are available, eliminating the loop of this VLAN group.

Figure 1-14



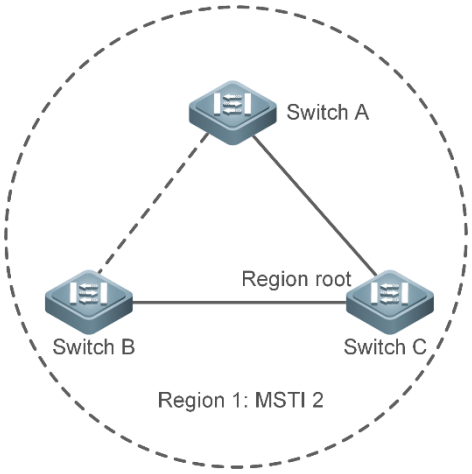
As shown in Figure 1-15, Device B has the highest priority in the MSTI 1 and thereby is selected as the region root. Then the link between B and C is enabled to enter the discarding state based on other parameters. Therefore, for the VLAN group of MSTI 1, only links from A to B and from A to C are available, eliminating the loop of this VLAN group.

Figure 1-15



As shown in Figure 1-16, Device C has the highest priority in the MSTI 2 and thereby is selected as the region root. Then the link between B and C is enabled to enter the discarding state based on other parameters. Therefore, for the VLAN group of MSTI 2, only links from B to C and from A to C are available, eliminating the loop of this VLAN group.

Figure 1-16

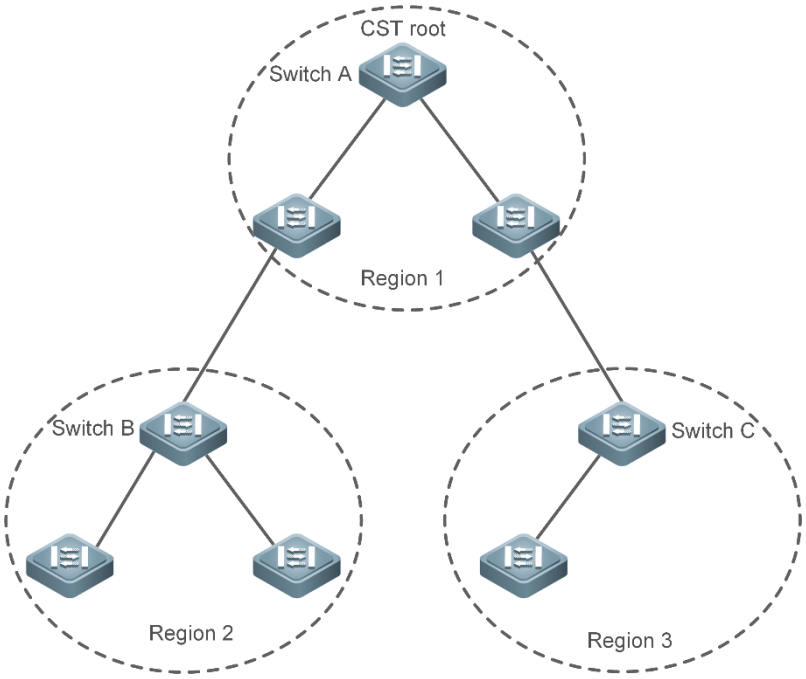


Note that MSTP does not consider the VLAN which a port belongs to. Therefore, you should configure the path cost and priority of a related port based on the actual VLAN configuration to prevent MSTP from incorrectly eliminating loops.

CST (Spanning Tree Between MST Regions)

Each MST region is similar to a large device for the CST. Different MST regions form a large network topology tree called CST. As shown in Figure 1-17, Device A, of which the bridge ID is the smallest, is selected as the root in the entire CST and the CIST regional root in this region. In MST region 2, since the root path cost from Device B to the CST root is lowest, Device B is selected as the CIST regional root in the region. For the same reason, Device C is selected as the CIST regional root.

Figure 1-17



The CIST regional root may be not the device of which the bridge ID is the smallest in the region but indicates the device of which the root path cost from this region to the CST root is the smallest.

For the MSTI, the root port of the CIST regional root has a new role: master port. The master port acts as the outbound port and is in forwarding state for all instance MSTIs. To make the topology more stable, the master port of each region to the CST root should be on the same device of the region if possible.

Compatibility Among MSTP, RSTP, and STP

Similar to RSTP, MSTP sends STP BPDUs to be compatible with STP. For details, see *Compatibility Between RSTP and STP*.

Since RSTP processes MSTP BPDUs of the CIST, MSTP does not need to send RSTP BPDUs to be compatible with it.

Each STP or RSTP device is a single region and does not form the same region with any devices.

1.3.4 MSTP Optional Features

MSTP optional features mainly include the edge port, BPDU guard, BPDU filter, TC guard, and guard mode. The optional features are mainly used to deploy MSTP configuration based on the network topology and application characteristics on the MSTP network. This enhances stability, robustness, and attack defense capabilities of MSTP, meeting application requirements of MSTP in different customer scenarios.

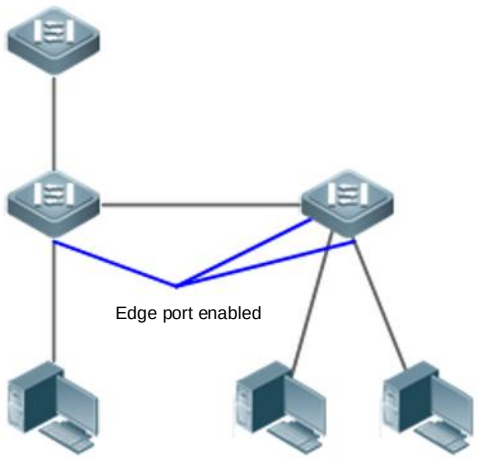
Working Principle

Edge Port

If a port of a device connects directly to a network terminal, this port is configured as an edge port to directly enter the forwarding state. If the edge port is not configured, the port needs to wait for 30s to enter the forwarding state.

Figure 1-18 shows the ports that can be configured as edge ports.

Figure 1-18



If an edge port still receives BPDUs, its Port Fast Operational State is Disabled and the port enters the forwarding state according to the normal STP algorithm.

BPDU Guard

BPDU guard can be enabled globally or on a port.

You are advised to run the **spanning-tree portfast bpduguard default** command in global configuration mode to enable global BPDU guard. If a port receiving a BPDU is configured as an edge port or automatically identified as an edge port, the port immediately enters the error-disabled state to indicate the configuration error. In addition, the port is disabled, indicating that a network device may be added by an unauthorized user to change the network topology.

You are advised to run the **spanning-tree bpduguard enable** command in interface configuration mode to enable BPDU guard on a port regardless of whether the port is configured as the edge port. In this case, the port enters the error-disabled state immediately after receiving a BPDU.

BPDU Filter

BPDU filter can be enabled globally or on a port.

You are advised to run the **spanning-tree portfast bpdufilter default** command in global configuration mode to enable BPDU filter globally. In this case, the edge port does not receive or send BPDUs, and the host directly connected to the edge port cannot receive BPDUs. If the port changes its Port Fast Operational State to Disabled after receiving a BPDU, BPDU filter automatically takes ineffective.

You are advised to run the **spanning-tree bpdufilter enable** command in interface configuration mode to enable BPDU filter on a port regardless of whether the port is configured as the edge port. In this case, the port does not receive or send BPDUs but directly enters the forwarding state.

TC Protection

TC BPDUs carry the TC. If a switch receives such packets, the network topology changes and the switch will delete the MAC address table. For Layer 3 devices in this case, the forwarding module is re-enabled and the port status in the ARP entry changes. When a device is attacked by forged TC BPDUs, it will frequently perform the preceding operations, causing heavy load and affecting network stability. To prevent this problem, you can enable TC protection.

TC protection can be globally enabled or disabled only. This function is disabled by default.

When TC protection is enabled, the switch deletes TC BPDUs within a specified period (generally 4s) after receiving them and monitors whether any TC BPDU is received during the period. If a device receives TC BPDUs during this period, it deletes them when the period expires. This can prevent the device from frequently deleting MAC address entries and ARP entries.

TC Guard

TC protection ensures fewer dynamic MAC addresses and ARP entries deleted when a large number of TC BPDUs are generated on a network. However, a device receiving TC attack packets still performs many removal operations and TC BPDUs can be spread, affecting the entire network. TC guard can be used to prevent TC BPDUs from spreading globally or on a port. If TC guard is enabled globally or on a port, a port receiving TC BPDUs filters these TC BPDUs or TC BPDUs generated by itself, so TC BPDUs will not be spread to other ports. This can effectively control possible TC attacks on a network to ensure network stability. On Layer 3 devices, this function can effectively prevent the access device from flapping and causing the core route to be unreachable.

- If TC guard is used incorrectly, communication between networks is interrupted.
- You are advised to enable this function only when unauthorized TC attack packets are received on the network.
- If TC guard is enabled globally, no port spreads TC BPDUs to others. This function can be enabled only on desktop access devices.

If TC guard is enabled on a port, the topology changes incurred and TC BPDUs received on the port will not be spread to other ports. This function can be enabled only on uplink ports, particularly on ports of the aggregation device connected to the core device.

TC Filter

If TC guard is enabled on a port, the port does not forward TC BPDUs received and generated by the port to other ports performing spanning tree calculation on the device. When the status of a port changes (for example, from blocking to forwarding), the port generates TC BPDUs, indicating that the topology may have changed.

Because TC guard prevents TC BPDUs from being spread, the device may not delete MAC addresses of the port when the network topology changes, causing a data forwarding error.

TC filter is introduced to resolve this problem. TC filter does not process TC BPDUs received by ports but processes TC BPDUs in case of normal topology changes. If the port that is not configured as the edge port frequently alternates between Up and Down, MAC addresses are deleted and the core route may be unreachable. Enabling TC filter can resolve this issue, and core routing entries can be updated in a timely manner when the topology changes.

TC filter is disabled by default.

BPDU Source MAC Address Check

BPDU source MAC address check prevents BPDUs from maliciously attacking switches and causing MSTP exceptions. When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check so that the switch receives BPDUs sent only by the peer switch and discards all other BPDUs, thereby preventing malicious attacks. You can enable BPDU source MAC address check in interface configuration mode. One port can only filter one MAC address. If you run the **no bpdu src-mac-check** command to disable BPDU source MAC address check on a port, the port receives all BPDUs.

BPDU Filter

If the Ethernet length of a BPDU exceeds 1500 bytes, this BPDU will be discarded. This function prevents the device from receiving unauthorized BPDUs.

Auto Edge

If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3s), the device regards a network device connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU.

You can run the **spanning-tree autoedge disabled** command to disable Auto Edge.

This function is enabled by default.

If Auto Edge conflicts with the manually configured edge port, the edge port takes effect.

Because Auto Edge is used for rapid negotiation and forwarding between the designated port and the downlink port, STP does not support this function. If the designated port is in forwarding state, the Auto Edge configuration does not take effect on this port. It takes effect only when rapid negotiation is re-performed, for example, when the network cable is removed and reinstalled.

If BPDU filter has been enabled on a port, the port directly enters the forwarding state and is not automatically identified as an edge port.

Auto Edge applies only to the designated port.

Root Guard

During network design, the root bridge and backup root bridge are usually allocated to the same region. Due to incorrect configuration of maintenance personnel or malicious attacks on a network, the root bridge may receive the configuration with a higher priority and thereby switches to the backup root bridge, causing incorrect changes in the network topology. Root guard is used to resolve this problem.

If root guard is enabled on a port, its role in all MSTIs is forcibly configured as the designated port. Once the port receives the configuration with a higher priority, it enters the root-inconsistent (blocking) state. If the port does not receive the configuration with a higher priority within a period, it returns to its original state.

If a port enters the blocking state due to root guard, you can manually restore the port to the normal state by disabling root guard on this port or disabling spanning tree guard (running **spanning-tree guard none** in interface configuration mode).

If root guard is used incorrectly, the network link will be terminated.

If root guard is enabled on a non-designated port, this port will be forcibly configured as a designated port and enter the BKN state. This indicates that the port enters the blocking state due to root inconsistency.

If a port receiving the configuration with a higher priority in MSTI 0 enters the BKN state, this port will be enforced in BKN state in all other MSTIs.

Root guard and loop guard cannot be configured on a port simultaneously.

Loop Guard

Due to the unidirectional link failure, the root port or backup port becomes the designated port and enters the forwarding state if it does not receive BPDUs, causing a network loop. Loop guard is used to prevent this problem.

If a port enabled with loop guard does not receive BPDUs, the port switches its role but stays in discarding state till it receives BPDUs and recalculates the spanning tree.

You can enable loop guard globally or on a port.

Root guard and loop guard cannot be configured on a port simultaneously.

Before the MSTP process is restarted on a port, the port enters the blocking state. If the port still receives no BPDU after the MSTP process is restarted, the port will become a designated port and enter the forwarding state. Therefore, you should check the cause why a port enters the blocking state in loop protection and rectify the fault as soon as possible before restarting the MSTP process. Otherwise, the spanning tree topology will still become abnormal after the MSTP process is restarted.

BPDU Transparent Transmission

In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved address. That is, devices compliance with IEEE 802.1Q do not forward the BPDUs received. However, devices may need to transparently transmit BPDUs during network deployment. For example, if STP is disabled on a device, the device needs to transparently transmit BPDUs so that the spanning tree between devices is properly calculated.

BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDUs.

1.4 Configuration

Configuration	Description and Command	
Enabling STP	(Mandatory) It is used to enable STP.	
	spanning-tree mode	Configures the STP mode.
	spanning-tree (with parameters)	Configures STP time parameters.
	spanning-tree	Enables STP
Configuring STP Compatibility	(Optional) It is used to be compatible with third-party devices.	
	spanning-tree compatible enable	Enables the compatibility mode of a port.
	clear spanning-tree detected-protocols	Performs mandatory version check for BPDUs.
Configuring an MST Region	(Optional) It is used to configure an MSTP region.	
	spanning-tree mst configuration	Enters the MST configuration mode.
Enabling Fast Convergence of RSTP	(Optional) It is used to configure whether the link type of a port is point-to-point connection.	
	spanning-tree link-type	Configures the link type.
Configuring Priorities	(Optional) It is used to configure the switch priority or port priority.	
	spanning-tree priority	Configures the switch priority.
	spanning-tree port-priority	Configures the port priority.
Configuring the Port Path Cost	(Optional) It is used to configure the path cost of a port or the default path cost calculation method.	
	spanning-tree cost	Configures the port path cost.
	spanning-tree pathcost method	Configures the default path cost calculation method.
Configuring the Maximum Hop Count of a BPDU	(Optional) It is used to configure the maximum hop count of a BPDU.	
	spanning-tree max-hops	Configures the maximum hop count of a BPDU.
Enabling the Edge Port	(Optional) It is used to enable edge port-related features.	
	spanning-tree portfast	Enables the edge port.
	spanning-tree portfast bpduguard default	Enables BPDU guard on all ports.
	spanning-tree bpduguard enable	Enables BPDU guard on a port.
	spanning-tree portfast bpdufilter default	Enables BPDU filter on all ports.
	spanning-tree bpdufilter enable	Enables BPDU filter on a port.
Enabling TC-related Features	(Optional) It is used to enable TC-related features.	
	spanning-tree tc-protection	Enables TC protection.

Configuration	Description and Command	
	spanning-tree tc-protection tc-guard	Enables TC guard on all ports.
	spanning-tree tc-guard	Enables TC guard on a port.
	spanning-tree ignore tc	Enables TC filter on a port.
Enabling BPDU Source MAC Address Check	(Optional) It is used to enable BPDU source MAC address check.	
	bpdu src-mac-check	Enables BPDU source MAC address check on a port.
Configuring Auto Edge	(Optional) It is used to configure Auto Edge.	
	spanning-tree autoedge	Enables Auto Edge on a port. This function is enabled by default.
Enabling Guard-related Features	(Optional) It is used to enable port guard features.	
	spanning-tree guard root	Enables root guard on a port.
	spanning-tree loopguard default	Enables loop guard on all ports.
	spanning-tree guard loop	Enables loop guard on a port.
	spanning-tree guard none	Disables the guard feature on a port.
Enabling BPDU Transparent Transmission	(Optional) It is used to enable BPDU transparent transmission	
	bridge-frame forwarding protocol bpdu	Enables BPDU transparent transmission.

1.4.1 Enabling STP

Configuration Effect

- Optional. Configure the STP mode.
- Optional. Configure STP time parameters.
- Enable STP globally.

Notes

- STP and Transparent Interconnection of Lots of Links (TRILL) of the data center cannot be enabled simultaneously.

Configuration Step

↘ Configuring the STP Mode

- Optional.
- Run the **spanning-tree mode** [**stp | rstp | mstp**] command to change the STP mode.
- According to 802.1 standards, STP, RSTP, and MSTP are compatible, without any configuration by the administrator. However, some vendors' devices do not conform to 802.1 standards, resulting in incompatibility. This command can be used to switch the spanning tree mode to an earlier version if other vendors' devices are incompatible with Ruijie devices.

Command	**spanning-tree mode** [**stp** | **rstp** | **mstp**]

Parameter Description	**mstp**: Indicates the Multiple Spanning Tree Protocol (MSTP), which is defined in IEEE 802.1s. **rstp**: Indicates the Rapid Spanning Tree Protocol (RSTP)), which is defined in IEEE 802.1w. **stp**: Indicates the Spanning Tree Protocol (STP)), which is defined in IEEE 802.1D.
Defaults	The default value is **mstp**.
Command Mode	Global configuration mode
Usage Guide	Some vendors' devices do not conform to 802.1 standards, resulting in incompatibility. If other vendors' devices are incompatible with Ruijie devices, run this command to switch the STP mode to an earlier version.

Configuring STP Time Parameters

- Optional.
- Run the **spanning-tree** [**forward-time** *forward* | **hello-time** *hello* | **max-age** *age* | **tx-hold-count** *tx-hold-count*] command to configure STP time parameters. One configuration command can carry only one parameter.

Command	**spanning-tree** [**forward-time** *forward*	**hello-time** *hello*	**max-age** *age*	**tx-hold-count** *tx-hold-count*]
Parameter Description	**forward-time** *forward*: Specifies the interval for changing the port status, in seconds. The value range is from 4 to 30. The default value is 15. **hello-time** *hello*: Specifies the interval for the device to send BPDUs, in seconds. The value range is from 1 to 10. The default value is 2. **max-age** *age*: Specifies the maximum timeout interval of BPDUs, in seconds. The value range is from 6 to 40. The default value is 20. **tx-hold-count** *tx-hold-count*: Configures the maximum number of BPDUs sent every second. The value range is from 1 to 10. The default value is 3.
Defaults	The default values of **forward-time**, **hello-time**, **max-age**, and **tx-hold-count** are 15, 2, 20, 20, and 3, respectively.
Command Mode	Global configuration mode
Usage Guide	The value ranges of **forward-time**, **hello-time**, and **max-age** are related. Changing the value range of one affects the value ranges of the other two parameters. The relationship is as follows: 2 x (Hello Time + 1.0 second) ≤ Max Age ≤ 2 x (Forward Delay – 1.0 second) If the preceding condition is not met, the topology may be unstable.

Enabling STP

- Mandatory. Unless otherwise specified, STP should be enabled on each device.
- Run the **spanning-tree** command to enable STP. STP is disabled by default.

Command	**spanning-tree**
Parameter Description	N/A
Defaults	STP is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Display the configuration.

Configuration Example

Enabling STP and Configuring Timer Parameters

Scenario **Figure 1-19**	
Configuration Steps	Enable STP and set the STP mode to STP on devices. Configure the timer parameters of Device A (root bridge) as follows: ● Hello Time = 4s ● Max Age = 25s ● Forward Delay = 18s

Device A	Step 1: Enable STP and set the STP mode to STP.
	`Hostname#configure terminal`
	`Hostname(config)#spanning-tree`
	`Hostname(config)#spanning-tree mode stp`
	Step 2: Configure timer parameters of Device A.
	`Hostname(config)#spanning-tree hello-time 4`
	`Hostname(config)#spanning-tree max-age 25`
	`Hostname(config)#spanning-tree forward-time 18`

Device B	Enable STP and set the STP mode to STP.
	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#spanning-tree`
	`Hostname(config)#spanning-tree mode stp`

Verification	● Run the **show spanning-tree summary** command to display the spanning tree topology and protocol configuration parameters.

Device A	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol stp`
	`  Root ID    Priority    0`
	`             Address     00d0.f822.3344`
	`             this bridge is root`
	`             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec`
	
	`  Bridge ID  Priority    0`
	`             Address     00d0.f822.3344`
	`             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec`

	Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p Gi0/1 Desg FWD 20000 128 False P2p
Device B	Hostname#show spanning-tree summary Spanning tree enabled protocol stp Root ID Priority 0 Address 00d0.f822.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 32768 Address 001a.a917.78cc Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Altn BLK 20000 128 False P2p Bound(STP) Gi0/1 Root FWD 20000 128 False P2p Bound(STP)

Common Errors

The timer parameters will take effect only after the device has been elected as the root bridge.

1.4.2 Configuring STP Compatibility

Configuration Effect

- Enable the compatibility mode of a port to implement interconnection between Ruijie devices and third-party devices.
- Enable protocol migration to perform forcible version check, which will affect compatibility between RSTP and STP.

Notes

- If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the port to realize interconnection between Ruijie devices and third-party devices.

Configuration Step

↘ Enabling the Compatibility Mode on a Port

- Optional.

Command	**spanning-tree compatible enable**
Parameter Description	N/A

Command Mode	Interface configuration mode
Usage Guide	If the compatibility mode is enabled on a port, this port will add different MSTI information into the to-be-sent BPDU based on the port to realize interconnection between Ruijie devices and third-party devices.

Enabling Protocol Migration

- Optional.
- If the peer device supports RSTP, you can enforce version check on the local device to force the two devices to run RSTP.

Command	**clear spanning-tree detected-protocols** [**interface** *interface-type interface-number*]
Parameter Description	**interface** *interface-type interface-number*: Indicates a port.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to enforce a port to send RSTP BPDUs and perform forcible check on them.

Verification

- Display the configuration.

Configuration Example

Enabling STP Compatibility

Scenario Figure 1-20	
Configuration Steps	• Configure MSTIs 1 and 2 on Device A and Device B, and map MSTI 1 to VLAN 10 and MSTI 2 to VLAN 20. • Add GigabitEthernet 0/1 and GigabitEthernet 0/2 to VLAN 10 and VLAN 20 respectively, and enable STP compatibility.

Device A	Step 1: Configure MSTIs 1 and 2, and map MSTI 1 to VLAN 10 and MSTI 2 to VLAN 20.
	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#spanning-tree mst configuration`
	`Hostname(config-mst)#instance 1 vlan 10`
	`Hostname(config-mst)#instance 2 vlan 20`
	Step 2: Configure the VLAN to which the port belongs, and enable STP compatibility on the port.
	`Hostname(config)#interface gigabitethernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)#switchport access vlan 10`
	`Hostname(config-if-GigabitEthernet 0/1)#spanning-tree compatible enable`

	Hostname(config-if-GigabitEthernet 0/1)#interface gigabitethernet 0/2 Hostname(config-if-GigabitEthernet 0/2)#switchport access vlan 20 Hostname(config-if-GigabitEthernet 0/2)#spanning-tree compatible enable
Device B	Perform the same steps as Device A.
Verification	● Run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated.

Device A	Hostname#show spanning-tree summary
	
	Spanning tree enabled protocol mstp
	MST 0 vlans map : 1-9, 11-19, 21-4094
	  Root ID Priority 32768
	  Address 001a.a917.78cc
	  this bridge is root
	  Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec
	
	  Bridge ID Priority 32768
	  Address 001a.a917.78cc
	  Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec
	
	Interface Role Sts Cost Prio OperEdge Type
	---------- ---- --- ---------- -------- -------- ----------
	Gi0/2 Desg FWD 20000 128 False P2p
	Gi0/1 Desg FWD 20000 128 False P2p
	
	MST 1 vlans map : 10
	  Region Root Priority 32768
	  Address 001a.a917.78cc
	  this bridge is region root
	
	  Bridge ID Priority 32768
	  Address 001a.a917.78cc
	
	Interface Role Sts Cost Prio OperEdge Type
	---------- ---- --- ---------- -------- -------- ----------
	Gi0/1 Desg FWD 20000 128 False P2p
	
	MST 2 vlans map : 20
	  Region Root Priority 32768
	  Address 001a.a917.78cc
	  this bridge is region root
	
	  Bridge ID Priority 32768
	  Address 001a.a917.78cc

	Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Desg FWD 20000 128 False P2p
Device B	Hostname#show spanning-tree summary Spanning tree enabled protocol mstp MST 0 vlans map : 1-9, 11-19, 21-4094 Root ID Priority 32768 Address 001a.a917.78cc this bridge is root Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Bridge ID Priority 32768 Address 00d0.f822.3344 Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Altn BLK 20000 128 False P2p Gi0/1 Root FWD 20000 128 False P2p MST 1 vlans map : 10 Region Root Priority 32768 Address 001a.a917.78cc this bridge is region root Bridge ID Priority 32768 Address 00d0.f822.3344 Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/1 Root FWD 20000 128 False P2p MST 2 vlans map : 20 Region Root Priority 32768 Address 001a.a917.78cc this bridge is region root Bridge ID Priority 32768 Address 00d0.f822.3344 Interface Role Sts Cost Prio OperEdge Type ---------- ---- --- ---------- -------- -------- ---------- Gi0/2 Root FWD 20000 128 False P2p

Common Errors

You are advised to configure the same VLAN list on the two sides of the link.

1.4.3 Configuring an MST Region

Configuration Effect

- This section describes how to configure an MST region to change devices in the MST region, so as to affect the network topology.

Notes

- To make multiple devices belong to the same MSTP region, configure the same name, revision number, and MSTI-VLAN mapping table for them.
- You can configure VLANs for MSTIs 0 to 64, and then the remaining VLANs are automatically allocated to MSTI 0. One VLAN belongs to only one MSTI.
- You are advised to configure the MSTI-VLAN mapping table after disabling STP. Then re-enable MSTP to ensure stability and convergence of the network topology.

Configuration Step

↘ Configuring an MST Region

- Optional.
- Configure an MST region when multiple devices need to belong to the same MST region.
- Run the **spanning-tree mst configuration** command to configure the MST region configuration mode.
- Run the **instance** *instance-id* **vlan** *vlan-range* command to configure the MSTI-VLAN mapping.
- Run the **name** *name* command to configure the MST name.
- Run the **revision** *version* command to configure the MST version number.

Command	**spanning-tree mst configuration**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to enter the MST configuration mode.

Command	**instance** *instance-id* **vlan** *vlan-range*
Parameter Description	*instance-id*: Indicates the MSTI ID. The value range is from 0 to 64. *vlan-range*: Indicates the VLAN ID. The value range is from 1 to 4,094.
Defaults	By default, only MSTI 0 exists, and all VLANs are mapped to MSTI 0.
Command Mode	MST configuration mode
Usage Guide	To add a VLAN group to an MSTI, run this command.

	For example, **instance 1 vlan 2-200**: Adds VLANs 2 to 200 to MSTI 1. **instance 1 vlan 2,20,200**: Adds VLANs 2, 20, and 200 to MSTI 1. You can run the **no instance** *instance-id* **vlan** *vlan-range* command to remove VLANs from an MSTI. The removed VLANs are automatically added to MSTI 0.

Command	**name** *name*
Parameter Description	*name*: Indicates the MST name. It consists of a maximum of 32 bytes.
Defaults	The name of an MST region is empty by default.
Command Mode	MST configuration mode
Usage Guide	N/A

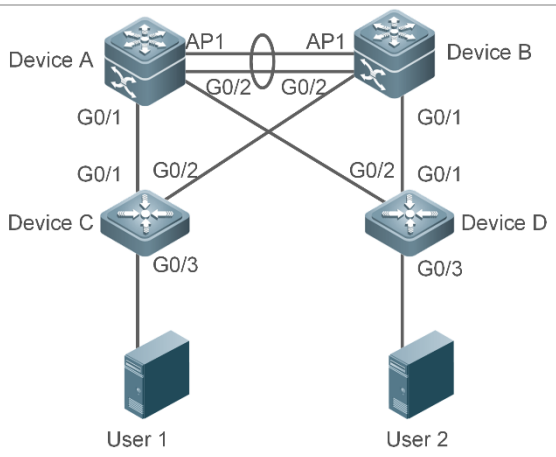
Command	**revision** *version*
Parameter Description	*version*: Indicates the MST revision number. The value range is from 0 to 65,535.
Defaults	The default revision value of an MST region is 0.
Command Mode	MST configuration mode
Usage Guide	N/A

Verification

- Run the **show spanning-tree mst configuration** command to display the MST region configuration.

Configuration Example

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

Scenario **Figure 1-21**	
Configuration Steps	● Enable MSTP and create MSTIs 1 and 2 on Device A, Device B, Device C, and Device D. ● Configure Device A as the root bridge of MSTIs 0 and 1 and Device B as the root bridge of MSTI 2. ● Configure Device A as the VRRP master device of VLANs 1 and 10 and Device B as the

	VRRP master device of VLAN 20.

Device A	Step 1: Configure VLANs 10 and 20, and configure ports as trunk ports.
	`Hostname(config)#vlan 10`
	`Hostname(config-vlan)#vlan 20`
	`Hostname(config-vlan)#exit`
	`Hostname(config)#interface range gigabitethernet 0/1-2`
	`Hostname(config-if-range)#switchport mode trunk`
	`Hostname(config-if-range)#interface aggregateport 1`
	`Hostname(config-if-AggregatePort 1)# switchport mode trunk`
	Step 2: Enable MSTP and create MSTIs 1 and 2.
	`Hostname(config)#spanning-tree`
	`Hostname(config)# spanning-tree mst configuration`
	`Hostname(config-mst)#instance 1 vlan 10`
	`Hostname(config-mst)#instance 2 vlan 20`
	`Hostname(config-mst)#exit`
	Step 3: Configure Device A as the root bridge of MSTIs 0 and 1.
	`Hostname(config)#spanning-tree mst 0 priority 4096`
	`Hostname(config)#spanning-tree mst 1 priority 4096`
	`Hostname(config)#spanning-tree mst 2 priority 8192`
	Step 4: Configure VRRP priorities to enable Device A to act as the VRRP master device of VLAN 10, and configure the virtual gateway IP address of VRRP.
	`Hostname(config)#interface vlan 10`
	`Hostname(config-if-VLAN 10)ip address 192.168.10.2 255.255.255.0`
	`Hostname(config-if-VLAN 10) vrrp 1 priority 120`
	`Hostname(config-if-VLAN 10) vrrp 1 ip 192.168.10.1`
	Step 5: Set the VRRP priority to the default value 100 to enable Device A to act as the VRRP backup device of VLAN 20.
	`Hostname(config)#interface vlan 20`
	`Hostname(config-if-VLAN 20)ip address 192.168.20.2 255.255.255.0`
	`Hostname(config-if-VLAN 20) vrrp 1 ip 192.168.20.1`

Device B	Step 1: Configure VLANs 10 and 20, and configure ports as trunk ports.
	`Hostname(config)#vlan 10`
	`Hostname(config-vlan)#vlan 20`
	`Hostname(config-vlan)#exit`
	`Hostname(config)#interface range gigabitethernet 0/1-2`
	`Hostname(config-if-range)#switchport mode trunk`
	`Hostname(config-if-range)#interface aggregateport 1`
	`Hostname(config-if-AggregatePort 1)# switchport mode trunk`
	Step 2: Enable MSTP and create MSTIs 1 and 2.
	`Hostname(config)#spanning-tree`
	`Hostname(config)# spanning-tree mst configuration`
	`Hostname(config-mst)#instance 1 vlan 10`
	`Hostname(config-mst)#instance 2 vlan 20`
	`Hostname(config-mst)#exit`

	Step 3: Configure Device A as the root bridge of MSTI 2.
	`Hostname(config)#spanning-tree mst 0 priority 8192`
	`Hostname(config)#spanning-tree mst 1 priority 8192`
	`Hostname(config)#spanning-tree mst 2 priority 4096`
	Step 4: Configure the virtual gateway IP address of VRRP.
	`Hostname(config)#interface vlan 10`
	`Hostname(config-if-VLAN 10)ip address 192.168.10.3 255.255.255.0`
	`Hostname(config-if-VLAN 10) vrrp 1 ip 192.168.10.1`
	Step 5: Set the VRRP priority to 120 to enable Device B to act as the VRRP backup device of VLAN 20.
	`Hostname(config)#interface vlan 20`
	`Hostname(config-if-VLAN 20)vrrp 1 priority 120`
	`Hostname(config-if-VLAN 20)ip address 192.168.20.3 255.255.255.0`
	`Hostname(config-if-VLAN 20) vrrp 1 ip 192.168.20.1`

Device C	Step 1: Configure VLANs 10 and 20, and configure ports as trunk ports.
	`Hostname(config)#vlan 10`
	`Hostname(config-vlan)#vlan 20`
	`Hostname(config-vlan)#exit`
	`Hostname(config)#interface range gigabitethernet 0/1-2`
	`Hostname(config-if-range)#switchport mode trunk`
	Step 2: Enable MSTP and create MSTIs 1 and 2.
	`Hostname(config)#spanning-tree`
	`Hostname(config)# spanning-tree mst configuration`
	`Hostname(config-mst)#instance 1 vlan 10`
	`Hostname(config-mst)#instance 2 vlan 20`
	`Hostname(config-mst)#exit`
	Step 3: Configure the port connecting Device C directly to users as an edge port and enable BPDU guard.
	`Hostname(config)#interface gigabitethernet 0/3`
	`Hostname(config-if-GigabitEthernet 0/3)#spanning-tree portfast`
	`Hostname(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable`

Device D	Perform the same steps as Device C.
Verification	● Run the **show spanning-tree summary** command to check whether the spanning tree topology is correctly calculated. ● Run the **show vrrp brief** command to check whether the VRRP master/backup devices are successfully created.

Device A	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans map : 1-9, 11-19, 21-4094`
	`  Root ID    Priority    4096`
	`             Address     00d0.f822.3344`
	`             this bridge is root`
	`             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec`

```
  Bridge ID  Priority    4096
             Address     00d0.f822.3344
             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Desg FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p

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

  Bridge ID  Priority    4096
             Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Desg FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p

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

  Bridge ID  Priority    8192
             Address     00d0.f822.3344

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Root FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p
```

Device B

```
Hostname#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
  Root ID    Priority    4096
             Address     00d0.f822.3344
```

```
             this bridge is root
             Hello Time   4 sec  Forward Delay 18 sec  Max Age 25 sec

  Bridge ID  Priority    8192
             Address     001a.a917.78cc
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Root FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p

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

  Bridge ID  Priority    8192
             Address     001a.a917.78cc

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Root FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p

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

  Bridge ID  Priority    4096
             Address     001a.a917.78cc

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Ag1              Desg FWD 19000      128      False    P2p
Gi0/1            Desg FWD 200000     128      False    P2p
Gi0/2            Desg FWD 200000     128      False    P2p
```

Device C

```
Hostname#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-4094
```

	Root ID Priority 4096 Address 00d0.f822.3344 this bridge is root Hello Time 4 sec Forward Delay 18 sec Max Age 25 sec Bridge ID Priority 32768 Address 001a.a979.00ea Hello Time 2 sec Forward Delay 15 sec Max Age 20 sec Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Altn BLK 200000 128 P2p False Fa0/1 Root FWD 200000 128 P2p False MST 1 vlans map : 10 Region Root Priority 4096 Address 00d0.f822.3344 this bridge is region root Bridge ID Priority 32768 Address 001a.a979.00ea Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Altn BLK 200000 128 P2p False Fa0/1 Root FWD 200000 128 P2p False MST 2 vlans map : 20 Region Root Priority 4096 Address 001a.a917.78cc this bridge is region root Bridge ID Priority 32768 Address 001a.a979.00ea Interface Role Sts Cost Prio Type OperEdge ---------- ---- --- ---------- -------- ----- ---------- Fa0/2 Root FWD 200000 128 P2p False Fa0/1 Altn BLK 200000 128 P2p False
Device D	Omitted.

Common Errors

- MST region configurations are inconsistent in the MSTP topology.
- VLANs are not created before you configure the MSTI-VLAN mapping.

- A device runs STP or RSTP in the MSTP+VRRP topology, but calculates the spanning tree according to the algorithms of different MST regions.

1.4.4 Enabling Fast Convergence of RSTP

Configuration Effect

- The link type affects fast convergence of RSTP.

Notes

- If the link type of a port is point-to-point, RSTP can rapidly converge. For details, see *Fast Convergence of RSTP*. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port. If a port works in full duplex mode, the device sets the link type to point-to-point. If a port works in half duplex mode, the device sets the link type to shared. You can also forcibly configure the link type to determine whether the port type is point-to-point.

Configuration Step

↘ Configuring the Link Type

- Optional.

Command	**spanning-tree link-type** { **point-to-point** | **shared** }
Parameter Description	**point-to-point**: Forcibly sets the link type of a port to be point-to-point. **shared**: Forcibly sets the link type of a port to be shared.
Defaults	The default connection type is **point-to-point** for full-duplex ports and **shared** for half-duplex ports.
Command Mode	Interface configuration mode
Usage Guide	If the link type of a port is point-to-point, RSTP can rapidly converge. If the link type is not configured, the device automatically sets the link type based on the duplex mode of the port.

Verification

- Run the **show spanning-tree interface** *interface-type interface-number* **link-type** command to display the configuration of the spanning tree port.
- Run the **show spanning-tree summary** command to display the link type of the port.

Configuration Example

↘ Enabling Fast Convergence of RSTP

Configuration Steps	● Set the link type of a port to point-to-point.
	`Hostname(config)#interface gigabitethernet 0/1` `Hostname(config-if-GigabitEthernet 0/1)#spanning-tree link-type point-to-point`
Verification	● Run the **show spanning-tree summary** command to display the link type of the port.
	`Hostname#show spanning-tree summary`

```
Spanning tree enabled protocol mstp
MST 0 vlans map : ALL
  Root ID    Priority    32768
             Address     001a.a917.78cc
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     00d0.f822.3344
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/1            Root FWD 20000      128      False    P2p
```

Common Errors

If a port works in half duplex mode, the device sets the link type to shared.

1.4.5 Configuring Priorities

Configuration Effect

- The switch priority determines a device used as the root of the entire network and the topology of the entire network.
- The port priority determines the port that enters the forwarding state.

Notes

- You are advised to set a higher priority (small value) for the core device to ensure stability of the entire network. You can assign different switch priorities to different MSTIs so that each MSTI runs an independent STP based on the assigned priorities. Devices in different regions use the priority only of the CIST (MSTI 0). For the bridge ID, the switch priority has 16 optional values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. They are integral multiples of 4096. The default value is 32768.
- If two ports are connected to a shared device, the device selects a port with a higher priority (smaller value) to enter the forwarding state and a port with a lower priority (larger value) to enter the discarding state. If the two ports have the same priority, the device selects the port with a smaller port ID to enter the forwarding state. You can assign different port priorities to different MSTIs on a port so that each MSTI runs an independent STP based on the assigned priorities.
- Similar to the switch priority, the port priority also has 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. They are integral multiples of 16. The default value is 128.

Configuration Step

↘ Configuring the Switch Priority

- Optional.

- To change the root or topology of a network, configure the switch priority.

Command	**spanning-tree** [**mst** *instance-id*] **priority** *priority*
Parameter Description	**mst** *instance-id*: Indicates the ID of an MSTI. The value range is from 0 to 64. The default value is 0. **priority** *priority*: Indicates the switch priority. There are 16 optional values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. They are integral multiples of 4096.
Defaults	The default bridge priority is 32768.
Command Mode	Global configuration mode
Usage Guide	Configure the switch priority to determine a device as the root of the entire network and to determine the topology of the entire network.

Configuring the Port Priority

- Optional.
- To change the preferred port entering the forwarding state, configure the port priority.

Command	spanning-tree [**mst** *instance-id*] **port-priority** *port-priority*
Parameter Description	**mst** *instance-id*: Indicates the ID of an MSTI. The value range is from 0 to 64. The default value is 0. **port-priority** *port-priority*: Indicates the port priority. There are 16 optional values: 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. They are integral multiples of 16.
Defaults	The default port priority is 128.
Command Mode	Interface configuration mode
Usage Guide	If a loop occurs in a region, the port with a higher priority is preferred to enter the forwarding state. If two ports have the same priority, the port with a smaller port ID is selected to enter the forwarding state.

Verification

- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Configuring the Port Priority

Scenario **Figure 1-22**	
Configuration Steps	● Configure the bridge priority so that Device A becomes the root bridge of the spanning tree. ● Configure the priority of GigabitEthernet 0/2 on Device A as 16 so that GigabitEthernet 0/2 on Device B can be selected as the root port.

Device A	Step 1: Enable STP and configure the bridge priority.
	`Hostname(config)#spanning-tree`
	`Hostname(config)#spanning-tree mst 0 priority 0`
	Step 2: Configure the priority of Gi 0/2.
	`Hostname(config)#interface gigabitethernet 0/2`
	`Hostname(config-if-GigabitEthernet 0/2)#spanning-tree mst 0 port-priority 16`

Device B	`Hostname(config)#spanning-tree`
Verification	● Run the **show spanning-tree summary** command to display the topology calculation result of the spanning tree.

Device A	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans map : ALL`
	`  Root ID    Priority    0`
	`             Address     00d0.f822.3344`
	`             this bridge is root`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`  Bridge ID  Priority    0`
	`             Address     00d0.f822.3344`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`Interface        Role Sts Cost       Prio     OperEdge Type`
	`---------------- ---- --- ---------- -------- -------- ----------------`
	`Gi0/2            Desg FWD 20000      16       False    P2p`
	`Gi0/1            Desg FWD 20000      128      False    P2p`

Device B	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans map : ALL`
	`  Root ID    Priority    0`
	`             Address     00d0.f822.3344`
	`             this bridge is root`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`  Bridge ID  Priority    32768`
	`             Address     001a.a917.78cc`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`Interface        Role Sts Cost       Prio     OperEdge Type`
	`---------------- ---- --- ---------- -------- -------- ----------------`
	`Gi0/2            Root FWD 20000      128      False    P2p`
	`Gi0/1            Altn BLK 20000      128      False    P2p`

Common Errors

The port priority will take effect only after the designated port has been changed.

1.4.6 Configuring the Port Path Cost

Configuration Effect

- Configuring the path cost of a port will determine the forwarding state of the port and the topology of the entire network.
- If the path cost of a port uses its default value, configuring the path cost calculation method affects the calculation result.

Notes

- A device selects a port as the root port if the path cost from this port to the root bridge is the lowest. Therefore, the port path cost determines the root port of the local device. The default port path cost is automatically calculated based on the port rate (Media Speed). A port with a higher rate will have a low path cost. Because this method can calculate the most proper path cost, do not change the path cost unless required. You can assign different path costs to different MSTIs on a port so that each MSTI runs an independent STP based on the assigned path costs.
- If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate. However, IEEE 802.1d-1998 and IEEE 802.1t define different path costs for the same link rate. The value is a an integer ranging from 1 to 65,535 in short mode for 802.1d-1998 and from 1 to 200,000,000 in long mode for IEEE 802.1t. The path cost of an aggregate port has two solutions:

  1. Ruijie solution: path cost of an aggregate port = port path cost x 95%

  2. Solution recommended in standards: path cost of an aggregate port = 20,000,000,000/actual link bandwidth of the aggregate port (actual link bandwidth of the aggregate port = bandwidth of a member port x number of active member ports)

  The administrator must unify the path cost calculation method on the entire network. The default standard is the private integer standard in long mode.
- The following table lists path costs automatically configured for different link rate in two solutions.

Port Rate	Port	IEEE 802.1d (Short)	IEEE 802.1t (Long)	IEEE 802.1t (Long Standard)
10M	Common port	100	2000000	2000000
	Aggregate port	95	1900000	2000000/linkupcnt
100M	Common port	19	200000	200000
	Aggregate port	18	190000	200000/linkupcnt
1000M	Common port	4	20000	20000
	Aggregate port	3	19000	20000/linkupcnt
10000M	Common port	2	2000	2000
	Aggregate port	1	1900	20000/linkupcnt

- The private integer standard in long mode is used by default. After the solution is changed to the path cost solution recommended by the standards, the path cost of an aggregate port changes with the number of member ports in Up state. If the port path cost changes, the network topology also will change.

- If an aggregate port is static, **linkupcnt** is the number of active member ports. If an aggregate port works in LACP mode, **linkupcnt** is the number of member ports forwarding data. If no member port in the aggregate port goes up, **linkupcnt** is 1. For details about the aggregate port and LACP, see the *Configuring Aggregate Interface*.

Configuration Step

Configuring the Port Path Cost

- Optional.
- To determine the port or path where data packets are forwarded preferentially, configure the port path cost.

Command	**spanning-tree** [**mst** *instance-id*] **cost** *cost*
Parameter Description	**mst** *instance-id*: Indicates the ID of an MSTI. The value range is from 0 to 64. The default value is 0. **cost** *cost*: Indicates the path cost. The value range is from 1 to 200,000,000.
Defaults	The port path cost is automatically calculated based on the link rate by default. For example, the port path cost of a 1000 Mbps port is 20,000, the port path cost of a 100 Mbps port is 200,000, and the port path cost of a 10 Mbps port is 2,000,000.
Command Mode	Interface configuration mode
Usage Guide	A larger value of *cost* indicates a higher path cost.

Configuring the Default Path Cost Calculation Method

- Optional.
- To change the path cost calculation method, configure the default path cost calculation method.

Command	**spanning-tree pathcost method** { *long* | **long** *standard* | *short* }
Parameter Description	*long*: Uses the path cost specified in 802.1t Long. *standard*: Calculates the cost according to the formula recommended in IEEE 802.1t Long Standard. *short*: Uses the path cost specified in 802.1d Short.
Defaults	The default port path cost calculation method is **long**.
Command Mode	Global configuration mode
Usage Guide	If the port path cost uses the default value, the device automatically calculates the port path cost based on the port rate.

Verification

- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Configuring the Port Path Cost

Scenario **Figure 1-23**	
Configuration Steps	● Configure the bridge priority so that Device A becomes the root bridge of the spanning tree. ● Configure the path cost of GigabitEthernet 0/2 on Device B is 1 so that GigabitEthernet 0/2 can be selected as the root port.
Device A	`Hostname(config)#spanning-tree` `Hostname(config)#spanning-tree mst 0 priority 0`

Device B	`Hostname(config)#spanning-tree`
	`Hostname(config)#interface gigabitethernet 0/2`
	`Hostname(config-if-GigabitEthernet 0/2)# spanning-tree cost 1`

Verification	● Run the **show spanning-tree summary** command to display the topology calculation result of the spanning tree.

Device A	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans map : ALL`
	`  Root ID    Priority    0`
	`             Address     00d0.f822.3344`
	`             this bridge is root`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`  Bridge ID  Priority    0`
	`             Address     00d0.f822.3344`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`Interface        Role Sts Cost       Prio     OperEdge Type`
	`---------------- ---- --- ---------- -------- -------- ----------------`
	`Gi0/2            Desg FWD 20000      128      False    P2p`
	`Gi0/1            Desg FWD 20000      128      False    P2p`

Device B	`Hostname#show spanning-tree summary`
	
	`Spanning tree enabled protocol mstp`
	`MST 0 vlans map : ALL`
	`  Root ID    Priority    0`
	`             Address     00d0.f822.3344`
	`             this bridge is root`
	`             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec`
	
	`  Bridge ID  Priority    32768`

```
             Address     001a.a917.78cc
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface        Role Sts Cost       Prio     OperEdge Type
---------------- ---- --- ---------- -------- -------- ----------------
Gi0/2            Root FWD 1          128      False    P2p
Gi0/1            Altn BLK 20000      128      False    P2p
```

Common Errors

The changed port path cost will take effect only on the receive port.

1.4.7 Configuring the Maximum Hop Count of a BPDU

Configuration Effect

- Configuring the maximum hop count of a BPDU will change the BPDU TTL and affect the network topology.

Notes

- The default maximum hop count of a BPDU is 20. You are advised not to change the default value in most situations.

Configuration Step

↘ Configuring the Maximum Hop Count

- Optional. For a large network topology, if a BPDU is transmitted for more than 20 hops, you are advised to change the maximum hop count.

Command	**spanning-tree max-hops** *hop-count*
Parameter Description	*hop-count*: Indicates the number of devices a BPDU passes through before the BPDU is discarded. The value range is from 1 to 40.
Defaults	The maximum hop count for a BPDU is 20 by default.
Command Mode	Global configuration mode
Usage Guide	In a region, the BPDU sent by the root bridge includes a hop count. Every time a BPDU passes through a device from the root bridge, the hop count decreases by 1. When the hop count becomes 0, the BPDU times out and the device discards the packet. This command specifies the number of devices a BPDU passes through in a region before the BPDU is discarded. Changing the maximum hop count will affect all MSTIs.

Verification

- Run the **show spanning-tree max-hops** command to display the maximum hop count.

Configuration Example

↘ Configuring the Maximum Hop Count of a BPDU

Configuration	● Set the maximum hop count of a BPDU to 25.

Steps	
	`Hostname(config)# spanning-tree max-hops 25`
Verification	● Run the **show spanning-tree** command to display the configuration.

	`Hostname# show spanning-tree`
	`StpVersion : MSTP`
	`SysStpStatus : ENABLED`
	`MaxAge : 20`
	`HelloTime : 2`
	`ForwardDelay : 15`
	`BridgeMaxAge : 20`
	`BridgeHelloTime : 2`
	`BridgeForwardDelay : 15`
	`MaxHops: 25`
	`TxHoldCount : 3`
	`PathCostMethod : Long`
	`BPDUGuard : Disabled`
	`BPDUFilter : Disabled`
	`LoopGuardDef : Disabled`
	
	`###### mst 0 vlans map : ALL`
	`BridgeAddr : 00d0.f822.3344`
	`Priority: 0`
	`TimeSinceTopologyChange : 2d:0h:46m:4s`
	`TopologyChanges : 25`
	`DesignatedRoot : 0.001a.a917.78cc`
	`RootCost : 0`
	`RootPort : GigabitEthernet 0/1`
	`CistRegionRoot : 0.001a.a917.78cc`
	`CistPathCost : 20000`

1.4.8 Enabling the Edge Port

Configuration Effect

- After a port is configured as the edge port, the port directly enters the forwarding state. When the port receives BPDUs, its Port Fast Operational State becomes disabled. In this case, the port can properly run the STP algorithm and enter the forwarding state.
- If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU.
- If BPDU filter is enabled on a port, the port does not send or receive BPDUs.

Notes

- Global BPDU guard takes effect only when the port is configured as the edge port.

- If BPDU filter is enabled globally, the edge port does not send or receive BPDUs. In this case, the host directly connected to the edge port does not receive any BPDUs. If the port changes its Port Fast Operational State to Disabled after receiving a BPDU, BPDU filter automatically becomes ineffective.
- Global BPDU filter takes effect only when the port is configured as the edge port.

Configuration Step

Enabling the Edge Port

- Optional.
- If a port connects directly to a network terminal, configure this port as an edge port.
- In global configuration mode, run the **spanning-tree portfast default** command to enable the edge port on all ports and the **no spanning-tree portfast default** command to disable the edge port on all ports.
- In interface configuration mode, run the **spanning-tree portfast** command to enable the edge port on a port and the **spanning-tree portfast disabled** command to disable the edge port on a port.

Command	**spanning-tree portfast default**
Parameter Description	N/A
Defaults	All ports are non-edge ports by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**spanning-tree portfast**
Parameter Description	N/A
Defaults	Ports are non-edge ports by default.
Command Mode	Interface configuration mode
Usage Guide	After a port is configured as the edge port, the port directly enters the forwarding state. When the port receives BPDUs, its Port Fast Operational State becomes disabled. In this case, the port can properly run the STP algorithm and enter the forwarding state.

Enabling BPDU Guard

- Optional.
- When device ports directly connect to network terminals, BPDU attacks on the ports may cause exceptions in the spanning tree topology. To prevent such attacks, you can enable BPDU guard on the ports. A port enabled with BPDU guard enters the error-disabled state after receiving a BPDU.
- If device ports directly connect to network terminals, you can enable BPDU guard to prevent loops on the ports. The prerequisite is that the downlink device (such as the hub) can forward BPDUs.
- In global configuration mode, run the **spanning-tree portfast bpduguard default** command to enable BPDU guard on all ports and the **no spanning-tree portfast bpduguard default** command to disable BPDU guard on all ports.

- In interface configuration mode, run the **spanning-tree bpduguard enable** command to enable BPDU guard on a port and the **spanning-tree bpduguard disabled** command to disable BPDU guard on a port.

Command	**spanning-tree portfast bpduguard default**
Parameter Description	N/A
Defaults	The global BPDU guard function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	If BPDU guard is enabled on a port, the port enters the error-disabled state after receiving a BPDU. Run the **show spanning-tree** command to display the configuration.

Command	**spanning-tree bpduguard enable**
Parameter Description	N/A
Defaults	BPDU guard is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	If BPDU guard is enabled on a port, the port enters the Error-Disabled state after receiving a BPDU.

Enabling BPDU Filter

- Optional.
- To prevent abnormal BPDUs from affecting the spanning tree topology, you can enable BPDU filter on a port to filter abnormal BPDUs.
- In global configuration mode, run the **spanning-tree portfast bpdufilter default** command to enable BPDU filter on all ports and the **no spanning-tree portfast bpdufilter default** command to disable BPDU filter on all ports.
- In interface configuration mode, run the **spanning-tree bpdufilter enable** command to enable BPDU filter on a port and the **spanning-tree bpdufilter disabled** command to disable BPDU filter on a port.

Command	**spanning-tree portfast bpdufilter default**
Parameter Description	N/A
Defaults	The global BPDU filter function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	If BPDU filter is enabled, corresponding ports do not send or receive BPDUs.

Command	**spanning-tree bpdufilter enable**
Parameter Description	N/A
Defaults	BPDU filter is disabled on a port by default.
Command Mode	Interface configuration mode

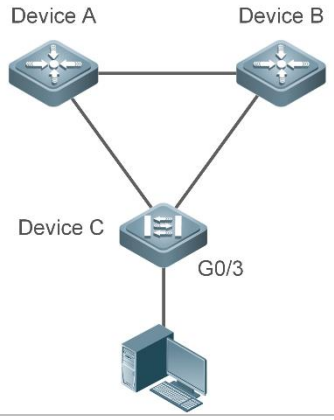
Usage Guide	If BPDU filter is enabled on a port, the port does not send or receives BPDUs.

Verification

- Run the **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id* command to display the spanning tree configuration of the port.

Configuration Example

Enabling the Edge Port

Scenario **Figure 1-24**	
Configuration Steps	● Configure GigabitEthernet 0/3 of Device C as an edge port and enable BPDU guard.

Device C	`Hostname(config)#interface gigabitethernet 0/3`
	`Hostname(config-if-GigabitEthernet 0/3)# spanning-tree portfast`
	`%Warning: portfast should only be enabled on ports connected to a single host. Connecting hubs, switches, bridges to this interface when portfast is enabled, can cause temporary loops.`
	`Hostname(config-if-GigabitEthernet 0/3)#spanning-tree bpduguard enable`

Verification	● Run the **show spanning-tree interface** command to display the port configuration.

Device C	`Hostname#show spanning-tree interface gigabitethernet 0/3`
	
	`PortAdminPortFast : Enabled`
	`PortOperPortFast : Enabled`
	`PortAdminAutoEdge : Enabled`
	`PortOperAutoEdge : Enabled`
	`PortAdminLinkType : auto`
	`PortOperLinkType : point-to-point`
	`PortBPDUGuard : Enabled`
	`PortBPDUFilter : Disabled`
	`PortGuardmode : None`
	
	`###### MST 0 vlans mapped :ALL`
	`PortState : forwarding`
	`PortPriority : 128`
	`PortDesignatedRoot : 0.00d0.f822.3344`

	PortDesignatedCost : 0 PortDesignatedBridge :0.00d0.f822.3344 PortDesignatedPortPriority : 128 PortDesignatedPort : 4 PortForwardTransitions : 1 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : designatedPort

1.4.9 Enabling TC-related Features

Configuration Effect

- If TC protection is enabled on a port, the port deletes TC BPDUs within a specified time (4s typically) after receiving them, preventing MAC and ARP entry from being deleted.
- If TC guard is enabled, a port receiving TC BPDUs filters TC BPDUs received or generated by itself so that TC BPDUs are not spread to other ports. In this way, possible TC attacks are efficiently prevented to keep the network stable.
- TC filter does not process TC BPDUs received by ports but processes TC BPDUs in case of normal topology changes.

Notes

- You are advised to enable TC guard only when unauthorized TC attack packets are received on a network.

Configuration Step

↘ Enabling TC Protection

- Optional.
- In global configuration mode, run the **spanning-tree tc-protection** command to enable TC protection on all ports and the **no spanning-tree tc-protection** command to disable TC protection on all ports.
- TC protection can be enabled or disabled globally only.

Command	**spanning-tree tc-protection**
Parameter Description	N/A
Defaults	The global TC protection function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Enabling TC Guard

- Optional.
- To filter received TC BPDUs or those generated on the local port due to topology changes, you can configure TC guard for the port.

- In global configuration mode, run the **spanning-tree tc-protection tc-guard** command to enable TC guard on all ports and the **no spanning-tree tc-protection tc-guard** command to disable TC guard on all ports.
- In interface configuration mode, run the **spanning-tree tc-guard** command to enable TC guard on a port and the **no spanning-tree tc-guard** command to disable TC guard on a port.

Command	**spanning-tree tc-protection tc-guard**
Parameter Description	N/A
Defaults	The global TC guard function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Enable TC guard to prevent TC BPDUs from being spread.

Command	**spanning-tree tc-guard**
Parameter Description	N/A
Defaults	TC guard is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	Enable TC guard to prevent TC BPDUs from being spread.

Enabling TC Filter

- Optional.
- TC filter is disabled by default.
- To filter TC BPDUs received on a port, you can enable TC filter on the port.
- In interface configuration mode, run the **spanning-tree ignore tc** command to enable TC filter on a port and the **no spanning-tree ignore tc** command to disable TC filter on a port.

Command	**spanning-tree ignore tc**
Parameter Description	N/A
Defaults	TC filter is disabled by default.
Command Mode	Interface configuration mode
Usage Guide	If TC filter is enabled on a port, the port does not process received TC BPDUs.

Verification

- Display the configuration.

Configuration Example

Enabling TC Guard on a Port

Configuration Steps	• Enable TC guard on a port.

	Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#spanning-tree tc-guard
Verification	● Run the **show run interface** command to display the TC guard configuration of the port.
	Hostname#show run interface gigabitethernet 0/1 Building configuration... Current configuration : 134 bytes interface GigabitEthernet 0/1 switchport mode trunk spanning-tree tc-guard

Common Errors

- If TC guard or TC filter is incorrectly configured, an error may occur during packet forwarding of a network device. For example, when the topology changes, the device fails to delete MAC address in a timely manner, causing packet forwarding errors.

1.4.10 Enabling BPDU Source MAC Address Check

Configuration Effect

- Enable BPDU source MAC address check. Then a device receives only BPDUs with the source MAC address being the specified MAC address and discards other BPDUs.

Notes

- When the switch connected to a port on a point-to-point link is determined, you can enable BPDU source MAC address check so that the switch receives the BPDUs sent only by the peer switch.

Configuration Step

↘ Enabling BPDU Source MAC Address Check

- Optional.
- To prevent malicious BPDUs, you can enable BPDU source MAC address check.
- In interface configuration mode, run the **bpdu src-mac-check** *mac-address* command to enable BPDU source MAC address check on a port and the **no bpdu src-mac-check** command to disable BPDU source check on a port.

Command	**bpdu src-mac-check** *mac-address*
Parameter Description	*mac-address*: Indicates that only BPDUs from this MAC address can be received.
Command Mode	BPDU source MAC address check is disabled on a port by default.
Usage Guide	Interface configuration mode
	BPDU source MAC address check is enabled to prevent a switch from malicious attacks generated by manually sending BPDUs and further prevent MSTP from malfunction. To prevent malicious

	attacks, when the peer switch on the point-to-point link of a port is determined, you can enable BPDU source MAC address check so that the switch receives the BPDUs sent only by the peer switch and discards all other BPDUs. In interface configuration mode, you can configure a MAC address corresponding to the BPDU source MAC address check for a specific port. Only one MAC address can be configured on one port.

Verification

- Display the configuration.

Configuration Example

Enabling BPDU Source MAC Address Check on a Port

Configuration Steps	● Enable BPDU source MAC address check on a port.
	`Hostname(config)#interface gigabitethernet 0/1` `Hostname(config-if-GigabitEthernet 0/1)#bpdu src-mac-check 00d0.f800.1234`
Verification	● Run the **show run interface** command to display the spanning tree configuration of the port.

	`Hostname#show run interface gigabitethernet 0/1`
	
	`Building configuration...`
	`Current configuration : 170 bytes`
	
	`interface GigabitEthernet 0/1`
	` switchport mode trunk`
	` bpdu src-mac-check 00d0.f800.1234`
	`spanning-tree link-type point-to-point`

Common Errors

- If BPDU source MAC address check is enabled on a port, the port receives only BPDUs with the configured MAC address being the source MAC address and discards all other BPDUs.

1.4.11 Configuring Auto Edge

Configuration Effect

- Enable Auto Edge. If a designated port does not receive any BPDUs within a specified time (3s), it is automatically identified as an edge port. However, if the port receives BPDUs, its Port Fast Operational State will become Disabled.

Notes

- Unless otherwise specified, do not disable Auto Edge.

Configuration Steps

Configuring Auto Edge

- Optional.

- In interface configuration mode, run the **spanning-tree autoedge** command to enable Auto Edge on a port and the **spanning-tree autoedge disabled** command to disable Auto Edge on a port.

Command	**spanning-tree autoedge**
Parameter Description	N/A
Defaults	Auto Edge is enabled on a designated port by default.
Command Mode	Interface configuration mode
Usage Guide	If the designated port of a device does not receive a BPDU from the downlink port within a specific period (3s), the device considers that a network device is connected to the designated port, configures the port as an edge port, and switches the port directly into the forwarding state. The edge port will be automatically identified as a non-edge port after receiving a BPDU. You can run the **spanning-tree autoedge disabled** command to disable Auto Edge.

Verification

- Display the configuration.

Configuration Example

↘ Disabling Auto Edge on a Port

Configuration Steps	- Disable Auto Edge on a port.
	`Hostname(config)#interface gigabitethernet 0/1` `Hostname(config-if-GigabitEthernet 0/1)#spanning-tree autoedge disabled`
Verification	- Run the **show spanning-tree interface** command to display the spanning tree configuration of the port.

	`Hostname#show spanning-tree interface gigabitethernet 0/1`
	
	`PortAdminPortFast : Disabled`
	`PortOperPortFast : Disabled`
	`PortAdminAutoEdge : Disabled`
	`PortOperAutoEdge : Disabled`
	`PortAdminLinkType : point-to-point`
	`PortOperLinkType : point-to-point`
	`PortBPDUGuard : Disabled`
	`PortBPDUFilter : Disabled`
	`PortGuardmode : None`
	
	`###### MST 0 vlans mapped :ALL`
	`PortState : forwarding`
	`PortPriority : 128`
	`PortDesignatedRoot : 0.00d0.f822.3344`
	`PortDesignatedCost : 0`

	PortDesignatedBridge :0.00d0.f822.3344 PortDesignatedPortPriority : 128 PortDesignatedPort : 2 PortForwardTransitions : 6 PortAdminPathCost : 20000 PortOperPathCost : 20000 Inconsistent states : normal PortRole : designatedPort

Common Errors

- If Auto Edge is enabled on a designated port and the designated port does not receive a BPDU within 3s, the port is identified as an edge port and immediately enters the forwarding state by default. If packet loss or packet sending/receiving delay exists, you are advised to disable Auto Edge.

1.4.12 Enabling Guard-related Features

Configuration Effect

- If root guard is enabled on a port, its roles in all MSTIs are forcibly used as the designated port. Once the port receives the configuration with a higher priority, it enters the root-inconsistent (blocking) state. If the port does not receive the configuration with a higher priority within a period, it returns to its original state.
- Due to the unidirectional link failure, the root port or backup port becomes the designated port and enters the forwarding state if it does not receive BPDUs, causing a network loop. Loop guard is used to prevent this problem.

Notes

- Root guard and loop guard cannot be configured on a port simultaneously.

Configuration Step

↘ Enabling Root Guard

- Optional.
- The root bridge may receive the configuration with a higher priority due to incorrect configuration by maintenance personnel or malicious attacks on a network. As a result, the root bridge may lose its role, causing incorrect topology changes. To prevent this problem, you can enable root guard on a designated port of a device.
- In interface configuration mode, run the **spanning-tree guard root** command to enable root guard on a port and the **no spanning-tree guard root** command to disable root guard on a port.

Command	**spanning-tree guard root**
Parameter Description	N/A
Defaults	Root guard is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	If root guard is enabled, the root bridge will not change due to incorrect configuration or unauthorized packet attacks.

Enabling Loop Guard

- Optional.
- You can enable loop guard on a port (root port, master port, or aggregate port) to prevent it from failing to receive BPDUs sent by the designated bridge, increasing device stability. Otherwise, the network topology will change, possibly causing a loop.
- In global configuration mode, run the **spanning-tree loopguard default** command to enable loop guard on all ports and the **no spanning-tree loopguard default** command to disable root guard on all ports.
- In interface configuration mode, run the **spanning-tree guard loop** command to enable root guard on a port and the **no spanning-tree guard loop** command to disable root guard on a port.

Command	**spanning-tree loopguard default**
Parameter Description	N/A
Defaults	The global loop guard function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	Enabling loop guard on a root port or backup port can prevent possible loops caused by BPDU receiving failures.

Command	**spanning-tree guard loop**
Parameter Description	N/A
Defaults	Loop guard is disabled on a port by default.
Command Mode	Interface configuration mode
Usage Guide	Enabling loop guard on a root port or backup port will prevent possible loops caused by BPDU receiving failures.

Disabling Guard

- Optional.

Command	**spanning-tree guard none**
Parameter Description	N/A
Defaults	By default, the guard function is not configured on a port.
Command Mode	Interface configuration mode
Usage Guide	N/A

Verification

- Display the configuration.

Configuration Example

Enabling Loop Guard on a Port

Scenario **Figure 1-25**	
Configuration Steps	● Configure Device A as the root bridge and Device B as a non-root bridge in a spanning tree. ● Enable loop guard on GigabitEthernet 0/1 and GigabitEthernet 0/2 of Device B.
Device A	`Hostname(config)#spanning-tree` `Hostname(config)#spanning-tree mst 0 priority 0`

Device B	`Hostname(config)#spanning-tree`
	`Hostname(config)#interface range gigabitethernet 0/1-2`
	`Hostname(config-if-range)#spanning-tree guard loop`

Verification	● Run the **show spanning-tree interface** command to display the spanning tree configuration of the port.
Device A	Omitted.

Device B	`Hostname#show spanning-tree interface gigabitethernet 0/1`
	
	`PortAdminPortFast : Disabled`
	`PortOperPortFast : Disabled`
	`PortAdminAutoEdge : Enabled`
	`PortOperAutoEdge : Disabled`
	`PortAdminLinkType : auto`
	`PortOperLinkType : point-to-point`
	`PortBPDUGuard : Disabled`
	`PortBPDUFilter : Disabled`
	`PortGuardmode  : Guard loop`
	
	`###### MST 0 vlans mapped :ALL`
	`PortState : forwarding`
	`PortPriority : 128`
	`PortDesignatedRoot : 0.001a.a917.78cc`
	`PortDesignatedCost : 0`
	`PortDesignatedBridge :0.001a.a917.78cc`
	`PortDesignatedPortPriority : 128`
	`PortDesignatedPort : 17`
	`PortForwardTransitions : 1`
	`PortAdminPathCost : 20000`
	`PortOperPathCost : 20000`
	`Inconsistent states : normal`
	`PortRole : rootPort`
	
	`Hostname#show spanning-tree interface gigabitethernet 0/2`

```
PortAdminPortFast : Disabled
PortOperPortFast : Disabled
PortAdminAutoEdge : Enabled
PortOperAutoEdge : Disabled
PortAdminLinkType : auto
PortOperLinkType : point-to-point
PortBPDUGuard : Disabled
PortBPDUFilter : Disabled
PortGuardmode  : Guard loop

###### MST 0 vlans mapped :ALL
PortState : discarding
PortPriority : 128
PortDesignatedRoot : 0.001a.a917.78cc
PortDesignatedCost : 0
PortDesignatedBridge :0.001a.a917.78cc
PortDesignatedPortPriority : 128
PortDesignatedPort : 18
PortForwardTransitions : 1
PortAdminPathCost : 20000
PortOperPathCost : 20000
Inconsistent states : normal
PortRole : alternatePort
```

Common Errors

- If root guard is enabled on the root port, master port, or aggregate port, the port may be incorrectly blocked.

1.4.13 Enabling BPDU Transparent Transmission

Configuration Effect

- If STP is disabled on a device, the device needs to transparently transmit BPDUs so that the spanning tree between devices is properly calculated.

Notes

- BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDUs.

Configuration Step

↘ Enabling BPDU Transparent Transmission

- Optional.
- If STP is disabled on a device that needs to transparently transmit BPDUs, enable BPDU transparent transmission.

- In global configuration mode, run the **bridge-frame forwarding protocol bpdu** command to enable BPDU transparent transmission and the **no bridge-frame forwarding protocol bpdu** command to disable BPDU transparent transmission.
- BPDU transparent transmission can be enabled only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDUs.

Command	**bridge-frame forwarding protocol bpdu**
Parameter Description	N/A
Defaults	BPDU transparent transmission is disabled by default.
Command Mode	Global configuration mode
Usage Guide	In IEEE 802.1Q, the destination MAC address 01-80-C2-00-00-00 of the BPDU is used as a reserved address. That is, devices compliance with IEEE 802.1Q do not forward the BPDUs received. However, devices may need to transparently transmit BPDUs in practice. For example, if STP is disabled on a device, the device needs to transparently transmit BPDUs so that the spanning tree between devices is properly calculated. BPDU transparent transmission takes effect only when STP is disabled. If STP is enabled on a device, the device does not transparently transmit BPDUs.

Verification

- Display the configuration.

Configuration Example

Enabling BPDU Transparent Transmission

Scenario **Figure 1-26**	
	● STP is enabled on Device A and Device C while is disabled on Device B.
Configuration Steps	● Enable BPDU transparent transmission on Device B so that STP between Device A and Device C can be correctly calculated.
Device B	`Hostname(config)#bridge-frame forwarding protocol bpdu`
Verification	● Run the **show running-config** command to check whether BPDU transparent transmission is enabled.

Device B	`Hostname#show running-config`
	
	`Building configuration...`
	`Current configuration : 694 bytes`
	`bridge-frame forwarding protocol bpdu`

1.5 Monitoring

Clearing

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

Command	Description
clear spanning-tree counters [**interface** *interface-type interface-number*]	Clears statistics of packets sent and received on a port.
clear spanning-tree mst *instance-id* **topochange record**	Clears STP topology change information.

Displaying

Command	Description
show spanning-tree	Displays MSTP parameters and spanning tree topology information.
show spanning-tree counters	Displays statistics on sent and received BPDUs.
show spanning-tree forward-time	Displays the port status change interval.
show spanning-tree hello time	Displays the interval for periodically sending BPDUs.
show spanning-tree inconsistentports	Displays ports blocked due to root guard or loop guard.
show spanning-tree max-age	Displays the maximum timeout time of a BPDU.
show spanning-tree max-hops	Displays the maximum hop count of BPDUs.
show spanning-tree mst *instance-id*	Displays the global spanning tree configuration of a specified MSTI.
show spanning-tree pathcost method	Displays the path cost calculation method.
show spanning-tree summary	Displays the spanning tree topology and port forwarding status information.
show spanning-tree tx-hold-count	Displays the maximum number of BPDUs that can be sent every second.
show spanning-tree [**mst** *instance-id*] **interface** *interface-type interface-number* [**bpdufilter** | **bpduguard** | **link-type** | **portfast**]	Displays the spanning tree configuration and status information of a port.
show spanning-tree mst configuration	Displays the MST region configuration.
show spanning-tree mst *instance-id* **topochange record**	Displays the topology change information of a port in a specified MSTI.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug mstp all	Debugs all MSTP functions.
debug mstp gr	Debugs the MSTP GR function.
debug mstp rx	Debugs the BPDU receiving.
debug mstp tx	Debugs BPDU transmission.
debug mstp event	Debugs MSTP events.

Command	Description
debug mstp loopguard	Debugs MSTP loop guard.
debug mstp rootguard	Debugs MSTP root guard.
debug mstp bridgedetect	Debugs the bridge detect state machine.
debug mstp portinfo	Debugs the port information state machine.
debug mstp protomigrat	Debugs the port protocol migration state machine.
debug mstp topochange	Debugs MSTP topology changes.
debug mstp receive	Debugs the MSTP receiving state machine.
debug mstp roletran	Debugs the port role transition state machine.
debug mstp statetran	Debugs the port state transition state machine.
debug mstp transmit	Debugs the MSTP transmission state machine.

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 Client
8. Configuring DNS Snooping
9. Configuring Bonjour Gateway
10. Configuring IPv6 Basics
11. Configuring DHCPv6
12. Configuring DHCPv6 Snooping
13. Configuring ND Snooping
14. Configuring ND Proxy
15. Configuring Tunnel
16. Configuring TCP
17. Configuring IP REF
18. Configuring FPM
19. Configuring SAVI

1 Configuring ARP

1.1 Overview

On a local area network (LAN), each IP network device has two addresses:

- Local address: The local address, found in the header of the data link layer (DLL) frame, is referred to as a DLL address. However, it is typically known as the MAC address as it is processed by the MAC sublayer within the DLL, and it uniquely identifies an IP network device on a LAN.
- Network address. Network addresses on the Internet represent IP network devices and also indicate the networks where the devices reside.

On 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:

- Address Resolution Protocol (ARP), which is defined in RFC 826
- Proxy ARP, which is defined in RFC 1027

ARP is used to bind MAC addresses to IP addresses. 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 a 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 MAC addresses of other users on the same network segment through ARP.
Proxy ARP-based Transparent Transmission	With proxy ARP, a user can directly communicate with users on another network without knowing such a network.

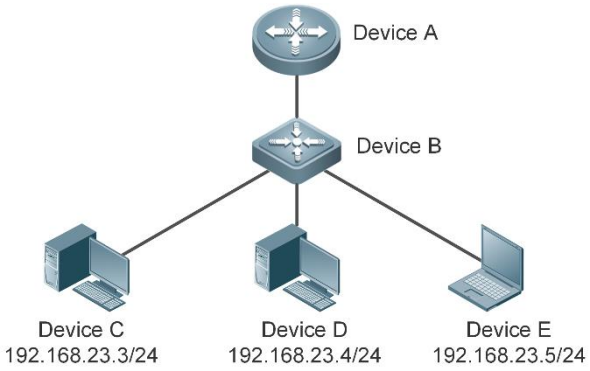
1.2.1 LAN-based ARP

Scenario

ARP is required on all IPv4 LANs.

- A user needs to learn MAC addresses of other users through ARP to communicate with them.

Figure 1-1



Remarks	Device A is a router. Device B is the gateway of the network segment where terminals reside. Device C, Device D, and Device E are hosts.

Deployment

- Enable ARP on a LAN to implement IP-MAC mapping.

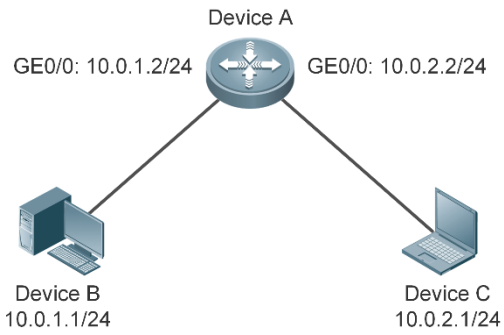
1.2.2 Proxy ARP-based Transparent Transmission

Scenario

Transparent transmission across IPv4 LANs is performed.

- Enable proxy ARP on the router to achieve direct communication between users on different network segments.

Figure 1-2



Remarks	Device A is connected to two LANs. Device B and Device C are hosts on different subnets. No default gateway is configured for them.

Deployment

- Enable proxy ARP on the subnet gateway. Then the gateway can act as a proxy to enable a host without any route information to obtain MAC addresses of IP users in other subnets.

1.3 Features

Overview

Feature	Description
Static ARP	You can manually specify IP-MAC mapping to prevent the device from learning incorrect ARP entries.
ARP Attributes	You can specify the ARP entry timeout, ARP request retransmission count and interval, and maximum number of unresolved ARP entries.
Trusted ARP	Trusted ARP is used to prevent ARP spoofing.
Gratuitous ARP	Gratuitous ARP is used to detect IP address conflicts and enable peripheral devices to update ARP entries.
Proxy ARP	A proxy replies to ARP request packets from other devices in different subnets.
Local Proxy ARP	A proxy replies to ARP request packets from other devices in the same subnet.
ARP Trustworthiness Detection	Neighbor Unreachable Detection (NUD) is used to ensure that correct ARP entries are learned.
Determing Host Existence Prior to ARP Proxy Service Provision	The Virtual Router Redundancy Protocol (VRRP) master responds to an ARP request packet as a proxy only when the destination IP address has been resolved.
ARP Packet Statistics Collection	ARP packet statistics are displayed.
Sending ARP Request Packets to a Specified Sub-VLAN of a Super-VLAN	In gateway authentication mode, dump terminals in a super-VLAN are deployed in authenticated VLANs, and the device proactively sends ARP request packets to a specific VLAN.

1.3.1 Static ARP

Static ARP entries can be configured manually or assigned by the authentication server. The manually configured ARP entries take precedence over delivered static ARP entries. Static ARP can prevent the device from learning incorrect ARP entries.

Working Principle

If static ARP entries are configured, the device does not proactively 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 Ethernet II, which is represented by ARPA.

1.3.2 ARP Attributes

You can specify the ARP timeout, ARP request retransmission count and interval, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a card.

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 packet 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 more network bandwidth is consumed.

ARP Request Retransmission Interval and Count

The device consecutively sends ARP request packets to resolve an IP address into a MAC address. A shorter retransmission interval speeds up resolution, while a higher retransmission count increases the likelihood of successfully resolving ARP entries at the expense of more bandwidth.

Maximum Number of Unresolved ARP Entries

On a LAN, ARP attacks and scanning may cause a large number of unresolved ARP entries to be generated on a gateway. As a result, the gateway fails to learn MAC addresses of users. To prevent such attacks, you can configure the maximum number of unresolved ARP entries.

Maximum Number of ARP Entries on an Interface

Configure the maximum number of ARP entries on a specified interface to prevent a waste of ARP entry resources.

Related Configuration

Configuring the ARP Timeout

Run the **arp timeout** *seconds* command in interface configuration mode to configure the ARP timeout. The default value is 3600s. You can change it as needed.

Configuring the ARP Request Retransmission Interval and Count

- Run the **arp retry interval** *seconds* command in global configuration mode to configure the ARP request retransmission interval. The default interval is 1s. You can change it as needed.
- Run the **arp retry times** *number* command in global configuration mode to configure the ARP request retransmission count. The default retransmission count is 5. You can change it as needed.

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 as needed.

Configuring the Maximum Number of ARP Entries on an Interface

Run the **arp cache interface-limit** *limit* command in interface configuration mode to configure the maximum number of ARP entries learned on an interface. The default number is 0. You can change it as needed. This command also applies to static ARP entries.

1.3.3 Trusted ARP

Working Principle

Trusted ARP entries are a special type added to the ARP table to prevent ARP spoofing. Trusted ARP entries blend characteristics of both static and dynamic ARP entries, with a priority higher than that of dynamic ARP entries but lower than that of static ARP entries. Trusted ARP has an aging mechanism similar to that of dynamic ARP. When an ARP entry ages, the device proactively sends an ARP request packet to detect whether the corresponding user exists. If the user sends a reply packet, the device considers the user active and updates the ARP timeout. Otherwise, the device deletes the ARP entry. Trusted ARP has characteristics of static ARP, that is, the device does not learn ARP packets to update the MAC address and interface ID in the ARP entry.

When a user goes online on a GSN client, the authentication server obtains the user's reliable IP-MAC mapping through the access switch, and adds trusted ARP entries to the user's gateway. This process is transparent to the network administrator and does not affect the administrator’s work on network management.

Since trusted ARP entries come from authentic sources and will not be updated, they can efficiently prevent ARP spoofing targeted at the gateway.

Related Configuration

Enabling Trusted ARP

- Run the **service trustedarp** command in global configuration mode to enable trusted ARP. This function is disabled by default.
- Run the **arp trusted user-vlan** *vid1* **translated-vlan** *vid2* command in global configuration mode to implement VLAN redirection. This function is disabled by default. If the VLAN pushed by the server differs from the VLAN in the trusted ARP entry, enable VLAN redirection.
- Run the **arp trusted aging** command in global configuration mode to enable ARP aging. Trusted ARP entries are not aged by default.
- Run the **arp trusted number** command in global configuration mode to configure the capacity of trusted ARP entries. The default value is half of the total capacity of ARP entries. You can change it as needed.

1.3.4 Gratuitous ARP

Working Principle

Gratuitous ARP packets are a special type of ARP packets where both the source and destination IP addresses are that of the local device. These packets serve two main purposes:

1 IP address conflict detection: If the device receives a gratuitous packet and finds the IP address in the packet the same as its own IP address, it sends an ARP reply packet to notify the peer end of the IP address conflict.

2 ARP update: When the MAC address of an interface changes, the device sends a gratuitous ARP packet to instruct other devices to update ARP entries.

The device can learn gratuitous ARP packets. After receiving a gratuitous ARP packet, the device checks whether the corresponding dynamic ARP entry exists. If so, the device updates the ARP entry based on information carried in the gratuitous ARP packet.

Related Configuration

Enabling Gratuitous ARP

Run the **arp gratuitous-send interval** *seconds* [*number*] command in interface configuration mode to enable gratuitous ARP. This function is disabled on interfaces by default. Typically, you need to enable this function on the gateway interface to periodically update the MAC address of the gateway on downlink devices, which prevents forged gateways.

1.3.5 Proxy ARP

Working Principle

The device enabled with proxy ARP can help a host without any routing information to obtain MAC addresses of IP users in other subnets. For example, if the device receiving an ARP request finds the source IP address on a different network segment from the destination IP address and knows the route to the destination address, the device sends an ARP reply packet containing its own Ethernet MAC address.

Related Configuration

↘ Enabling Proxy ARP

- Run the **ip proxy-arp** command in interface configuration mode to enable proxy ARP.

1.3.6 Local Proxy ARP

Working Principle

Local proxy ARP means that a device acts as a proxy in the local VLAN (common VLAN or sub VLAN).

After local proxy ARP is enabled, the device can help users to obtain MAC addresses of other users within the same subnet. For example, when port protection is enabled on the device, users connected to different ports are isolated at Layer 2. After local proxy ARP is enabled, the device receiving an ARP request packet acts as a proxy to send an ARP reply packet containing its own Ethernet MAC address. In this case, different users communicate with each other through Layer 3 routes.

Related Configuration

↘ Enabling Local Proxy ARP

- Run the **local-proxy-arp** command in interface configuration mode to enable local proxy ARP.
- This function is disabled by default.
- This command is supported only on switch virtual interfaces (SVIs).

1.3.7 ARP Trustworthiness Detection

Working Principle

The **arp trust-monitor enable** command is used to enable ARP anti-spoofing to prevent excessive useless ARP entries from occupying device resources. After ARP trustworthiness detection is enabled on a Layer 3 interface, the device receives ARP request packets from this interface:

1 If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs NUD after 1s to 5s. That is, the device begins to age the newly learned ARP entry and sends a unicast ARP request packet. If the

device receives an ARP update packet from the peer end within the aging time, it stores the entry. If not, it deletes the entry.

2 If the corresponding ARP entry exists, NUD is not performed.

3 If the MAC address in the existing dynamic ARP entry is updated, the device also performs NUD.

Because this function introduces a strict confirmation procedure into the ARP learning process, it impacts the efficiency of ARP learning.

After this function is disabled, NUD is not required for learning and updating ARP entries.

Related Configuration

Enabling ARP Trustworthiness Detection

Run the **arp trust-monitor enable** command in interface configuration mode to enable ARP trustworthiness detection. This function is disabled by default.

1.3.8 Determing Host Existence Prior to ARP Proxy Service Provisioning

Supported functions are subject to the product version.

Working Principle

When two devices form a VRRP group and enabled with local ARP proxy, if the VRRP backup device sends an ARP request packet to a terminal, the VRRP master device will act as a proxy of the terminal and send an ARP reply packet to the VRRP backup device regardless of whether the terminal exists. As a result, the VRRP master device learns a large number of proxy ARP entries.

After the **arp proxy-resolved** command is configured, the VRRP master device first determines whether the ARP entry corresponding to the destination IP address exists upon receiving an ARP request packet. If such an entry exists, the VRRP master device acts as an ARP proxy; if not, it does not. Additionally, the gateway automatically broadcasts an ARP request packet to obtain the ARP entry for the destination IP address. This prevents situations where the gateway fails to act as a proxy and respond to ARP request packets for the destination IP address due to the absence of the corresponding ARP entry.

After the **no arp proxy-resolved** command is configured, if proxy conditions are met, the VRRP master device directly acts as a proxy upon receiving an ARP request packet, without determining whether the ARP entry corresponding to the destination IP address has been resolved.

Related Configuration

Configuring a Device Not to Determine Existence of the ARP Entry Corresponding to a Destination IP Address When the Device Responds to an ARP Request Packet as an ARP Proxy

- Run the **no arp proxy-resolved** command in global configuration mode.
- The **arp proxy-resolved** command is enabled by default.

1.3.9 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.

1.3.10 Sending ARP Request Packets to a Specified Sub-VLAN of a Super-VLAN

Supported functions are subject to the product version.

Working Principle

When numerous sub-VLANs are present within a super-VLAN, the device defaults to broadcasting ARP request packets proactively to the super-VLAN. This can result in excessive packet replication due to the high number of sub-VLANs, potentially impacting device performance.

Most terminals (such as PCs and servers) request ARP information from the gateway before accessing the network. Therefore, there is no need for the device to proactively broadcast ARP request packets to the sub-VLANs where these terminals reside. For dumb terminals that do not proactively send free ARP request packets, run the **arp resolve vlan** *vlan-list* command to configure the device to proactively send ARP request packets to VLANs in the specified VLAN list.

Related Configuration

Configuring the Device to Send ARP Request Packets to a Specific Sub-VLAN of a Super-VLAN

- Run the **arp resolve vlan** *vlan-list* command in global configuration mode to configure the device to send ARP request packets to a specific sub-VLAN of a super-VLAN.
- The device sends ARP request packets to the super-VLAN by default.

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 count, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a card.	
	arp timeout	Configures the ARP timeout.
	arp retry interval	Configures the retransmission interval of ARP request packets.
	arp retry times	Configures the retransmission count of ARP request packets.
	arp unresolve	Configures the maximum number of unresolved ARP entries.
	arp cache interface-limit	Configures the maximum number of ARP entries on an interface.

Configuration	Description and Command	
Enabling Trusted ARP	(Optional) It is used to enable ARP anti-spoofing.	
	service trustedarp	Enables trusted ARP.
	arp trusted user-vlan	Enables VLAN redirection when a trusted ARP entry is added.
	arp trusted aging	Enables trusted ARP aging.
	arp trusted	Configures the capacity of trusted ARP entries.
Enabling Gratuitous ARP	(Optional) It is used to detect IP address conflicts and enables peripheral devices to update ARP entries.	
	arp gratuitous-send interval	Enables gratuitous ARP.
Enabling Proxy ARP	(Optional) It is used to configure the device as a proxy to reply to ARP request packets from devices in different subnets.	
	ip proxy-arp	Enables proxy ARP.
Enabling Local Proxy ARP	(Optional) It is used to configure the device as a proxy to reply to ARP request packets from other devices in the same subnet.	
	local-proxy-arp	Enables local proxy ARP.
Enabling ARP Trustworthiness Detection	(Optional) It is used to configure the device to unicast ARP request packets to ensure that correct ARP entries are learned.	
	arp trust-monitor enable	Enabling ARP trustworthiness detection.
Configuring the Device to Determine Host Existence Prior to ARP Proxy Service Provisioning	(Optional) It is used to configure the VRRP Master Device to Forcibly Respond to ARP Request Packets as a Proxy.	
	no arp proxy-resolved	Configures the VRRP Master Device to Forcibly Respond to ARP Request Packets as a Proxy.
Configuring the Device to Send ARP Request Packets to a Specified Sub-VLAN of a Super-VLAN	(Optional) It is used to configure the device to send ARP request packets to a specified sub-VLAN of a super-VLAN.	
	arp resolve vlan	Configures the device to send ARP request packets to a specified sub-VLAN of a super-VLAN.

1.4.1 Enabling Static ARP

Configuration Effect

You 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 performing Layer 3 routing.

Configuration Step

Configuring Static ARP Entries

- Optional.
- You can configure a static ARP entry to bind the IP address of the uplink device to its MAC address to prevent MAC address change caused by ARP attacks.
- Configure static ARP entries in global configuration mode.

Verification

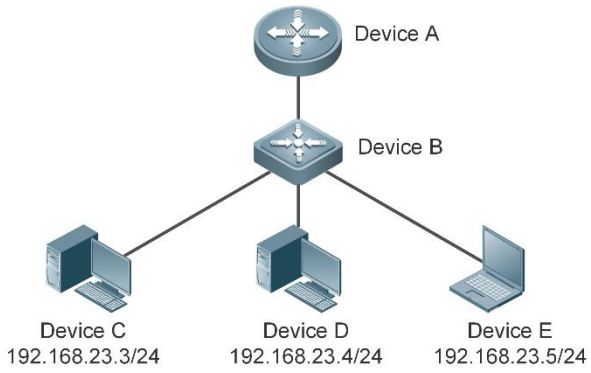
Run the **show running-config** command to check whether the configuration takes effect. Or, run the **show arp static** command to check whether a static ARP cache table is created.

Related Commands

Configuring Static ARP Entries

Command	**arp** *ip-address mac-address type*
Parameter Description	*ip-address*: Indicates the IP address mapped to a MAC address, which is in four-part dotted-decimal format. *mac-address*: Indicates the DLL address, consisting of 48 bits. *type*: Indicates the ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.
Command Mode	Global configuration mode
Usage Guide	The RGOS queries a 48-bit MAC address based on a 32-bit IP address in the ARP cache table. Because most hosts support dynamic ARP resolution, the static ARP mapping are not configured. Use the **clear arp-cache** command to delete dynamic ARP entries.

Configuration Example

Scenario	 ● Device A is the router. ● Device B is the gateway of the network segment where terminals reside. ● Device C, Device D, and Device E are terminals.
Configuration Steps	● Configure a static ARP entry on Device B to statically bind the IP address of Device A to the MAC address. `Hostname(config)#arp 192.168.23.1 00D0.F822.334B arpa`

Verification	● Run the **show arp static** command to display the static ARP entry.
	`Hostname#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

You can specify the ARP timeout, ARP request retransmission interval and count, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a card.

Configuration Step

Configuring the ARP Timeout

- Optional.
- On a LAN, if a user goes online or offline frequently, set a small ARP timeout so that invalid ARP entries can be deleted as soon as possible.
- Configure the ARP timeout in interface configuration mode.

Configuring the ARP Request Retransmission Interval and Count

- Optional.
- If network resources are insufficient, set a large ARP request retransmission interval and a small retransmission count to reduce network bandwidth occupied.
- Configure the ARP request retransmission interval and count in global configuration mode.

Configuring the Maximum Number of Unresolved ARP Entries

- Optional.
- If network resources are insufficient, set the maximum number of unresolved ARP entries to a small value to reduce network bandwidth occupied.
- Configure the maximum number of unresolved ARP entries in global configuration mode.

Configuring the Maximum Number of ARP Entries on an Interface

- Optional.
- Configure the maximum number of ARP entries on an interface in interface configuration mode.

Verification

- Run the **show arp timeout** command to display the timeout of all interfaces.
- Run the **show running-config** command to display the ARP request retransmission interval and count, maximum number of unresolved ARP entries, maximum number of ARP entries on an interface, and maximum number of ARP entries on a card.

Related Commands

Configuring the ARP Timeout

Command	**arp timeout** *seconds*
Parameter Description	*seconds*: Indicates the timeout, in seconds. The value range is from 0 to 2147483. The default value is 3600.
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 more network bandwidth is consumed. Unless otherwise specified, do not configure the ARP timeout.

Configuring the Retransmission Interval of ARP Request Packets

Command	**arp retry interval** *seconds*
Parameter Description	*seconds*: Indicates the retransmission interval of ARP request packets, in seconds. The value range is from 1 to 3600. The default value is 1.
Command Mode	Global configuration mode
Usage Guide	If a device frequently sends ARP request packets, network performance will be affected. You can set a long ARP request retransmission interval. Ensure that this interval does not exceed the ARP timeout.

Configuring the Retransmission Count of ARP Request Packets

Command	**arp retry times** *number*
Parameter Description	number: Indicates the retransmission count of ARP request packets. The value range is 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 a small retransmission count of ARP request packets.

Configuring the Maximum Number of Unresolved ARP Entries

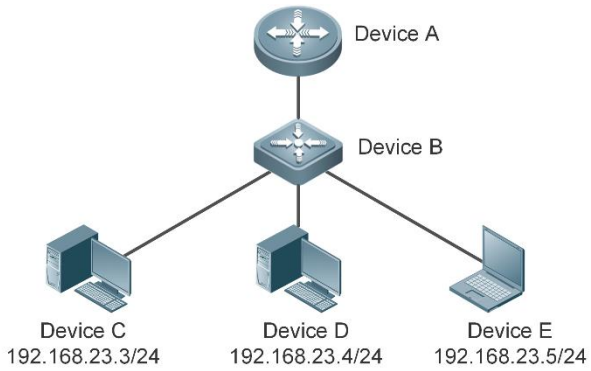
Command	**arp unresolve** *number*
Parameter Description	*number*: Indicates the maximum number of unresolved ARP entries. The value range is from 1 to 8192. The default value is 8192.
Command Mode	Global configuration mode
Usage Guide	If a large number of unresolved entries exist in the ARP cache table and remain in the table after a while, 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.

Configuring the Maximum Number of ARP Entries on an Interface

Command	**arp cache interface-limit** *limit*
Parameter Description	*limit*: Indicates the maximum number of ARP entries that can be learned on an interface, including configured ARP entries and dynamically learned ARP entries. The value range is from 0 to the ARP entry capacity supported by the device. The value 0 indicates that the number of ARP entries that can be learned on an interface is not limited.
Command Mode	Interface configuration mode
Usage Guide	Limiting the number of ARP entries on an interface can prevent malicious ARP attacks from generating excessive ARP entries on the device and occupying entry resources. The configured value must be equal to or greater than the number of the ARP entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ARP entry capacity supported by the device.

Configuration Example

Scenario	 ● Device A is the router. ● Device B is the gateway of the network segment where terminals reside. ● Device C, Device D, and Device E are terminals.
Configuration Steps	● Set the ARP timeout to 60 seconds on GigabitEthernet 0/1. ● Set the maximum number of learned ARP entries to 300 on GigabitEthernet 0/1. ● Set the retransmission interval of ARP request packets to 3s. ● Set the retransmission count of ARP request packets to 4. ● Set the maximum number of unresolved ARP entries to 4096.

	`Hostname(config)#interface gigabitethernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)#arp timeout 60`
	`Hostname(config-if-GigabitEthernet 0/1)#arp cache interface-limit 300`
	`Hostname(config-if-GigabitEthernet 0/1)#exit`
	`Hostname(config)#arp retry interval 3`
	`Hostname(config)#arp retry times 4`
	`Hostname(config)#arp unresolve 4096`

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 count, maximum number of unresolved ARP entries, and maximum number of ARP entries on the interface.
	Hostname#show arp timeout Interface arp timeout(sec) ---------- ---------- GigabitEthernet 0/1 60 GigabitEthernet 0/2 3600 GigabitEthernet 0/4 3600 GigabitEthernet 0/5 3600 GigabitEthernet 0/7 3600 VLAN 100 3600 VLAN 111 3600 Mgmt 0 3600 Hostname# show running-config arp unresolve 4096 arp retry times 4 arp retry interval 3 ! interface GigabitEthernet 0/1 arp cache interface-limit 300

1.4.3 Enabling Trusted ARP

Configuration Effect

- The gateway is protected against ARP spoofing.

Notes

- N/A

Configuration Step

- To deploy a GSN solution, enable trusted ARP.
- Enable trusted ARP in global configuration mode.

Verification

- Run the **show arp trusted** command to display trusted ARP entries.
- Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

↘ Enabling Trusted ARP

Command	**service trustedarp**
Parameter Description	N/A

Command Mode	Global configuration mode
Usage Guide	Trusted ARP defends against ARP spoofing on the device. It needs to be used with the GSN solution.

Enabling VLAN Redirection When a Trusted ARP Entry Is Added

Command	**arp trusted user-vlan** *vid1* **translated-vlan** *vid2*
Parameter Description	*vid1*: Indicates the VLAN ID configured on the server. *vid2*: Indicates the ID of the VLAN redirected.
Command Mode	Global configuration mode
Usage Guide	This command takes effect only after trusted ARP is enabled. Configure this command only when the VLAN pushed by the server differs from the VLAN in the trusted ARP entry.

Displaying Trusted ARP Entries

Command	**show arp trusted** [*ip* [*mask*]]
Parameter Description	*ip*: Indicates the IP address. The ARP entry of the specified IP address is displayed. If **trusted** is specified, only trusted ARP entries are displayed. Otherwise, non-trusted ARP entries are displayed. *mask*: Indicates that ARP entries within the IP subnet are displayed. If **trusted** is specified, only trusted ARP entries are displayed. Otherwise, non-trusted ARP entries are displayed.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Deleting Trusted ARP Entries

Command	**clear arp-cache trusted** [*ip* [*mask*]]
Parameter Description	*ip*: Indicates the IP address, from which ARP entries are to be cleared. All dynamic ARP entries are deleted by default. *mask*: Indicates the mask of a subnet, from which ARP entries are to be cleared. Dynamic ARP entries specified by the preceding IP address are deleted by default.
Command Mode	Privileged EXEC mode
Usage Guide	After you run the **clear arp-cache trusted** command to delete all trusted ARP entries on the switch, users may fail to access the network. You are advised to use the **clear arp-cache trusted** *ip* command to delete a specified trusted ARP entry.

Enabling Trusted ARP Aging

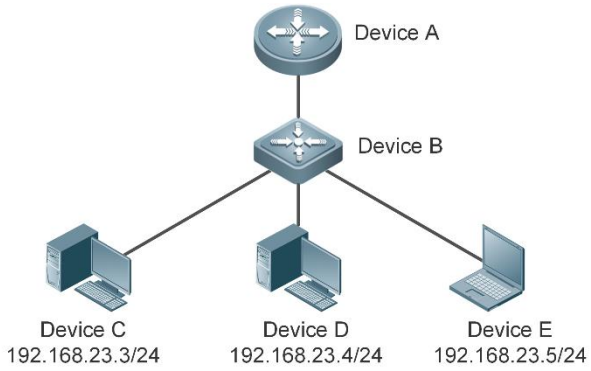
Command	**arp trusted aging**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After you configure this command, trusted ARP entries begin to age. The aging time is the same as the dynamic ARP aging time. You can run the **arp timeout** command in interface configuration mode

	to configure the aging time.

Adjusting the Capacity of Trusted ARP Entries

Command	**arp trusted** *number*
Parameter Description	*number*: Indicates the capacity of trusted ARP entries. The minimum value is 10. The maximum number is the capacity supported by the device minus 1,024. By default, the maximum number of trusted ARP entries is half of the total capacity of ARP entries.
Command Mode	Global configuration mode
Usage Guide	To make this command take effect, enable trusted ARP first. Trusted ARP entries and other entries share the memory. If trusted ARP entries occupy much space, dynamic ARP entries may not have sufficient space. Set the number of ARP entries as needed. Do not use a large value.

Configuration Example

Scenario	 ● Device A is the router. ● Device B is the gateway of the network segment where terminals reside. ● Device C, Device D, and Device E are terminals.
Configuration Steps	● Enable trusted ARP. ● Enable VLAN redirection. ● Enable trusted ARP aging. ● Set the maximum number of trusted ARP entries to 1024.

	`Hostname(config)# service trustedarp`
	`Hostname(config)#arp trusted user-vlan 2-9 translated-vlan 10`
	`Hostname(config)#arp trusted aging`
	`Hostname(config)#arp trusted 1024`

Verification	● Run the **show running-config** command to check whether the configurations take effect.

	`Hostname# show running-config`
	`service trustedarp`
	`arp trusted user-vlan 2-9 translated-vlan 10`
	`arp trusted aging`
	`arp trusted 1024`

Common Errors

- Trusted ARP is disabled, causing a failure to assign ARP entries.

1.4.4 Enabling Gratuitous ARP

Configuration Effect

The interface periodically sends gratuitous ARP packets.

Configuration Step

- Optional.
- When a device acts as the gateway, enable gratuitous ARP on an interface to prevent users from learning incorrect gateway MAC addresses due to ARP spoofing.
- Enable gratuitous ARP in interface configuration mode.

Verification

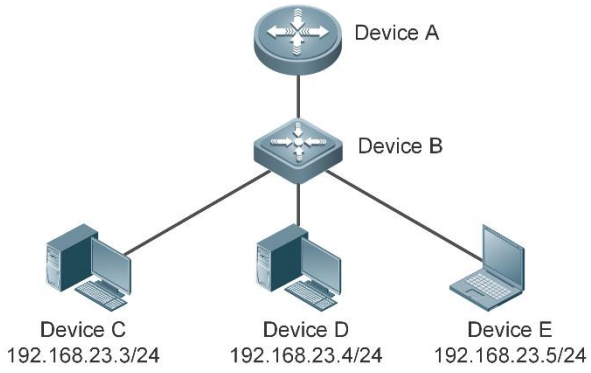
Run the **show running-config interface** [*name*] command to check whether the configuration is successful.

Related Commands

↘ Enabling Gratuitous ARP

Command	**arp gratuitous-send interval** *seconds* [*number*]
Parameter Description	*seconds*: Indicates the interval for sending a gratuitous ARP request packets, in seconds. The value range is from 1 to 3600. *number*: Indicates the number of gratuitous ARP request packets that are sent. The default value is 1. The value range is from 1 to 100.
Command Mode	Interface configuration mode
Usage Guide	If a network interface of a device acts as the gateway for downstream devices but a downstream device pretends to be the gateway, enable gratuitous ARP on the interface to advertise itself as the real gateway.

Configuration Example

Scenario	 ● Device A is the router. ● Device B is the gateway of the network segment where terminals reside. ● Device C, Device D, and Device E are terminals.
Configuration Steps	● Configure GigabitEthernet 0/1 to send a gratuitous ARP packet every 5s.

	`Hostname(config-if-GigabitEthernet 0/1)#arp gratuitous-send interval 5`
Verification	● Run the **show running-config interface** command to check whether the configuration takes effect.

	`Hostname#show running-config interface gigabitethernet 0/1`
	
	`Building configuration...`
	`Current configuration : 127 bytes`
	`!`
	`interface GigabitEthernet 0/1`
	` duplex auto`
	` speed auto`
	` ip address 30.1.1.1 255.255.255.0`
	` arp gratuitous-send interval 5`

1.4.5 Enabling Proxy ARP

Configuration Effect

The device acts as a proxy to reply to ARP request packets from other users.

Notes

By default, proxy ARP is disabled on Layer 3 switches while enabled on routers.

Configuration Step

- Optional.
- If a user without any route information needs to obtain the MAC addresses of the IP users in other subnets, enable proxy ARP on the device so that the device can act as a proxy to send ARP replies.
- Enable proxy ARP in interface configuration mode.

Verification

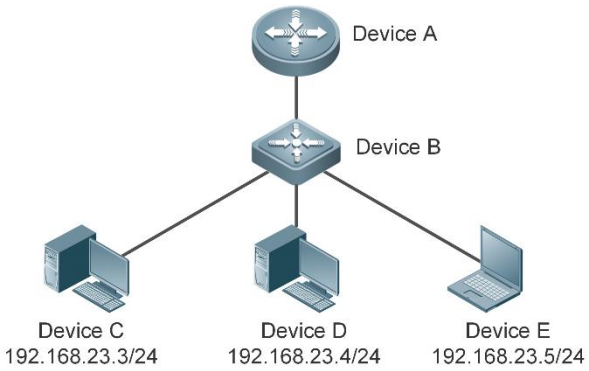
Run the **show ip interface** [*name*] command to check whether the configuration takes effect.

Related Commands

↘ Enabling Proxy ARP

Command	**ip proxy-arp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	 ● Device A is the router. ● Device B is the gateway of the network segment where terminals reside. ● Device C, Device D, and Device E are terminals.
Configuration Steps	● Enable proxy ARP on GigabitEthernet 0/1.
	`Hostname(config-if-GigabitEthernet 0/1)#ip proxy-arp`
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: DOWN`
	`  IP interface type is: BROADCAST`
	`  IP interface MTU is: 1500`
	`  IP address is:`
	`    No address configured`
	`  IP address negotiate is: OFF`
	`  Forward direct-broadcast is: OFF`
	`  ICMP mask reply is: ON`
	`  Send ICMP redirect is: ON`
	`  Send ICMP unreachable is: ON`
	`  DHCP relay is: OFF`
	`  Fast switch is: ON`
	`  Help address is: 0.0.0.0`
	`  Proxy ARP is: ON`
	`ARP packet input number: 0`
	`  Request packet     : 0`
	`  Reply packet       : 0`
	`  Unknown packet     : 0`
	`TTL invalid packet number: 0`
	`ICMP packet input number: 0`
	` Echo request       : 0`
	` Echo reply         : 0`
	` Unreachable        : 0`
	` Source quench      : 0`
	` Routing redirect   : 0`

1.4.6 Enabling Local Proxy ARP

Configuration Effect

The device acts as a proxy to reply to ARP request packets from other users in the same subnet.

Notes

Local proxy ARP is supported only on SVIs.

Configuration Step

- Optional.
- If a user enabled with port protection needs to communicate with users in the VLAN, enable local proxy ARP on the device.
- Enable local proxy ARP in interface configuration mode.

Verification

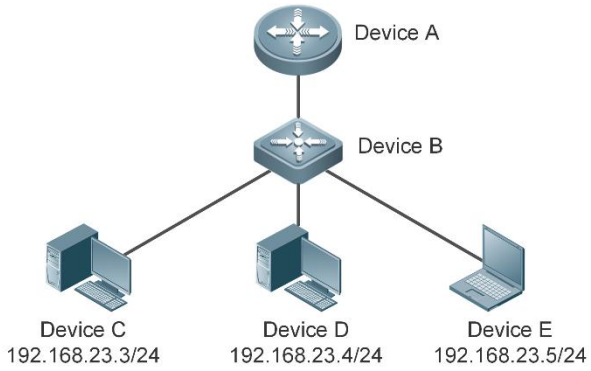
Run the **show run interface** [*name*] command to check whether the configuration takes effect.

Related Commands

Enabling Local Proxy ARP

Command	**local-proxy-arp**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Scenario	 ● Device A is the router. ● Device B is the gateway of the network segment where terminals reside. ● Device C, Device D, and Device E are terminals.
Configuration Steps	● Enable local proxy ARP on the interface of VLAN 1.
	`Hostname(config-if-VLAN 1)#local-proxy-arp`

Verification	● Run the **show ip interface** command to check whether the configuration takes effect.

	`Hostname#show running-config interface vlan 1`
	
	`Building configuration...`
	`Current configuration : 53 bytes`
	
	`interface VLAN 1`
	` ip address 192.168.1.2 255.255.255.0`
	` local-proxy-arp`

1.4.7 Enabling ARP Trustworthiness Detection

Configuration Effect

Enable ARP trustworthiness detection. If the device receiving an ARP request packet fails to find the corresponding entry, it performs NUD. If the MAC address in the existing dynamic ARP entry is updated, the device immediately performs NUD to prevent ARP attacks.

Notes

Because this function introduces a strict confirmation procedure into the ARP learning process, it impacts the efficiency of ARP learning.

Configuration Step

- Optional.
- If the device needs to learn ARP entries, enable ARP trustworthiness detection on the device. If the device receiving an ARP request packet fails to find the corresponding entry, it needs to send a unicast ARP request packet to check whether the peer end exists. If so, the device learns the ARP entry. If not, the device does not learn the ARP entry. If the MAC address in the ARP entry changes, the device will immediately perform NUD to prevent ARP spoofing.
- Enable ARP trustworthiness detection in interface configuration mode.

Verification

Run the **show running-config interface** [*name*] command to check whether the configuration take effect

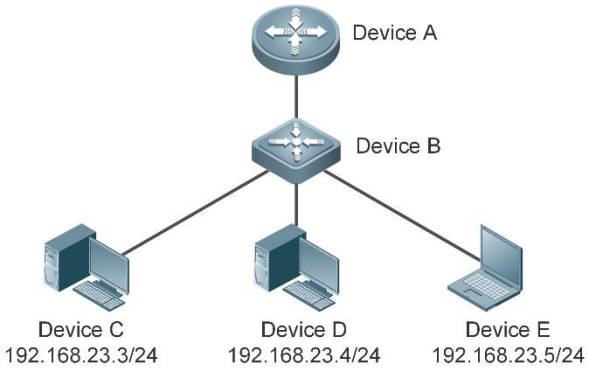
Related Commands

↘ Enabling ARP Trustworthiness Detection

Command	**arp trust-monitor enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	If the corresponding ARP entry exists and the MAC address is not updated, the device enabled

	with this function does not perform NUD. If the MAC address of the existing dynamic ARP entry is updated, the device enabled with this function immediately performs NUD. After this function is disabled, the device does not perform NUD for learning or updating ARP entries.

Configuration Example

Scenario	 ● Device A is the router. ● Device B is the gateway of the network segment where terminals reside. ● Device C, Device D, and Device E are terminals.
Configuration Steps	● Enable ARP trustworthiness detection on GigabitEthernet 0/1.
	`Hostname(config-if-GigabitEthernet 0/1)#arp trust-monitor enable`
Verification	● Run the **show running-config interface** command to check whether the configuration takes effect.

	`Hostname#show running-config interface gigabitethernet 0/1`
	
	`Building configuration...`
	`Current configuration : 184 bytes`
	`!`
	`interface GigabitEthernet 0/1`
	` duplex auto`
	` speed auto`
	` ip address 30.1.1.1 255.255.255.0`
	` arp trust-monitor enable`

1.4.8 Configuring the Device to Determine Host Existence Prior to ARP Proxy Service Provisioning

Supported functions are subject to the product version.

Configuration Effect

Enable the local ARP proxy on the VRRP master device. When responding to an ARP request packet as a proxy, the VRRP master device does not need to determine whether the ARP entry corresponding to the destination IP address exists.

Notes

The **arp proxy-resolved** command is enabled on the device by default. That is, by default, the VRRP master device responds to an ARP request packet as a proxy only after the destination IP address has been resolved.

Configuration Step

- Optional.
- Run the **no arp proxy-resolved** command when the VRRP master device needs to forcibly respond to ARP request packets as a proxy.
- Configure this function in global configuration mode.

Verification

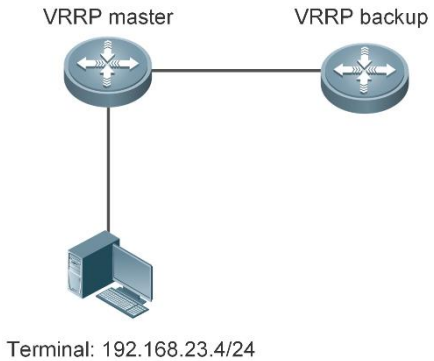
Run the **show running-config** command to check whether the configuration is successful.

Related Commands

Configuring the VRRP Master Device to Forcibly Respond to ARP Request Packets as a Proxy

Command	**no arp proxy-resolved**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Whether this configuration is supported depends on the actual product.

Configuration Example

Scenario	
Configuration Steps	● Configure the VRRP master device to forcibly respond to ARP request packets as a proxy, with no need to determine whether destination IP addresses have been resolved.
	`Hostname(config)#no arp proxy-resolved`
Verification	● Run the **show running-config** command to check whether the configuration is successful.
	`Hostname#show running-config` ` no arp proxy-resolved`

Common Errors

- N/A

1.4.9 Configuring the Device to Send ARP Request Packets to a Specified Sub-VLAN of a Super-VLAN

Supported functions are subject to the product version.

Configuration Effect

In gateway authentication mode, enable dumb terminals in a super-VLAN to be deployed in an authenticated VLAN, so that the device can proactively send ARP request packets to specific VLANs.

Notes

After the **arp resolve vlan** *vlan-list* command is configured, ARP request packets are sent only to VLANs in the specified VLAN list of a super-VLAN. In particular, if an authentication-exempt VLAN is configured and the authentication-exempt VLAN is not in the value specified by *vlan-list* of **arp resolve vlan**, ARP request packets will not be broadcast to the authentication-exempt VLAN.

Configuration Step

- Optional.
- Run the **arp resolve vlan** *vlan-list* command to configure the device to send ARP request packets to specified sub-VLANs of a super-VLAN.

Verification

Run the **show running-config** command to check whether the configuration is successful.

Related Commands

Configuring the Device to Send ARP Request Packets to a Specified Sub-VLAN of a Super-VLAN

Command	**arp resolve vlan**
Parameter Description	*vlan-list*: Sets the list of sub-VLANs in a super-VLAN, where ARP request packets are sent only to these sub-VLANs. **none**: Specifies that no ARP resolution request is sent to any sub-VLAN of a super-VLAN.
Command Mode	Global configuration mode
Usage Guide	Whether this configuration is supported depends on the actual product.

Configuration Example

Configuration Steps	• Enable the device to provide active ARP resolution for VLANs 10–20 and VLANs 25–30.
	`Hostname(config)# arp resolve vlan 10-20,25-30`
Verification	• Run the **show running-config** command to check whether the configuration is successful.
	`Hostname# show running-config`

	`arp resolve vlan 10-20,25-30`

Common Errors

- N/A

1.5 Monitoring

Clearing

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

Command	Description
clear arp-cache [**interface** *interface-name* | [**trusted**] *ip* [*mask*]]	Clears dynamic ARP entries. In gateway authentication mode, dynamic ARP entries in authentication VLANs are not cleared.

Displaying

Command	Description
show arp [*interface-type interface-number* | [*ip* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**]	Displays the ARP table.
show ip arp	Displays the ARP table.
show arp trusted [*ip* [*mask*]	Displays the trusted ARP table.
show arp counter	Displays the ARP entry counter.
show arp timeout	Displays the timeout of dynamic ARP entries.
show arp packet statistics [*interface*]	Displays ARP packet statistics.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug arp	Debugs ARP packet sending and receiving.
debug arp event	Debugs creation and deletion of ARP entries.

1 Configuring Proxy ARP

1.1 Overview

Proxy ARP enables the device to function as a proxy on a wireless local area network (WLAN) to respond to ARP request packets of another device. Because Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is used for communication on a wireless network, proxy ARP can prevent ARP broadcast packets on 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
Proxy ARP Service on a WLAN	The access controller (AC) acts as a proxy to respond to ARP request packets of any device on the WLAN.

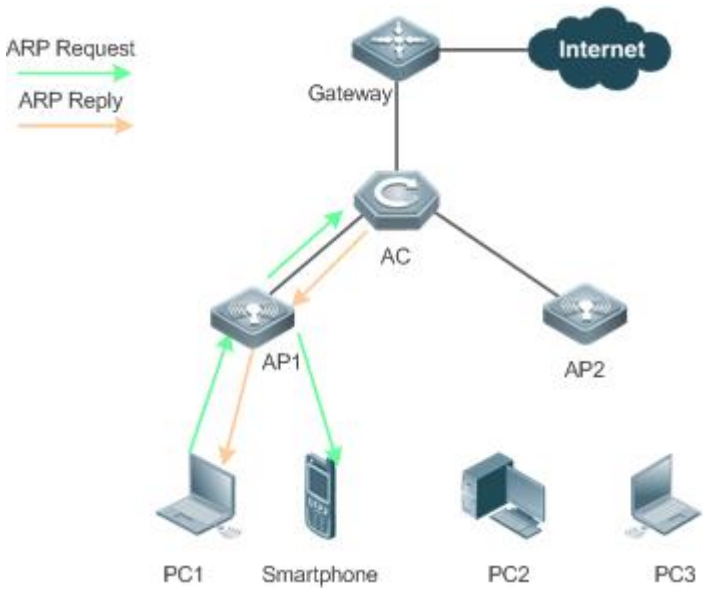
1.2.1 Proxy ARP Service on a WLAN

Scenario

In centralized forwarding mode of the fit AP, the AC acts a proxy for ARP request packets of any device on the WLAN.

- The AC needs to learn the MAC address of a device on the WLAN before responding to this device.

Figure 1-1



Remarks	The preceding figure is the flowchart of the ARP request packets that stations (STAs) send to the gateway or other devices in centralized forwarding mode of the fit AP on the WLAN.

Deployment

- Deploy a network consisting of the gateway, AC, APs, and STAs. The AC enabled with proxy ARP (enabled by default) works as a proxy to respond to ARP request packets of STAs to prevent ARP request packets from being broadcast to other APs.
- The proxy ARP function works on the AC and is transparent to users. You can run this function without any other configurations.

1.3 Features

Basic Concepts

↘ Proxy ARP

Layer 2 proxy ARP, also called proxy ARP, enables a device on a WLAN to work as a proxy to respond to ARP request packets of another device. Because CSMA/CA is used for communication on a wireless network, proxy ARP can prevent ARP packets on one AP from being broadcast to another AP, which increases the bandwidth utilization of the WLAN and enhances user experience.

Overview

Feature	Description
Wireless Proxy ARP	The AC works as a proxy for STAs to prevent ARP request packets from being broadcast to other APs.

1.3.1 Wireless Proxy ARP

Working Principle

In typical wireless networking, a STA usually accesses the Internet through an AP and an AC. Typically, multiple STAs are associated with one AP, while multiple APs are associated with one AC. When STAs connected to one AP access STAs connected to another AP, or wireless users and wired users access each other, ARP packets must be transmitted through the AC, making it easy for deploying proxy ARP on the AC.

The working process of proxy ARP is as follows:

1 The AC learns the source IP address and source MAC address from the transmitted ARP packet to generate an ARP entry.

2 According to the ARP entry, the AC works as a proxy on the network to respond to ARP request packets 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 packet.

4 ARP reply packets are forwarded in the same manner as 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 packet to PC2 and the AC.
3. From this ARP request packet, the AC learns the IP address and MAC address of PC3 and forwards this ARP request packet to the gateway, AP1, and PC1 and the smartphone connected to AP1.
4. The gateway sends an ARP reply packet to PC4 through AC. Then the AC learns the IP address and MAC address of the gateway.
5. PC1 initiates an ARP request packet to the IP address of the gateway.
6. AP1 forwards this ARP request packet to PC2 and AC.
7. The AC learns the IP and MAC address of PC1 and works as a proxy for the gateway to directly send an ARP reply packet 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 Proxy ARP

- By default, Layer 2 proxy ARP is enabled.
- Run the **no proxy-arp enable** command to disable Layer 2 proxy ARP.

1.4 Configuration

Configuration	Description and Command	
Enabling Layer 2 Proxy ARP	(Optional) By default, Layer 2 proxy ARP is enabled.	
	proxy-arp enable	Enables Layer 2 proxy ARP
Enabling Proxy ARP on the Device to Only Learn ARP Entries of Wireless Ports	(Optional) By default, learning of only ARP entries on wireless ports is disabled.	
	proxy-arp learn only-wlan [**except** *ip-address*]	Enables proxy ARP on the device to learn only ARP packets of wireless ports and excluded IP addresses.

1.4.1 Enabling Layer 2 Proxy ARP

Configuration Effect

Enabling Layer 2 Proxy ARP improves wireless bandwidth efficiency and user experience.

Notes

N/A

Configuration Step

Enabling Layer 2 Proxy ARP

- By default, Layer-2 proxy ARP is enabled.
- In a wireless IPv4 scenario, enabling Layer 2 proxy ARP on AC to enhance network bandwidth utilization and user experience.

Verification

Run the **show running-config** command to check whether Layer 2 proxy ARP is enabled.

Related Commands

Disabling Layer 2 Proxy ARP

Command	**no proxy-arp enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Disabling Layer 2 Proxy ARP

Configuration Steps	• Disable Layer 2 proxy ARP.
	`Hostname(config)# no proxy-arp enable`
Verification	• Run the **show running-config** command to check whether Layer 2 proxy ARP is enabled.
	`Hostname# show running-config` `no proxy-arp enable`

Common Errors

N/A

1.4.2 Enabling Proxy ARP on the Device to Only Learn ARP Entries of Wireless Ports

Configuration Effect

Enable learning of only ARP entries on wireless ports according to the actual topology. The device can learn excluded IP addresses on wired ports. In this way, the ARP entry capacity on an AC will not be fully occupied by ARP packets on wired ports.

Notes

If there is a sufficient proxy ARP volume (queried through the **show proxy-arp statistic** command), do not enable this function. This is because learning ARP packets of wired ports helps decrease flooding of broadcast ARP packets of wired users.

Configuration Step

Enabling Proxy ARP on the Device to Learn Only ARP Packets of Wireless Ports

- By default, this function is disabled.
- If the AC that does not serve as a gateway is enabled with this function, you are advised to configure an excluded IP address so that the device learns the IP address of the gateway of the wired port.

Verification

Run the **show running-config** command to check whether this function is enabled.

Related Commands

Enabling Proxy ARP on the Device to Learn Only ARP Packets of Wireless Ports

Command	**proxy-arp learn only-wlan** [**except** *ip-address*]
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	You can enable this function when all of the following requirements are met: ● The AC works in centralized forwarding mode. ● The AC interconnects with the gateway. Configure a super-VLAN and many sub-VLANs for STAs on the gateway. ● Proxy ARP entries are easily used up due to a large number of users (run the **show proxy-arp statistics** command to display proxy ARP statistics).

Configuration Example

Enabling Proxy ARP on the Device to Learn Only ARP Packets of Wireless Ports

Configuration Steps	● Enable proxy ARP on the device to learn only ARP packets of wireless ports as well as excluded IP addresses, 192.168.21.1 and 92.168.22.1.
	`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 this function is enabled.

	`Hostname#show running-config`
	`proxy-arp learn only-wlan except 192.168.21.1`
	`proxy-arp learn only-wlan except 192.168.22.1`

Common Errors

N/A

1.5 Monitoring

Clearing

Command	Description
clear proxy-arp [*ip-address vlan-id*]	Clears the specified proxy ARP entry.
clear proxy-arp	Clears all proxy ARP entries.

Displaying

Command	Description
show proxy-arp [*ip-address*]	Displays all proxy ARP entries.
show proxy-arp dynamic	Displays dynamic proxy ARP entries.
show proxy-arp statistics	Displays proxy ARP statistics.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug proxy-arp	Debugs receiving/sending of ARP packets.

1 Configuring IPv4 Basics

1.1 Overview

The Internet Protocol (IP) sends packets to the destination from the source by using logical (or virtual) addresses, that is, IP addresses. At the network layer, routers forward packets based on IP addresses.

Protocols and Standards

- RFC 1918: Address Allocation for Private Internets
- RFC 1166: Internet Numbers

1.2 Applications

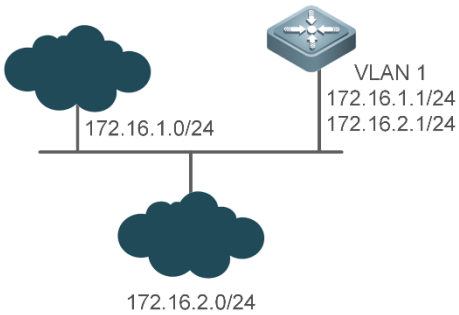
Application	Description
Configuring an IP Address for Communication	Two networks communicate through one interface.

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 on the two network segments can communicate with the Internet through devices and computers between the two network segments can communicate with each other.

Figure 1-1 Configuring IP Addresses



Deployment

- Configure two IP addresses in VLAN 1. One is a primary IP address and the other is a secondary IP address.
- For hosts on the network segment 172.16.1.0/24, set the gateway address to 172.16.1.1. For hosts on the network segment 172.16.2.0/24, set the gateway address to 172.16.2.1.

1.3 Features

Basic Concepts

IP Address

An IP address consists of 32 bits in binary notation. To facilitate writing and description, an IP address is generally expressed in decimal notation. When the IP address is expressed in decimal notation, an IP address is divided into four groups, with eight bits in each group. The value range of each group is from 0 to 255, and groups are separated by a full stop (.). For example, the value 192.168.1.1 is an IP address expressed in decimal notation.

IP addresses are used for interconnection at the IP layer. A 32-bit IP address consists of two parts, namely, network bits and host bits. Based on 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 address	1	1	1	0	Multicast address	

The addresses with the first four most significant bits 1111 cannot be assigned. These addresses are called class E addresses and are reserved.

When IP addresses are planned during network construction, they should be assigned according to the network's specific requirements. If the network requires Internet connectivity, users must apply for IP addresses from the appropriate agency. In China, this process is managed by the China Internet Network Information Center (CNNIC). The Internet Corporation for Assigned Names and Numbers (ICANN) oversees the final assignment of IP addresses globally. For internal private networks, users do not need to apply for IP addresses, but assigning IP addresses randomly is discouraged. It is advisable to use 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 on 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 details about IP address assignment, TCP/UDP ports, and other codes, refer to RFC 1166.

Subnet Mask

A subnet mask is also a 32-bit value. It designates which bits in an IP address signify the network address. In a subnet mask, IP address bits corresponding to '1' bits designate the network address, while bits corresponding to '0' bits designate the host address. For instance, in class A networks, the subnet mask is 255.0.0.0. Using subnet masks allows for the division of a network into multiple subnets. Subnetting involves using some host address bits as part of the network address, reducing host capacity while increasing the number of networks. In such cases, subnet masks are referred to as 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:

- Directed broadcast: All hosts on the specified network are packet receivers and the host bits of a destination address are all 1s.
- Limited broadcast: All hosts on all networks are packet receivers and the 32 bits of a destination address are all 1s.

ICMP Packet

The 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 network exceptions occur.

TTL

The Time To Live (TTL) refers to the number of network segments where packets are allowed to pass before they are discarded. The TTL is included in an IP packet, signaling how long the packet can remain on the network before it should be discarded.

Features

Feature	Description
IP Address	The IP protocol can run on an interface only when the interface is configured with an IP address.
Broadcast Packet Processing	Broadcast addresses are configured, so broadcast packets can be forwarded and processed.
Sending ICMP Packets	ICMP packets are sent and received.
Limiting the Transmission Rate of ICMP Error Packets	This function prevents Denial of Service (DoS) attacks.
IP MTU	The Maximum Transmission Unit (MTU) of IP packets on an interface is configured.
IP TTL	The TTL of unicast packets and broadcast packets is configured.
IP Source Route	Source routes for receiving packets are checked.
IP Address Pool	The IP address pool is used to assign an IP address to the peer end through Point-to-Point Protocol (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 the Dynamic Host Configuration Protocol (DHCP)

3 Obtaining IP addresses through PPP negotiation

4 Borrowing IP addresses of other interfaces

These approaches are 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 *Configuring DHCP*. The following describes the other three approaches for obtaining IP addresses.

Configuring an IP Address for an Interface

A device can receive and send IP packets only after the device is configured with an IP address. The IP protocol can run on an interface only when the interface is configured with an IP address.

Configuring Multiple IP Addresses for an Interface

Multiple IP addresses can be configured for an interface, of which one is a primary IP address and the others are secondary IP addresses. The number of secondary IP addresses is not limited. However, secondary IP addresses must belong to different networks and secondary IP addresses must be on different networks from primary IP addresses. In network construction, secondary IP addresses are often used in the following situations:

- 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 legacy networks are Layer 2 bridged networks without subnetting. You can use secondary IP addresses to upgrade the network to a routing network based on the 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 be not 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 borrowed by multiple interfaces.

IP addresses of borrowing interfaces are always consistent with and vary with IP addresses of borrowed interfaces.

Configuring an IP Address of a BVI Interface on an AP Through an AC

The configuration modes on an AC include the AP configuration mode, AP group configuration mode, and all-AP configuration mode, which are in descending order of priority. The configuration pushed to an AP has the highest priority.

In any AP configuration mode, you can configure an IP address for only one bridge virtual interface (BVI) by using the **ap-interface bvi** *num* **ip address** *ip-address network-mask* command or the **ap-interface bvi** *num***ip address dynamic** command.

On a fit AP network, if the **ap-interface bvi** *num***ip address** *ip-address network-mask* command is used, the AP needs to be assigned within different VLANs. Otherwise, an address conflict occurs. If the **ap-interface bvi** *num***ip address dynamic** command is used, the problem does not occur.

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.

Borrowing an IP Address from Another Interface

- 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.

Configuring an IP Address of a BVI on an AP Through an AC

- By default, the IP address of a BVI is not configured in AP configuration mode.
- The **ap-interface bvi** *num* **ip address** command is used to configure the IP address of a BVI of an AP on an AC.

1.3.2 Broadcast Packet Processing

Working Principle

Broadcast is classified into two types:

- Limited broadcast: The IP address is 255.255.255.255. Because such an address is prohibited by routers, the broadcast is called local network broadcast.
- Directed broadcast: All host bits are 1s, for example, 192.168.1.255/24. 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, severely impacting its performance, leading to what is known as a broadcast storm. Devices provide some approaches to contain broadcast storms within the local network and prevent their spread. Layer 2 network devices such as bridges and switches can propagate broadcast storms.

The most effective approach to prevent broadcast storms is to assign a directed broadcast address to each network. This involves using directed broadcast but not limited broadcast in the IP protocol to disseminate 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 device indirectly connected to the destination subnet forwards the packets. After directed broadcast packets reach the device directly connected to the subnet, the device converts directed broadcast packets to limited broadcast packets (destination IP address is 255.255.255.255) and broadcasts 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 specified 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 Packet

A device receives non-broadcast packets destined for itself, and the packets contain the IP protocol that cannot be supported by the device. The device sends an ICMP protocol unreachable packet to the source host. Besides, if the device does not know a route to forward packets, it also sends an ICMP host unreachable packet.

ICMP Redirection Packet

Sometimes, a route may be less than optimal. In this case, a device sends 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 packet 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 Packet

Sometimes, a network device sends an ICMP mask request packet to obtain the mask of a subnet. The network device that receives the ICMP mask request packet sends a mask response packet.

Timestamp Query

RFC 792 requests the system to return the current system time when the system receives an ICMP timestamp query request.

To prevent attackers from obtaining the system time through the protocol and attacking time-based authentication protocols, you can disable the timestamp query function. Then the device directly discards received ICMP timestamp query requests.

Related Configuration

Enabling the ICMP Protocol Unreachable Packet

- By default, the ICMP Protocol unreachable packet function is enabled on an interface.
- You can run the [**no**] **ip unreachables** command to disable or enable the function.

Enabling the ICMP Redirection Packet

- By default, the ICMP redirection packet function is enabled on an interface.
- You can run the [**no**] **ip redirects** command to disable or enable the function.

Enabling the ICMP Mask Response Packet

- By default, the ICMP mask response packet function is enabled on an interface.
- You can run the [**no**] **ip mask-reply** command to disable or enable the function.

Enabling Timestamp Query

- By default, a timestamp query message is not sent.
- You can run the [**no**] **ip icmp timestamp** command to enable or disable the function.

1.3.4 Limiting the 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 be not 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 the DF Bit in the IP Header

- By default, 10 packets are transmitted at an interval of 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

- By default, 10 packets are transmitted at an interval of 100 milliseconds.
- The **ip icmp error-interval** command can be used to configure the transmission rate.

1.3.5 IP MTU

Working Principle

If the size of an IP packet exceeds the IP MTU, the RGOS software splits the packet. For all devices on 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 MTU of IP packets.

1.3.6 IP TTL

Working Principle

An IP packet is transmitted from the source address to the destination address through routers. After the TTL is set, the TTL decreases by 1 every time when the IP packet passes a router. When the TTL drops to zero, the router discards the packet. This prevents infinite transmission of useless packets and waste of bandwidth.

Related Configuration

↘ Setting the IP TTL

- By default, the IP TTL of an interface is 64.
- The **ip ttl** command can be used to set the IP TTL of an interface.

1.3.7 IP Source Route

Working Principle

Devices support IP source routes. When a device receives an IP packet, it checks options such as the 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 one option is enabled for the packet, an action is taken. 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 bypass the network where faults occur. 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 the function.

1.3.8 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 about the client. If the client passes 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 the function.

Creating an Address Pool

- By default, no IP address pool is configured.
- The **ip local pool** command can be used to create an address pool.

1.4 Configuration

Configuration	Description and Command	
Configuring an 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 unnumbered	Borrows an IP address from another interface.
	ap-interface bvi *num* **ip address**	Configures the IP address of a BVI on an AP through an AC.
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 packets and host unreachable packets.
	ip redirects	Enables ICMP redirection packets.
	ip mask-reply	Enables ICMP mask response packets.
	ip icmp timestamp	Enables timestamp query.
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.
Setting the IP TTL	(Optional) It is used to configure the TTL of unicast packets and broadcast packets.	
	ip ttl	Sets the TTL.

Configuration	Description and Command	
Configuring an IP Source Route	(Optional) It is used to check the source routes.	
	ip source-route	Enables the IP source route function.
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

1.4.1 Configuring an IP Addresses of an Interface

Configuration Effect

Configure an IP address of an interface for communication.

Notes

- N/A

Configuration Step

Configuring an IP Address of an Interface

- Mandatory.
- Perform the configuration in Layer 3 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 Layer 3 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 Layer 3 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*: Specifies the 32-bit IP address, with 8 bits for each group. The IP address is expressed in decimal notation and groups are separated by a full stop (.). *network-mask*: Specifies the 32-bit network mask. The value 1 indicates the mask bit and the value 0 indicates the host bit. Every 8 bits form one group. The network mask is expressed in decimal notation and groups are separated by a full stop (.).

	secondary: Indicates the secondary IP address.
Command Mode	Interface configuration mode
Usage Guide	N/A

Borrowing an IP Addresses from Another Interface

Command	**ip unnumbered** *interface-type interface-number*
Parameter Description	*interface-type*: Specifies the interface type. *interface-number*: Specifies the interface number.
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, and 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. 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 Serial Line Internet Protocol (SLIP), High-Level Data Link Control (HDLC), PPP, Link Access Procedure Balanced (LAPB), and Frame Relay (FR), the serial interface can be set to an unnumbered interface. During FR encapsulation, 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.

Configuring the IP Address of a BVI on an AP Through an AC

Command	**ap-interface bvi** *num***ip address** {*ip-address network-mask* | **dynamic**}
Parameter Description	*num*: Specifies the BVI number. *ip-address*: Specifies the 32-bit IP address, with 8 bits for each group. The IP address is expressed in decimal notation and groups are separated by a full stop (.). *network-mask*: Specifies the 32-bit network mask. The value 1 indicates the mask bit and the value 0 indicates the host bit. **dynamic:** Configures the IP address and mask of a BVI on an AP by dynamically obtaining IP addresses and masks.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	Run the command in AP configuration mode or AP group configuration mode. In other words, the configuration modes on an AC include the AP configuration mode, AP group configuration mode, and all-AP configuration mode, which are in descending order of priority. You can configure an IP address for only one BVI in any AP configuration mode. According to the priority, the AC selects the configuration of the highest priority and pushes it to the corresponding AP.

	⚠ On a fit AP network, if the **ap-interface bvi** *num* **ip address** *ip-address network-mask* command is used, the AP needs to be assigned within different VLANs. Otherwise, an address conflict occurs. If the **ap-interface bvi** *num***ip address dynamic** command is used, the problem does not occur.

Configuration Example

Configuring an IP Address for an Interface

Configuration Steps	● Configure IP address 192.168.23.110 255.255.255.0 on GigabitEthernet 0/1.

	`Hostname#configure terminal`
	`Hostname(config)#interface gigabitethernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# no switchport`
	`Hostname(config-if-GigabitEthernet 0/1)#ip 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)`

Configuring the IP Address of a BVI on an AP Through an AC

Configuration Steps	● Configure the IP address of BVI 2 of an AP to 192.168.2.1 255.255.255.0 in the configuration mode of **ap120**.

	`Hostname(config)#ap-config ap120`
	`You are going to config AP(ap120), which is online now.`
	`Hostname(config-ap)#ap-interface bvi 2 ip address 192.168.2.1 255.255.255.0`

Verification	● Run the **show ap-config running-config** command on the AC to check whether the configuration takes effect.

	`Hostname# show ap-config running-config`
	`ap-config ap120`
	`ap-interface bvi 2 ip address 192.168.2.1 255.255.255.0`

	● Run the **show ip interface brief** command on the AP to check whether the configuration takes effect.

	`Hostname# show ip interface brief`
	`Interface  IP-Address(Pri)  IP-Address(Sec)  Status  Protocol`
	`BVI 2  192.168.2.1/24  no address  up  up`

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 Step

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 Layer 3 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 the host does not belong to, enable directed broadcast forwarding.
- Perform the configuration in Layer 3 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*: Specifies the broadcast address of an IP network.
Command Mode	Interface configuration mode
Usage Guide	Typically, 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 and receive self-defined broadcast packets and broadcast packets with the address 255.255.255.255.

Allowing Forwarding of Directed Broadcast Packets

Command	**ip directed-broadcast** [*access-list-number*]
Parameter Description	*access-list-number*: Specifies the number of an access control list (ACL). The value range is from 1 to 199 and from 1300 to 2699. After an ACL is defined, only directed broadcast packets that match the ACL are forwarded.
Command	Interface configuration mode

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 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 packets, ICMP redirection packets, and mask response packets on an interface.

Notes

N/A

Configuration Step

↘ Enabling ICMP Unreachable Packets

- By default, ICMP unreachable packets are enabled.
- Optional.
- The **no ip unreachables** command can be used to disable ICMP unreachable packets.
- Perform the configuration in Layer 3 interface configuration mode.

↘ Enabling ICMP Redirection Packets

- By default, ICMP redirection packets are enabled.
- Optional.
- The **no ip redirects** command can be used to disable ICMP redirection packets.
- Perform the configuration in Layer 3 interface configuration mode.

↘ Enabling ICMP Mask Response Packets

- By default, ICMP mask response messages are enabled.
- Optional.

- The **no ip mask-reply** command can be used to disable ICMP mask response packets.
- Perform the configuration in Layer 3 interface configuration mode.

Enabling Timestamp Query

- By default, timestamp query is enabled.
- Optional.
- The **no ip icmp timestamp** command can be used to disable timestamp query.
- Perform the configuration in global configuration mode.

Verification

- Run the **show ip interface** command to check whether the configuration takes effect.
- Run the **show running-config** command to check whether notifications of expired TTL are disabled.
- Run the **show running-config** command to check whether timestamp query is enabled.

Related Commands

Enabling ICMP Unreachable Packets

Command	**ip unreachables**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Redirection Packets

Command	**ip redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Enabling ICMP Mask Response Packets

Command	**ip mask-reply**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Disabling Timestamp Query

Command	**no ip icmp timestamp**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	● Enable ICMP unreachable packets, ICMP redirection packets, and mask response packets on GigabitEthernet 0/1.

	`Hostname# configure terminal`
	`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 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 Step

↘ 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*: Indicates the refresh cycle of a token bucket. The value range is from 0 to 2147483647 and the default value is 100 ms. When the value is 0, the transmission rate of ICMP error packets is not limited. *bucket-size*: Indicates the 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 be not sent. As a result, the path MTU discovery function becomes ineffective. To avoid this problem, you should limit the transmission rate of ICMP destination unreachable packets and other ICMP error packets respectively. You are advised to set the refresh cycle to an integral multiple of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not an integral multiple of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to an integral multiple of 10 milliseconds. For example, if the refresh rate is set to 3 per 15 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds.

Configuring the Transmission Rate of Other ICMP Error Packets

Command	**ip icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh cycle of a token bucket. The value range is 0 to 2147483647, and the default value is 100 ms. When the value is 0, the transmission rate of ICMP error packets is not limited. *bucket-size*: Indicates the number of tokens contained in a token bucket. The value range is 1 to 200 and the default value is 10.
Command Mode	Global configuration mode.
Usage Guide	This function limits the transmission rate of ICMP error packets to prevent DoS attacks by using the token bucket algorithm. You are advised to set the refresh cycle to an integral multiple of 10 milliseconds. If the refresh cycle is set to a value greater than 0 and smaller than 10 milliseconds, the refresh cycle that actually takes

	effect is 10 milliseconds. For example, if the refresh rate is set to 1 per 5 milliseconds, the refresh rate that actually takes effect is 2 per 10 milliseconds. If the refresh cycle is not an integral multiple of 10 milliseconds, the refresh cycle that actually takes effect is automatically converted to an integral multiple 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 the 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 MTU of IP packets.

Notes

N/A

Configuration Step

- Optional.
- When the IP MTU of interconnected interfaces is different on devices on the same physical network segment, set the IP MTU to the same value.
- Perform the configuration in Layer 3 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*: Indicates the MTU of IP packets. The value range is from 68 bytes to 1500 bytes.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

Configuration Steps	● Set the IP MTU of 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 of an interface.

Notes

N/A

Configuration Step

- Optional.
- Perform the configuration in Layer 3 interface configuration mode.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

↘ Setting the IP TTL

Command	**ip ttl** *value*
Parameter Description	*value*: Indicates the TTL. 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 running-config** command to check whether the configuration takes effect.

	Hostname#show running-config ip ttl 100

1.4.7 Configuring an IP Source Route

Configuration Effect

Enable or disable the IP source route function.

Notes

N/A

Configuration Step

- 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 running-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 running-config** command to check whether the configuration takes effect.
	Hostname#show running-config no ip source-route

1.4.8 Configuring an IP Address Pool

Configuration Effect

Assign an IP address to a client through PPP negotiation.

Notes

N/A

Configuration Step

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 Layer 3 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*: Indicates the name of a local IP address pool. **default** indicates the default address pool name. *low-ip-address*: Indicates the smallest IP address in an IP address pool. *high-ip-address*: Indicates the largest IP address in an IP address pool, which is optional. 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.

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`

Verification	● Run the **show running-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`
	`!`

1.5 Monitoring

Displaying

Command	Description
show ip interface [*interface-type interface-number* | **brief**]	Displays the IP address of an interface.
show ip packet statistics [**total** | *interface-name*]	Displays IP packet statistics.
show ip packet queuepool [*pool-name*]	Displays IP packet sending and receiving statistics of the protocol stack.
show ip raw-socket [*num*]	Displays IPv4 raw sockets.
show ip sockets	Displays all IPv4 sockets.
show ip udp [**local-port** *num*]	Displays IPv4 UDP sockets.
show ip udp statistics	Displays statistics on IPv4 UDP sockets.

1 Configuring NAT

1.1 Overview

Network Address Translation (NAT) technology translates an 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 method conserves public IP addresses by using a small number to represent a large amount of private IP addresses.

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

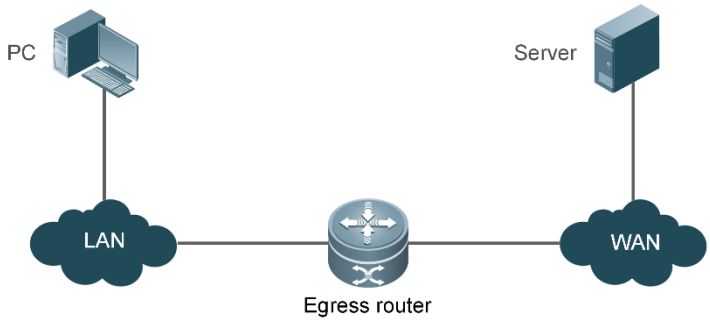
Application	Description
Intranet Users' Access to the Internet	NAT allows an intranet to communicate with the Internet by translating an internal private IP address into a globally unique IP address.
External Users' Access to an Intranet Server	NAT allows external networks to access internal devices by mapping one or more internal hosts to a network server.
Source/Destination Address Translation for Internal Users	When two private networks that need 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 heavy, multiple hosts are deployed for load balancing. In this case, NAT can be used for load balancing TCP traffic.

1.2.1 Intranet Users' Access to the Internet

Scenario

A PC is located on an intranet, while a server is located on an extranet, as shown in Figure 1-1. Because IP addresses are about to be exhausted, only one or a few public IP addresses are allocated to the entire campus network. An egress device belongs to the intranet, and connects to the extranet. Basic NAT functions need to be configured 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 extranet.

Deployment

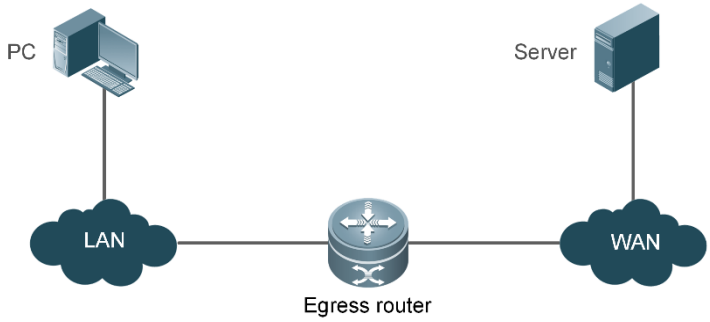
- Configure NAT for an intranet interface and an extranet interface.
- Configure static source address translation on the egress device.

1.2.2 External Users' Access to an Intranet Server

Scenario

A PC is located on an extranet, while a server (such as a web server) is located on an intranet, as shown in Figure 1-2. Because IP addresses are about to be exhausted, 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 extranet.
The server is deployed on the intranet.

Deployment

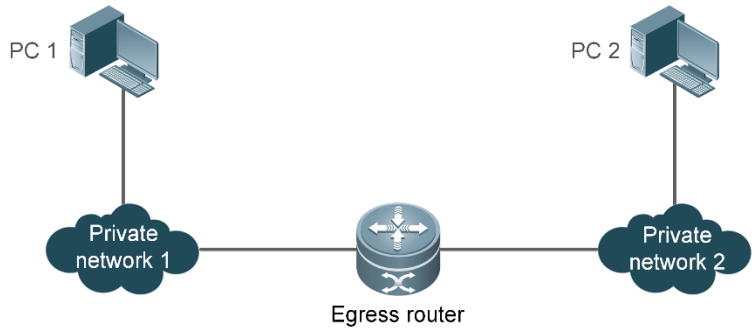
- Configure NAT for an internal interface and an external interface.
- Configure server port address translation rules on the egress device.

1.2.3 Source/Destination Address Translation for Internal Users

Scenario

PC 1 is located on private network 1, while PC 2 is located on private network 2, as shown in Figure 1-3. Because the two private networks are separately managed, address overlapping occurs on their IP network segments. For example, the IP addresses of PC 1 and PC 2 are configured on 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.

Deployment

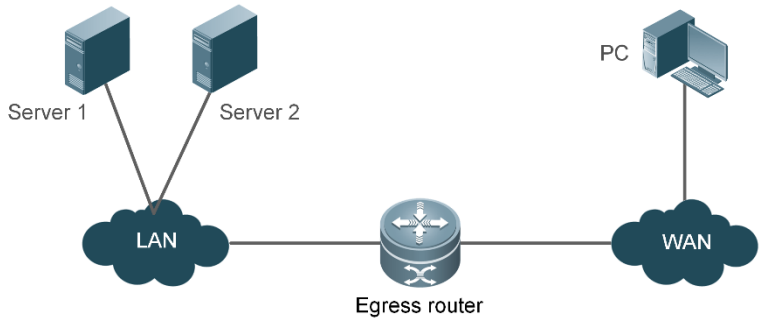
- Configure NAT for an internal interface and an external interface.
- Configure dynamic translation of the internal source address on the egress device.
- Configure dynamic translation of the external source address on the egress device.

1.2.4 Intranet Server Load Balancing

Scenario

Server 1 and Server 2 are located on an intranet, and form a cluster, as shown in Figure 1-4. A PC is located on an extranet. Because IP addresses are about to be exhausted, 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 egress device needs to distribute the server access traffic of the external user to the two servers; therefore, NAT load balancing needs to be enabled on the egress device.

Figure 1-4



The egress device connects both the intranet and extranet.

Servers are deployed on the intranet.

Deployment

- Configure NAT for an internal interface and an external interface.
- Configure TCP load balancing using NAT on the egress device.

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 within private networks, which are not allocated for Internet use 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. Typically, a private network is an intranet, and a public network is an extranet.

Static NAT

Static NAT allows one-to-one permanent mappings between internal local addresses and internal global addresses. Static NAT is used when an extranet needs to access internal hosts using a fixed global routable address.

Dynamic NAT

Dynamic NAT establishes temporary mapping relationships between internal local addresses and internal global addresses. The temporary mapping relationships will be removed if they are not used in a given period of time. Dynamic NAT can be configured in the scenario where 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	Translates internal private addresses into globally unique addresses, so that the intranet and the public network can communicate with each other.
NAPT	Maps multiple internal local addresses to one internal global address, so as to resolve the problem of IP address exhaustion.
Overlapping NAT	Enables overlapping networks to communicate.
TCP Load Balancing	Resolves the problem of TCP traffic overload.
Constructing a Local Server	Enables the extranet to access the local server.
ALG	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 internal 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 at 192.168.1.2 to an extranet server at 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 for 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 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 internal private IP address 192.168.1.2.

The preceding NAT process is transparent to terminals (hosts and servers in the preceding figures). For the extranet server, the IP address of the intranet host is 30.1.1.1 and the extranet server does not know the IP address 192.168.1.2. Therefore, NAT shields the private network of an enterprise.

Basic NAT includes static NAT and dynamic NAT.

Related Configuration

↘ Configuring NAT Interfaces

- A routed port is not a NAT interface by default.
- For a routed port, run the **ip nat** { **inside | outside** } command to specify a pair of NAT interfaces. For a non-routed port, 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 external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external 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

Traditional NAT employs one-to-one address mapping, which fails to meet requirements of all hosts on intranets to communicate with extranets. For example, when the intranet lacks global IP addresses or even does not apply for global IP addresses, or has only one global IP address to connect to an Internet Service Provider (ISP) but a large number of hosts on the intranet need to access the Internet, NAPT is necessary in such scenarios.

Multiple internal local addresses can map to one internal global address using NAPT.

When NAPT mappings for a large number of public IP addresses are configured and NAPT is deployed on the egress gateway in VRRP scenarios, association between the VRRP groups and the extranet interface link status and protocol status needs to be used if attacks occur on the extranet. In addition, the advertisement count multiplier needs to be adjusted to reduce the VRRP active/standby switchover frequency. To ensure that the NAT device can send free ARP packets from local host addresses and respond to ARP requests correctly during a VRRP active/standby switchover, you should associate the NAT device with a VRRP group and restrict the rate at which gratuitous ARP packets are sent.

Working Principle

NAPT, also known as multi-to-one address translation, allows multiple internal addresses to be mapped to one public address. NAPT maps both IP addresses and port numbers; that is, source addresses of data packets from different internal addresses can be mapped 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 implements conversion between "private IP address + port number" and "public IP address + port number".

Static NAPT

Static NAPT is used to map the specified port on a specified host on an intranet to the specified port of a global address, while static NAT maps an internal host to a global address. Static NAPT is applicable to intranet hosts that provide the information service, and 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. It provides a temporary one-to-one "IP address + port" mapping relationship.

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 external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external 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, only one IP address is defined in the address pool, and one IP address can be translated using NAT for up to 64,512 times. If one IP address is not enough, multiple IP addresses can be defined in the address pool.

1.3.3 Overlapping NAT

Address overlapping indicates that 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. Two overlapping network hosts cannot communicate, because both hosts consider that the peer host is located on the local network. Overlapping NAT is especially designed to implement communication between two networks with the same IP address. After overlapping NAT is configured, an extranet host address will be represented as another host address on 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 internal address into a unique external address. In addition, NAT needs to translate the external address that overlaps with the internal address into another unique internal 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 external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external interface need to be configured.

Configuring Internal Source Address Translation

- Internal source address translation is not configured by default.

- Static/Dynamic basic NAT or static/dynamic NAPT can be used for internal source address translation. For details, see 1.3.1 Basic NAT and 1.3.2 NAPT.

Configuring Static Translation of External Source Addresses

- Static translation of external source addresses is not configured by default.
- Use the **ip nat outside source static** *global-ip local-ip* command to configure static translation of external source addresses.

Configuring Dynamic Translation of External Source Addresses

- Dynamic translation of external source addresses is not configured by default.
- Use the **ip nat outside source list** *access-list-number* **pool** *pool-name* command to configure dynamic translation of external source addresses.

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.
- 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 internal destination address translation.

1.3.4 TCP Load Balancing

When the TCP traffic load of an intranet host is heavy, multiple hosts can be deployed to implement TCP service load balancing. In this case, NAT can be used to address this issue.

Working Principle

A NAT-enabled virtual host is created 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 load balance traffic.

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 external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external interface need to be configured.

Configuring an 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.

Configuring an 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 extended ACL must be configured based on destination IP address matching.

Configuring Internal Destination Address Translation

- Internal destination address translation is not configured by default.
- Use the **ip nat inside destination list** *access-list-number* **pool** *pool-name* command to configure internal 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) on an intranet. The user hopes that network hosts on a WAN can access the three servers, while common users of the intranet can use the gateway for Internet access.

Working Principle

One or more internal hosts are mapped 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 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 external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external interface need to be configured.

Configuring Internal Address and Port Translation

- Internal 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 internal 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 ineffective for the 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

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 application layer communication. ALG is enabled for NAT by default. The protocols that support ALG include DNS, FTP, H323, PPTP, TFTP, RTSP, and SIP.

Related Configuration

Enabling or Disabling ALG

- By default, ALG for all supported protocols is enabled.
- Use the **no ip nat translation dns** command to disable ALG for DNS.
- Use the **no ip nat translation ftp** command to disable ALG for FTP.
- Use the **no ip nat translation h323** command to disable ALG for H323.
- Use the **no ip nat translation pptp** command to disable ALG for PPTP.
- Use the **no ip nat translation tftp** command to disable ALG for TFTP.
- Use the **no ip nat translation rtsp** command to disable ALG for RTSP.
- Run the **no ip nat translation sip** command to disable ALG for SIP.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic NAT	(Mandatory) It is used to configure one-to-one NAT for internal PCs to connect to a WAN.	
	ip nat inside	Configures the interface to connect to the intranet.
	ip nat outside	Configures the interface to connect to the extranet.
	(Optional) It is used to configure static NAT.	
	ip nat inside source static *local-ip global-ip* [**permit-inside**] [**netmask** *mask*] [**match** interface]	Defines static internal source address translation.
	(Optional) It is used to configure dynamic NAT.	

Configuration	Description and Command	
	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, multiple IP addresses are defined. The number of address pools to be defined depend on the number of intranet users.
	access-list *access-list-number* **permit** *ip-address wildcard*	Defines an ACL so that only addresses matching this ACL are translated.
	ip nat inside source list *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**]	Defines dynamic source address translation. The *overload* parameter is only used to ensure compatibility with mainstream vendors' devices.
Configuring NAPT	(Mandatory) It is used to configure NAPT.	
	ip nat inside	Configures the interface to connect to the intranet.
	ip nat outside	Configures the interface to connect to the extranet.
	(Optional) 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 static internal source address translation.
	(Optional) 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, 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 dynamic source address translation. The *overload* parameter is only used to ensure compatibility with mainstream vendors' devices.
Configuring Overlapping NAT	(Mandatory) It is used to enable overlapping NAT.	
	ip nat inside	Configures the interface to connect to the intranet.
	ip nat outside	Configures the interface to connect to the extranet.

Configuration	Description and Command	
	ip nat inside source static *local-ip global-ip*	Configures internal source address translation.
	⚠ (Optional) It is used to configure static NAT.	
	ip nat outside source static *global-ip local-ip*	Configures static NAT.
	⚠ (Optional) 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 dynamic source address translation. The *overload* parameter is only used to ensure compatibility with mainstream vendors' devices.
Configuring TCP Load Balancing	⚠ (Mandatory) It is used to configure destination address polling and translation.	
	ip nat inside	Configures the interface to connect to the intranet.
	ip nat outside	Configures the interface to connect to the extranet.
	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 an extended ACL based on destination IP address matching.
	ip nat inside destination list *access-list-number* **pool** *pool-name*	Defines dynamic internal destination address translation.
Configuring ALG	⚠ (Optional) 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) 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.

Configuration	Description and Command	
Configuring the Interval at Which Gratuitous ARP Packets Are Sent	(Optional) 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 needs to be configured for an intranet to communicate with an extranet by translating an internal private IP address into a globally unique IP address. You can configure static or dynamic NAT or both to implement interconnection.

Notes

- At least one internal interface and one external 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 Step

Configuring the NAT Internal Interface

- Mandatory.
- Configure the LAN interface to connect to the intranet as the NAT internal interface unless otherwise stated.

Configuring the NAT External Interface

- Mandatory.
- Configure the WAN interface to connect to the extranet as the NAT external interface unless otherwise stated.

Configuring Static NAT

- Optional.
- Configure static NAT in global configuration mode when a small number of users on the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional.
- Configure dynamic NAT in global configuration mode when a large number of users on the intranet need to access the extranet.

Verification

N/A

Commands

Configuring the NAT Internal Interface and External Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: Indicates the internal interface. **outside**: Indicates the external interface.
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external 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*: Indicates the internal address. *global-ip*: Indicates the external address. **permit-inside**: Permits intranet users to access the host specified by *local-ip* using the address specified by *global-ip*. **netmask** *mask*: Indicates the 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 an Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: Indicates the name of the address pool. *start-ip*: Indicates the start IP address. *end-ip*: Indicates the end IP address. **netmask** *mask*: Indicates the network mask of addresses. **prefix-length** *prefix-length*: Indicates the length of the network mask of 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 regardless of whether **rotary** is configured. The **rotary** parameter is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

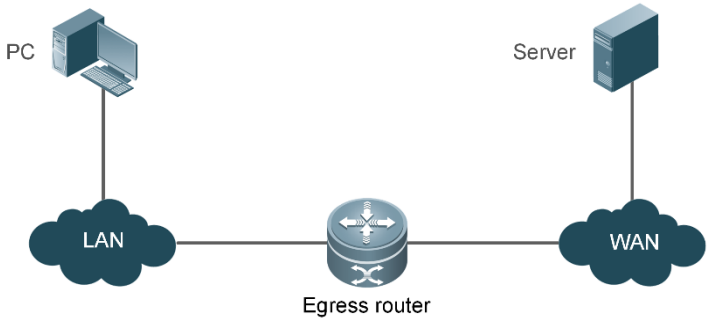
Configuring Dynamic NAT

Command	**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *address-pool-name* } [**overload**]
Parameter Description	*access-list-number*: Specifies the ACL number. **pool** *pool-name*: Specifies the name of an address pool.

	interface *interface-type interface-number*: Implements NAPT using the address of the external global interface. **overload**: Indicates that each global address in the address pool can be reused for NAPT. Global addresses are reused even if this parameter is not configured. This parameter is used to ensure compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Enabling Intranet Users to Access an Extranet Server

Scenario Figure 1-1	
Configuration Steps	● Configure **ip nat inside** on the internal interface. ● Configure **ip nat outside** on the external 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 internal or external interface is not configured.
- The ACL configuration is incorrect.

1.4.2 Configuring NAPT

Networking Requirements

Traditional NAT employs one-to-one address mapping, which fails to meet requirements of all hosts on intranets to communicate with extranets. For example, when the intranet lacks global IP addresses or even does not apply for global IP addresses, or has only one global IP address to connect to an ISP but a large number of hosts on the intranet need to access the Internet, NAPT is necessary in such scenarios.

Multiple internal local addresses can be mapped to one internal global address using NAPT.

Notes

- At least one internal interface and one external 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 Step

Configuring the NAT Internal Interface

- Mandatory.
- Configure the LAN interface to connect to the intranet as the NAT internal interface unless otherwise stated.

Configuring the NAT External Interface

- Mandatory.
- Configure the WAN interface to connect to the extranet as the NAT external interface unless otherwise stated.

Configuring Static NAPT

- Optional.
- Configure static NAPT in global configuration mode when a small number of users on the intranet need to access the extranet.

Configuring Dynamic NAPT

- Optional.
- Configure dynamic NAPT in global configuration mode when a large number of users on the intranet need to access the extranet.

Verification

N/A

Commands

Configuring the NAT Internal or External Interface

Command	ip nat { inside | outside }

Parameter Description	**inside**: Indicates the internal interface. **outside**: Indicates the external interface.
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external 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**: Indicates UDP. **tcp**: Indicates TCP. *local-ip*: Indicates the internal address. *local-port*: Indicates the internal local port. *global-ip*: Indicates the external address. *global-port*: Indicates the external global port. **permit-inside**: Permits intranet users to access the host specified by *local-ip* using the address specified by *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 value specified by *global-ip* unless **permit-inside** has been configured. If **permit-inside** is not configured, internal hosts can access the internal server by using the value specified by *local-ip* only.

Configuring an Address Pool

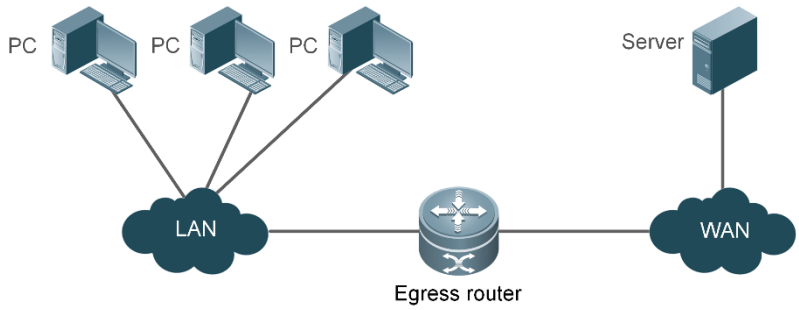
Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: Indicates the name of the address pool. *start-ip*: Indicates the start IP address. *end-ip*: Indicates the end IP address. **netmask** *mask*: Indicates the network mask of addresses. **prefix-length** *prefix-length*: Indicates the length of the network mask of 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 regardless of whether **rotary** is configured. The **rotary** parameter 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*: Specifies an ACL number. **pool** *pool-name*: Indicates the name of the address pool. **interface** *interface-type interface-number*: Implements NAPT using the global address of the external interface. **overload**: Indicates that each global address in the address pool can be reused for NAPT. 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 1-2	
Configuration Steps	● Configure **ip nat inside** on the internal interface. ● Configure **ip nat outside** on the external 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 internal or external interface is not configured.
- The ACL configuration is incorrect.

1.4.3 Configuring Overlapping NAT

Networking Requirements

Address overlapping indicates that 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. Two overlapping network hosts cannot communicate, because both hosts consider that the peer host is located on the local network. Overlapping NAT is especially designed to implement communication between two networks with the same IP address. After overlapping NAT is configured, an extranet host address will be represented as another host address on 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 Step

↘ Configuring the NAT Internal Interface

- Mandatory.
- Configure the LAN interface to connect to the intranet as the NAT internal interface unless otherwise stated.

↘ Configuring the NAT External Interface

- Mandatory.
- Configure the WAN interface to connect to the extranet as the NAT external interface unless otherwise stated.

↘ Configuring Static Translation of External Source Addresses

- Optional.

- Configure static translation of external source addresses in global configuration mode when a small number of users on the extranet need to access the intranet.

Configuring Dynamic Translation of External Source Addresses

- Optional.
- Configure dynamic translation of external source addresses in global configuration mode when a large number of users on the extranet need to access the intranet.

Configuring an ACL

- The ACL configuration is mandatory when dynamic source address mapping is used.
- Restrict the range of users requiring source address translation on the intranet.

Configuring a Static Route

- Mandatory.
- Specify the network egress after internal destination address translation.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: Indicates the internal interface. **outside**: Indicates the external interface.
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the external interface and the internal interface and the data packet meets a certain rule. Therefore, at least one internal interface and one external interface need to be configured on the device.

Configuring Static Translation of External Source Addresses

Command	**ip nat outside source static** *global-ip local-ip*
Parameter Description	*global-ip*: Indicates the external global address. *local-ip*: Indicates the internal local address.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Static Translation of the External 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*: Indicates the protocol number. *global-ip*: Indicates the external global address.

	global-port: Indicates the external global port. *local-ip*: Indicates the internal local address. *local-port*: Indicates the internal local port.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring an Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: Indicates the name of the address pool. *start-ip*: Indicates the start IP address. *end-ip*: Indicates the end IP address. **netmask** *mask*: Indicates the network mask of addresses. **prefix-length** *prefix-length*: Indicates the length of the network mask of 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 regardless of whether **rotary** is configured. The **rotary** parameter is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

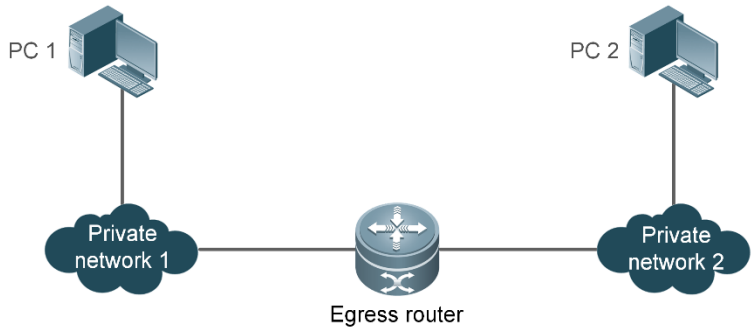
Configuring Dynamic Translation of External Source Addresses

Command	**ip nat outside source list** *access-list-number* **pool** *pool-name*
Parameter Description	*access-list-number*: Indicates the ACL number. **pool** *pool-name*: Indicates the name of the address pool.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

The following configuration example describes the configuration related to static translation of external source addresses.

Static Translation of External Source Addresses

Scenario **Figure 1-3**	
Configuration Steps	● Configure **ip nat inside** on the internal interface. ● Configure **ip nat outside** on the external interface. ● Configure a rule for dynamic translation of internal source addresses. ● Configure a rule for static translation of external source addresses.

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 internal or external interface is not configured.
- The ACL configuration is incorrect.
- No static route is configured or no IP address is configured for the external 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 heavy, multiple hosts can be deployed to implement TCP service load balancing. In this case, NAT can be used to address this issue. 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 Step

Configuring the NAT Internal Interface

- Mandatory.
- Configure the LAN interface to connect to the intranet as the NAT internal interface unless otherwise stated.

Configuring the NAT External Interface

- Mandatory.
- Configure the WAN interface to connect to the extranet as the NAT external interface unless otherwise stated.

Configuring Dynamic Translation of Internal Destination Addresses

- Mandatory.
- Configure dynamic translation of internal destination addresses in global configuration mode for TCP load balancing.

Verification

N/A

Commands

Configuring the NAT Internal and External Interfaces

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: Indicates the internal interface. **outside**: Indicates the external interface.
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external interface need to be configured on the device.

Configuring an Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *netmask* | **prefix-length** *prefix-length* } [**type rotary**]

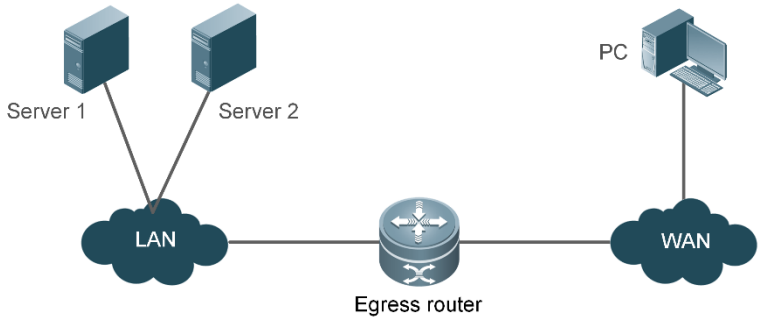
Parameter Description	*pool-name*: Indicates the name of the address pool. *start-ip*: Indicates the start IP address. *end-ip*: Indicates the end IP address. **netmask** *mask*: Indicates the network mask of addresses. **prefix-length** *prefix-length*: Indicates the length of the network mask of addresses. **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 regardless of whether **rotary** is configured. The **rotary** parameter is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	

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	

Configuration Example

Enabling Extranet User to Access an Intranet Server

Scenario **Figure 1-4**	
Configuration Steps	● Configure **ip nat inside** on the internal interface. ● Configure **ip nat outside** on the external interface. ● Configure a rule for dynamic internal 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 internal or external 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 preceding 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

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, problems may occur. ALG technology can parse application layer packet information and perform address translation for multi-channel protocols, so as to translate or process IP addresses or ports requiring address translation or some fields requiring special processing, thereby guaranteeing application layer communication.

Notes

- At least one internal interface and one external interface need to be configured during the ALG configuration.
- The newly configured NAT rules take effect on new flows only but not on any existing flows.

Configuration Step

↘ Configuring the NAT Internal Interface

- Mandatory.
- Configure the LAN interface to connect to the intranet as the NAT internal interface unless otherwise stated.

↘ Configuring the NAT External Interface

- Mandatory.

- Configure the WAN interface to connect to the extranet as the NAT external interface unless otherwise stated.

Configuring Static NAT

- Optional.
- Configure static NAT in global configuration mode when a small number of users on the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional.
- Configure dynamic NAT in global configuration mode when a large number of users on the intranet need to access the extranet.

Configuring ALG

- Optional.
- The ALG configuration is mandatory if DNS, FTP, TFTP, PPTP, H323, RTSP, or SIP requires communication through NAT transversal.

Verification

N/A

Commands

Configuring the NAT Internal and External Interfaces

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: Indicates the internal interface. **outside**: Indicates the external interface.
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the external interface and the internal interface and the data packet meets a rule. Therefore, at least one internal interface and one external 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*: Indicates the internal address. *global-ip*: Indicates the external address. **permit-inside**: Permits intranet users to access the host specified by *local-ip* using *global-ip*. **netmask** *mask*: Indicates the 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 an Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: Indicates the name of the address pool. *start-ip*: Indicates the start IP address. *end-ip*: Indicates the end IP address. **netmask** *mask*: Indicates the network mask of addresses. **prefix-length** *prefix-length*: Indicates the length of the network mask of 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 regardless of whether **rotary** is configured. The **rotary** parameter is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Dynamic NAT

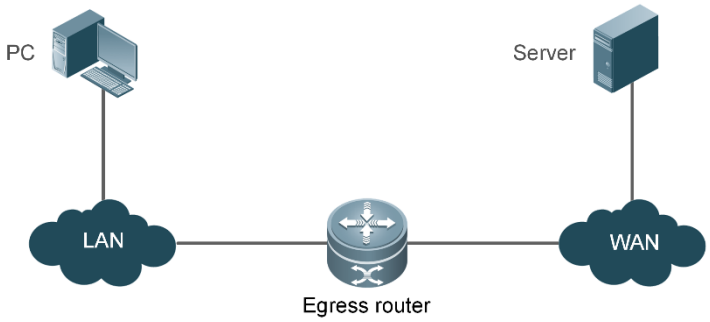
Command	**ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**]
Parameter Description	*access-list-number*: Specifies an ACL number. **pool** *pool-name*: Indicates the name of the address pool. **interface** *interface-type interface-number*: Implements NAPT using the global address of the external interface. **overload**: Indicates that each global address in the address pool can be reused for NAPT. 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

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 a UDP connection of the DNS application. The default value is 0. *port_num*: Defines 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 internal interface. ● Configure **ip nat outside** on the external 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 internal or external interface is not configured.
- The ACL configuration is incorrect.

1.4.6 Configuring Special NAT Applications

Networking Requirements

For some advanced applications of NAT, source addresses or destination addresses of some specific IP packets need to be modified.

Notes

- At least one internal interface and one external 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 Step

Configuring the NAT Internal Interface

- Mandatory.
- Configure the LAN interface to connect to the intranet as the NAT internal interface unless otherwise stated.

Configuring the NAT External Interface

- Mandatory.
- Configure the WAN interface to connect to the extranet as the NAT external interface unless otherwise stated.

Configuring Static NAT

- Optional.
- Configure static NAT in global configuration mode when a small number of users on the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional.
- Configure dynamic NAT in global configuration mode when a large number of users on the intranet need to access the extranet.

Configuring Special NAT Applications

- Optional.
- This configuration is mandatory if special address translation is required for communication of some applications.

Verification

N/A

Commands

Configuring the NAT Inside Interface and NAT Outside Interface

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: Indicates the internal interface. **outside**: Indicates the external interface.
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the external interface and the internal interface and the data packet meets a certain rule. Therefore, at least one internal interface and one external 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*: Indicates the internal address. *global-ip*: Indicates the external address. **permit-inside**: Permits intranet users to access the host specified by *local-ip* using *global-ip*. **netmask** *mask*: Indicates the 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 an Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: Indicates the name of the address pool. *start-ip*: Indicates the start IP address. *end-ip*: Indicates the end IP address. **netmask** *mask*: Indicates the network mask of addresses. **prefix-length** *prefix-length*: Indicates the length of the network mask of 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 regardless of whether **rotary** is configured. The **rotary** parameter is used to keep compatibility with Cisco commands.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuring Dynamic NAT

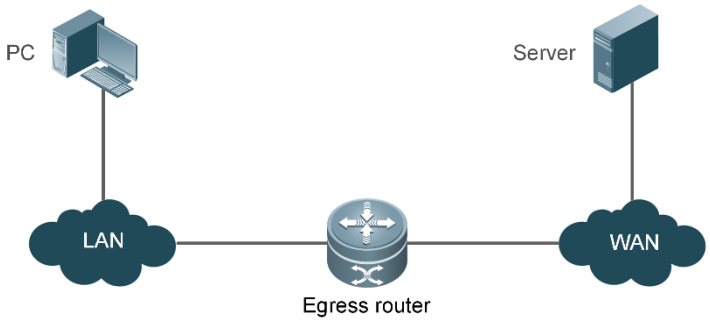
Command	**ip nat inside source list** *access-list-number* **pool** *address-pool* **ip nat inside source list** *access-list-number* { **interface** *interface-type interface-number* | **pool** *pool-name* } [**overload**]
Parameter Description	*access-list-number*: Specifies an ACL number. **pool** *pool-name*: Indicates the name of the address pool. **interface** *interface-type interface-number*: Implements NAPT using the global address of the external interface. **overload**: Indicates that each global address in the address pool can be reused for NAPT. 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

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*: Indicates the internal address. *global-ip*: Indicates the exteranl address. **dest-change** *ip-address port-num*: Changes the destination IP address and port of the packet that satisfies conditions. **src-change** *ip-address*: Changes 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 internal interface. ● Configure **ip nat outside** on the external 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 internal or external interface is not configured.

1.4.7 Configuring the Interval at Which Gratuitous ARP Packets Are Sent

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

- The NAT-enabled device is disabled from sending gratuitous ARP packets by default.
- Gratuitous ARP packets are sent to the external interface only.

Configuration Step

Configuring the NAT Internal Interface

- Mandatory.
- Configure the LAN interface to connect to the intranet as the NAT internal interface unless otherwise stated.

Configuring the NAT External Interface

- Mandatory.
- Configure the WAN interface to connect to the extranet as the NAT external interface unless otherwise stated.

Configuring Static NAT

- Optional.
- Configure static NAT in global configuration mode when a small number of users on the intranet need to access the extranet.

Configuring Dynamic NAT

- Optional.
- Configure dynamic NAT in global configuration mode when a large number of users on the intranet need to access the extranet.

Configuring the Interval at Which Gratuitous ARP Packets Are Sent

- Optional.
- The NAT-enabled device 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 Internal and External Interfaces

Command	**ip nat { inside | outside }**
Parameter Description	**inside**: Indicates the internal interface. **outside**: Indicates the external interface.
Command Mode	Interface configuration mode
Configuration Usage	NAT does not work on a data packet unless a route exists between the external interface and the internal interface and the data packet meets a certain rule. Therefore, at least one internal interface and one external 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*: Indicates the internal address. *global-ip*: Indicates the external address. **permit-inside**: Permits intranet users to access the host specified by *local-ip* using *global-ip*. **netmask** *mask*: Indicates the 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 an Address Pool

Command	**ip nat pool** *pool-name* [*start-ip end-ip*] { **netmask** *mask* | **prefix-length** *prefix-length* } [**type rotary**]
Parameter Description	*pool-name*: Indicates the name of the address pool. *start-ip*: Indicates the start IP address. *end-ip*: Indicates the end IP address. **netmask** *mask*: Indicates the network mask of addresses. **prefix-length** *prefix-length*: Indicates the length of the network mask of 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 regardless of whether **rotary** is configured. The **rotary** parameter 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**]

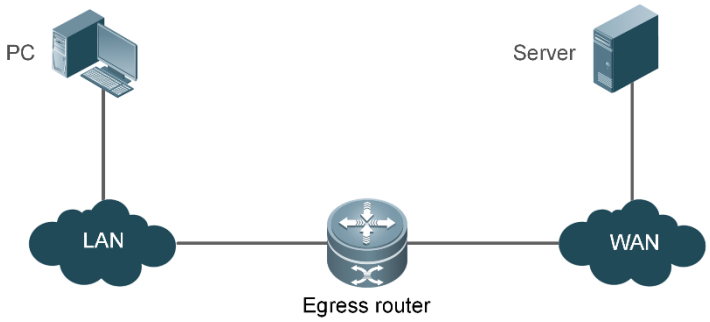
Parameter Description	*access-list-number*: Specifies an ACL number. **pool** *pool-name*: Indicates the name of the address pool. **interface** *interface-type interface-number*: Implements NAPT using the global address of the external interface. **overload**: Indicates that each global address in the address pool can be reused for NAPT. 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

Configuring the Interval at Which Gratuitous ARP Packets Are Sent

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 range is from 1 to 86400.
Command Mode	Global configuration mode
Configuration Usage	N/A

Configuration Example

Sending Gratuitous ARP Packets Regularly

Scenario **Figure 1-11**	
Configuration Steps	● Configure **ip nat inside** on the internal interface. ● Configure **ip nat outside** on the external interface. ● Configure a dynamic NAT rule. ● Configure 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.
- The NAT rule is incorrect.

1.5 Monitoring

Displaying

Command	Function
show ip nat translations [*acl_num*] [**gre** | **icmp** | **tcp** | **udp**] [**verbose**] [**vrf** *vrf_name*]	Displays NAT translation.

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.

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 located in different subnets, they need a DHCP relay to forward DHCP request and reply packets.

Protocols and Standards

- RFC 2131: Dynamic Host Configuration Protocol
- RFC 2132: DHCP Options and BOOTP Vendor Extensions
- RFC 3046: DHCP Relay Agent Information Option

1.2 Applications

Application	Description
Providing the DHCP Service on a LAN	IP addresses are assigned to clients on a local area network (LAN).
Enabling the DHCP Client	The downstream device is enabled with the DHCP client function.
Applying the DHCP Server in an MPLS Scenario	The DHCP server is deployed in L2VPN and L3VPN scenarios.
Applying an AM Rule on the DHCP Server	The DHCP server is deployed in a super-VLAN.
Applying the DHCP Relay Agent on a Wired Network	The DHCP relay agent allows users from different network segments to request IP addresses for accessing the Internet from a wired network.
Deploying the DHCP Relay Agent on a WLAN	The DHCP relay agent allows users from different network segments to request IP addresses for accessing the Internet from a WLAN.
Applying an AM Rule on the DHCP Relay	In a super-VLAN, users from different network segments request IP addresses.
Applying Address Assignment in a Cluster	Address assignment is balanced in a cluster.
Preferentially Using the DNS Addresses Obtained from an External DHCP Server in Externally on a WLAN	On a WLAN, the DNS address obtained from an external DHCP server is preferentially used on a WLAN.
Applying Class Rules on the DHCP Server	The DHCP server matches packets against class rules to obtain IP addresses in a specified network segment.

1.2.1 Providing the DHCP Service on a LAN

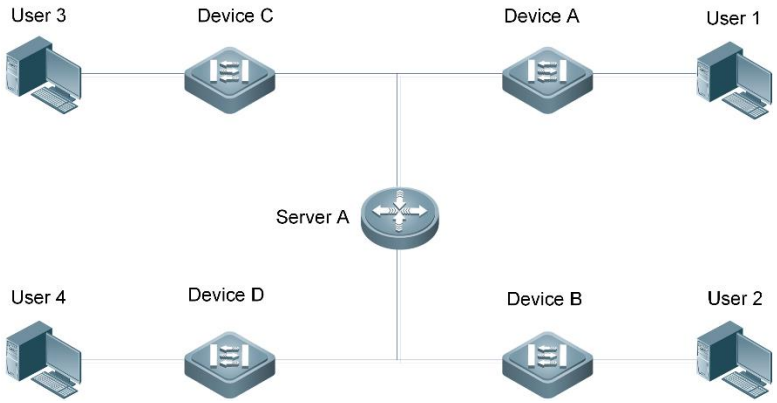
Scenario

Assign IP addresses to four users on a LAN.

For example, assign IP addresses to User1, User2, User3, and User4, as shown in the following figure.

- The four users are connected to server S through devices A, B, C, and D.

Figure 1-1



Remarks	Server A is an egress gateway used as the DHCP server. Devices A, B, C and D are access devices that provide Layer 2 transparent transmission. User1, Use2, User3, and User4 are LAN users.

Deployment

- Enable the DHCP server on Server A.
- Deploy Layer 2 VLAN transparent transmission on devices A, B, C and D.
- User1, Use2, User3, and User4 initiate DHCP client requests.

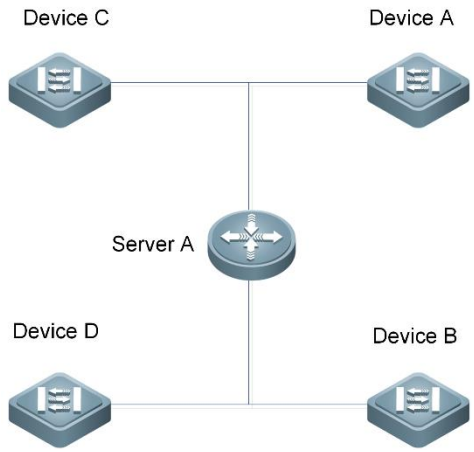
1.2.2 Enabling the DHCP Client

Scenario

Access switches A, B, C, and D on a LAN request server S to assign IP addresses.

For example, enable the DHCP client on the interfaces of devices A, B, C and D to request IP addresses, as shown in the following figure.

Figure 1-2



Remarks	Server A is an egress gateway working as a DHCP server. Devices A, B, C, and D are access devices with the DHCP client enabled on interfaces.

Deployment

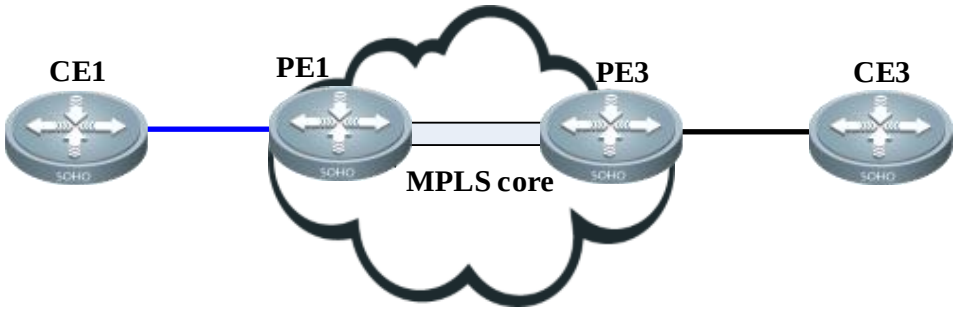
- Enable the DHCP server on server S.
- Enable the DHCP client on interfaces of devices A, B, C and D.

1.2.3 Applying the DHCP Server in an MPLS Scenario

Scenario

As shown in the following figure, if PE1 is a DHCP server and CE1 is a DHCP client in an L3VPN scenario, this situation is normal. If PE1 is a DHCP server and CE1 is a DHCP client in an L2VPN scenario, the AC interface on PE1 cannot be configured with an IP address, and consequently DHCP packets cannot reach the server.

Figure 1-3 MPLS Network Topology (L2VPN/L3VPN)



Remarks	In an MPLS core domain, PE1 and PE3 form a VPLS network. CE1 and CE3 are connected to the same VPLS through PE1 and PE3, respectively. CE1 is multi-homed to PE1 and PE3, and connected to the same VPLS domain. Enable the DHCP server on PE1.

Deployment

- Configure PE1 and PE3 in an L3VPN scenario, and enable the DHCP server on PE1.
- Enable the DHCP client on CE1.

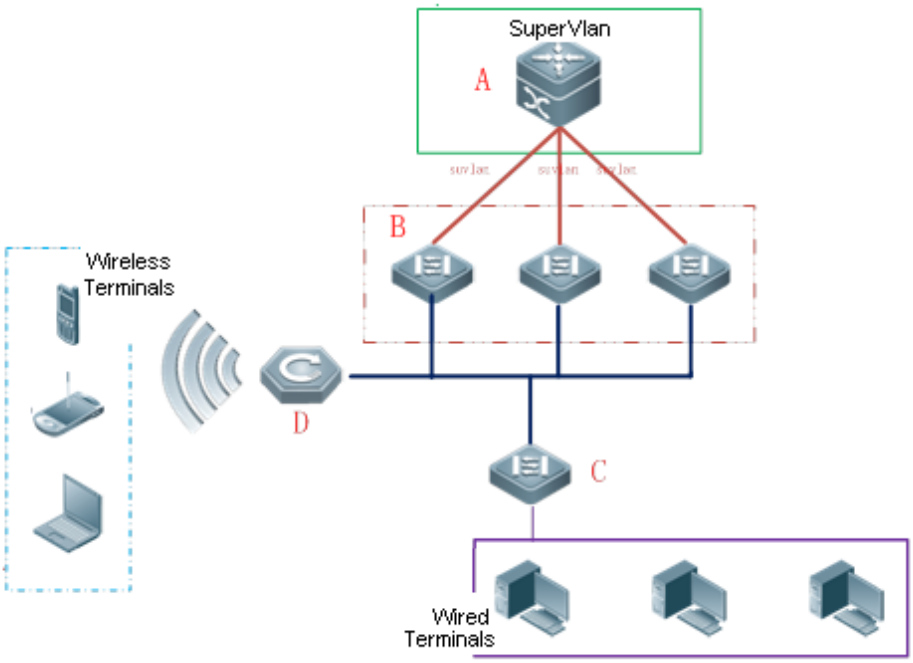
1.2.4 Applying an AM Rule on the DHCP Server

Scenario

As shown in Figure 1-4, create a super-VLAN, configure an AM rule and enable the DHCP server on the core switch A. B is an aggregation switch, C an access switch, and D a wireless access device. The requirements are as follows:

- Assign IP addresses dynamically based on the VLAN and interface.
- Assign IP addresses statically based on the VLAN.
- Assign IP addresses dynamically based on the default AM rule.

Figure 1-4 Applying an AM Rule on the DHCP Server



Deployment

- Configure an AM rule, enable the DHCP server, and create a super-VLAN on A.
- Create VLANs on B and C to transparently transmit DHCP packets from wired users to A to request IP addresses.
- Enable the wireless function on D to transparently transmit DHCP packets from wireless users to A to request IP addresses.

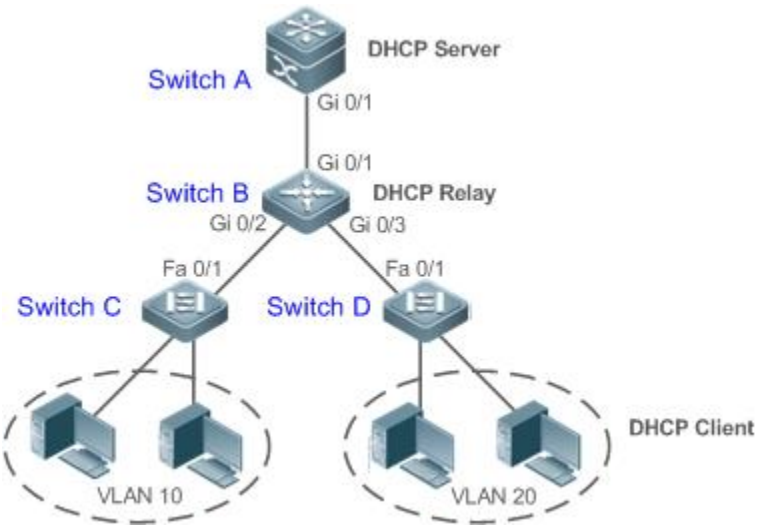
1.2.5 Applying the DHCP Relay Agent on a Wired Network

Scenario

As shown in the following figure, Switch C and Switch D function as access devices where PC users in VLAN 10 and VLAN 20 reside. Switch B functions as a gateway, and Switch A functions as a core device. The requirements are as follows:

- Switch A can function as a DHCP server to dynamically assign IP addresses from different network segments to users in different VLANs.
- Users connected to Switch C and Switch D can dynamically obtain IP addresses from different network segments.

Figure 1-5 DHCP Server Network Topology



Deployment

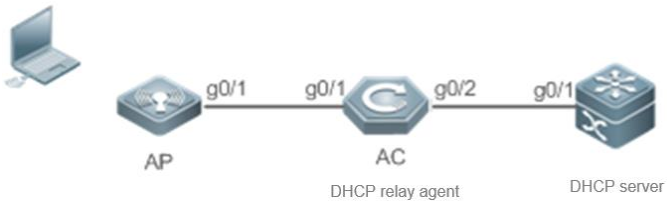
- Configure Layer 2 communication between Switch B and Switch C and between Switch B and Switch D.
- Specify a DHCP server address and enable the DHCP relay agent on Switch B.
- Create a DHCP address pool for users in VLAN 10 and VLAN 20 separately and enable the DHCP server on Switch A.

1.2.6 Deploying the DHCP Relay Agent on a WLAN

Scenario

Wireless users on different network segments obtain IP addresses to access the Internet.

Figure 1-6 DHCP Relay Agent



Remarks	The AP is a wireless access point. The AC is a wireless management device and DHCP relay agent. The DHCP server is a core device that is responsible for assigning IP addresses to wireless users.

Deployment

- Connect the AP to to the AC.
- Enable the DHCP relay agent on AC.
- Enable the DHCP server on the core device.

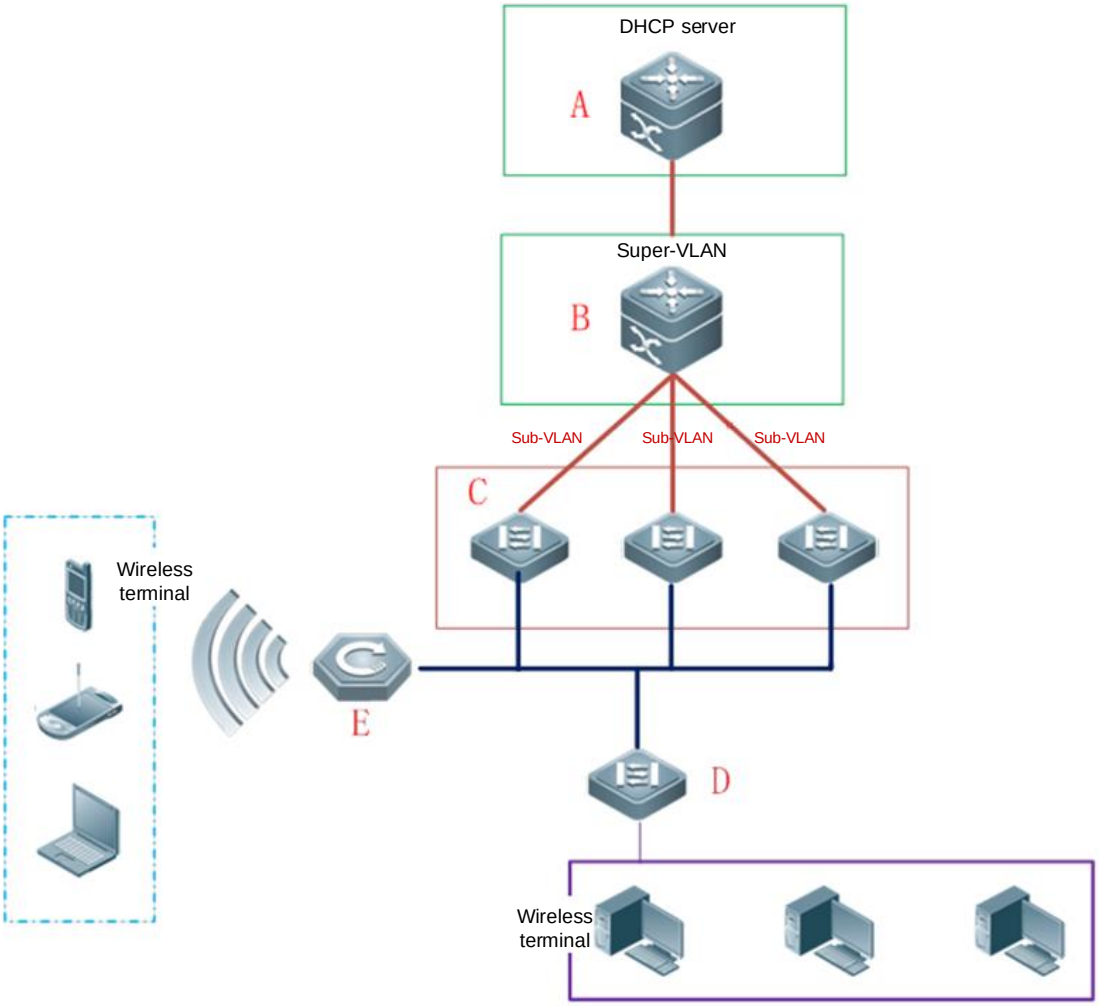
1.2.7 Applying an AM Rule on the DHCP Relay Agent

Scenario

As shown in Figure 1-7, A is a DHCP server, B a core switch configured with a super-VLAN, an AM rule, and the DHCP relay agent, C an aggregation switch, D an access switch, and E a wireless access device. The requirements are as follows:

- The AM rule relies on VLAN and interface configurations. According to this rule, the DHCP relay agent selects a subnet address as the Giaddress for relay packets, forwarding them to the DHCP server to request an IP address for the client.
- Based on the default AM rule, the DHCP relay agent selects a subnet address as the Giaddress for relay packets, forwarding them to the DHCP server to request an IP address for the client.

Figure 1-7 Applying AM Rule on the DHCP Relay Agent



Deployment

- Enable the DHCP server on A.
- Configure an AM rule, enable the DHCP relay agent, and create a super-VLAN on B.

- Create VLANs on C and D to transparently transmit DHCP packets from wired users to B to request IP addresses.
- Enable the wireless function on E to transparently transmit DHCP packets from wireless users to B to request IP addresses.

1.2.8 Applying Address Assignment in a Cluster

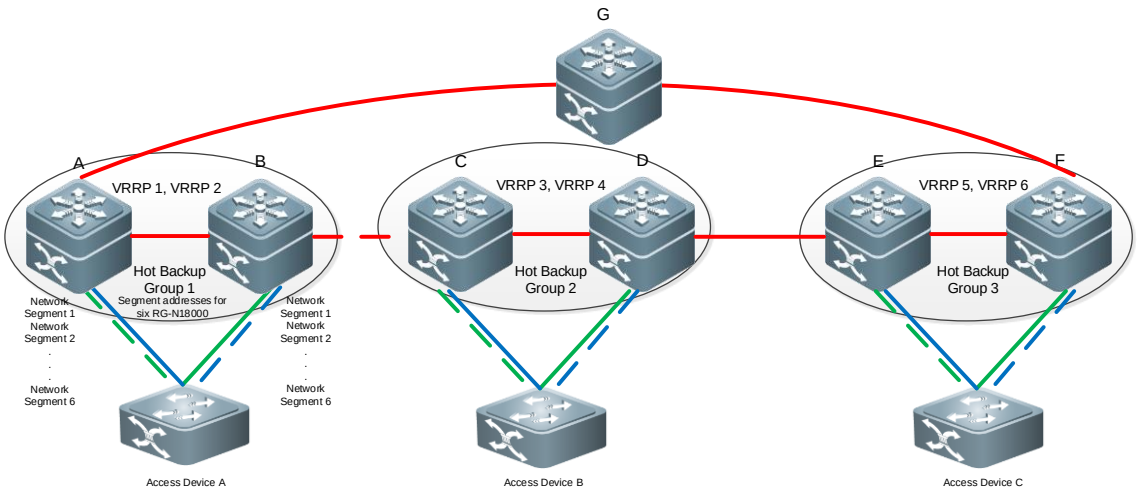
Scenario

As shown in the following figure, a cluster consists of the core ring, user VLAN, and management VLAN:

- Core ring: Seven RG-N18000 core switches form an ERPS ring, with two VRRP groups enabled on each of A/B, C/D, and E/F. That is, there are six virtual gateways. Device G serves as a backup, that is, physical gateway. Each gateway provides authentication and Internet access for 75,000 users. The DHCP server is enabled on A and B for AA hot standby, with each providing address assignment for 275,000 users. The DHCP server balances user services to the seven gateways, ensuring that each gateway provides the Internet access service for 75,000 users. DHCP snooping is enabled on each core device. Each core device encapsulates the corresponding gateway address only for DHCP packets of users served by the core device and forwards the DHCP packets to the DHCP server, without providing security functions. Each core device provides the authentication service for 75,000 users, providing responses for 5,600 users within 7s.
- User VLAN: A simple network mode is used, with a super-VLAN on the user side to ensure that the user's IP address and gateway address remain unchanged regardless of migration. Because the core ring is deployed on a large Layer 2 network, noise reduction is required to ensure the MAC or ARP entry capacity. ARP entries are not configured on the DHCP server of A and B, and DHCP snooping is used for forwarding based on the interface and VLAN to avoid ARP entry insufficiency.
- Management VLAN: This function is enabled on A and B for data hot standby of the DHCP server, and is enabled on A to G for device status monitoring through BFD.

The access loop consists of access device A, core device A, and core device B. Packets are distributed through REUP.

Figure 1-8 Integrated Address Assignment Network Topology



Remarks	A and B function as core devices and form VRRP group 1, and are enabled with the DHCP server. C and D function as core devices and form VRRP group 2. E and F function as core devices and form VRRP group 3. G is a backup.

Deployment

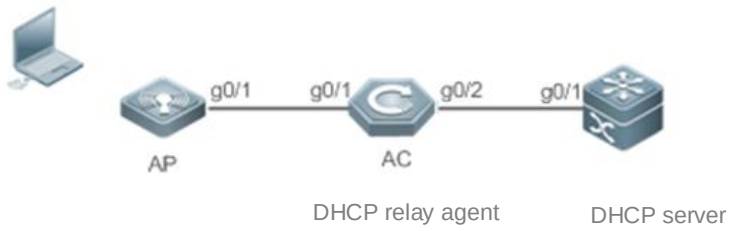
- On A and B, enable the DHCP server, enable the dedicated hot standby channel, and configure BFD.
- Configure two VRRP groups as user gateways on each of A, B, C, D, E, and F.

1.2.9 Preferentially Using the DNS Addresses Obtained from an External DHCP Server in Externally on a WLAN

Scenario

When the WAN interface of a wireless fat AP operates in PPPoE or DHCP client mode, a DNS address can be automatically obtained from an external DHCP server and be configured on the local DHCP server, so that the user does not need to perform DNS configuration. When the fat AP serves as the DHCP server to allocate addresses, it preferentially uses the DNS address obtained from an external DHCP server.

Figure 1-9 Networking of the DHCP Server



Remarks	When an AP operates in fat AP mode and the WAN interface of the fat AP operates in PPPoE or DHCP client mode, the AP can obtain an IP address and a DNS address from an external DHCP server, and serves as the DHCP server to assign addresses to STAs.

Deployment

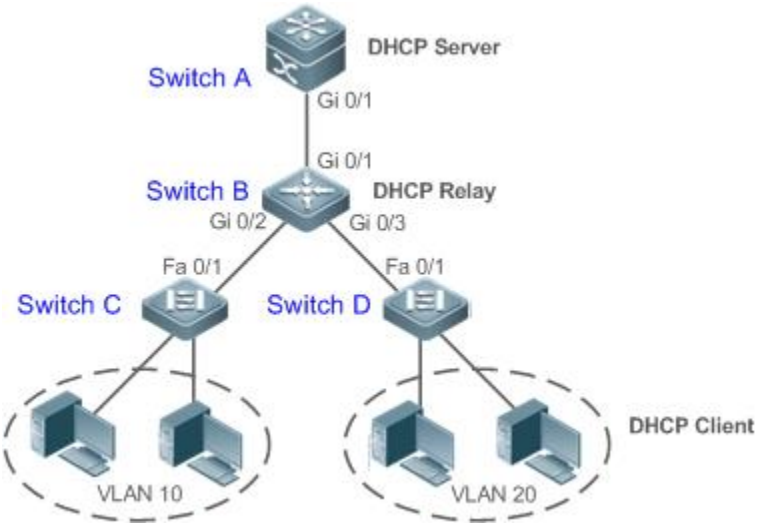
- Configure the AP as a fat AP and enable the PPPoE or DHCP client function on the WAN interface of the fat AP.
- Enable the DHCP server on the fat AP to assign addresses to STAs.
- Preferentially assign the DNS address obtained through PPPoE or the DHCP client to STAs.

1.2.10 Applying Class Rules on the DHCP Server

Scenario

On a LAN, users served by different access devices are assigned with addresses on different network segments to facilitate management of IP addresses and physical locations of terminals.

As shown in the following figure, two PCs belong to each of VLAN 10 and VLAN 20. Switch C and Switch D function as access devices, and each are configured with DHCP snooping and Option 82. Switch B functions as the relay agent and forwards packets to the DHCP server. Switch A used as the DHCP server is configured with the address pool and class rules. A terminal can match the corresponding class rule on the DHCP server based on Option 82 information imported by the access device, to obtain an IP address on a specified network segment.



Remarks	Switch C and Switch D function as access devices. Switch B functions as a gateway. Switch A functions as a core device.

Deployment

- Configure Switch A as the DHCP server and specify class rules.
- Configure Switch B as the DHCP relay agent.
- Configure Switch C as the access device and add DHCP snooping and Option 82.

1.3 Features

Basic Concepts

DHCP Server

Based on RFC 2131, the DHCP server assigns IP addresses to clients and manages these IP addresses.

DHCP Client

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

DHCP Relay Agent

When a DHCP client and a DHCP server are not in a same subnet, they need a DHCP relay agent to forward DHCP request and reply packets.

Lease

The 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 being leased to a client. Before a lease expires, a client needs to renew the lease through a DHCP 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 that is 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 the lease service for a DHCP client. For example, a public option include IP addresses of the default gateway, WINS server, and a DNS server. The DHCP server allows other options to be configured. Though most options are defined in RFC 2132, you can add user-defined options.

Overview

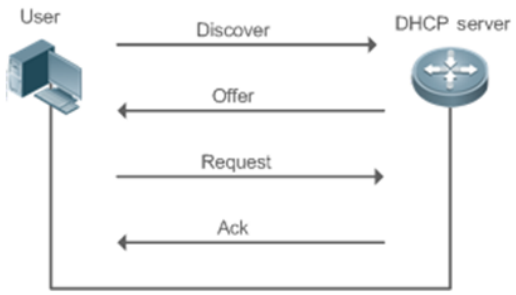
Feature	Description
DHCP Server	Enables the DHCP server on a device, so the device can assign IP addresses dynamically and pushes configurations to DHCP clients.
DHCP Relay Agent	Enables the DHCP relay agent on a device, so the device can forward DHCP request and reply packets across different network segments.
DHCP Client	Enables the DHCP client on a device, so it can obtain an IP address and the configuration automatically from a DHCP server.
AM Rule	Enables an AM rule on a device, so the device can assign IP addresses based on the rule.
Class Rule	Enables 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 1-10



A host requests an IP address through DHCP as follows:

1 A host broadcasts a DHCP Discover packet to find DHCP servers on a network.

2 DHCP servers unicast or broadcast (based attributes 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 request an IP address.

4 A DHCP server unicasts a DHCP ACK packet to the host to acknowledge the request.

A DHCP client may receive DHCP Offer packets from multiple DHCP servers, but usually it accepts only the first DHCP Offer packet. Besides, the address specified in a DHCP Offer packet is not necessarily assigned. Instead, it is retained by the DHCP server until a client sends a request.

To request an IP address, a client broadcasts a DHCP Request packet so that all DHCP servers sending DHCP Offer packets may receive the packet and release pre-allocated IP addresses.

If a DHCP Offer packet contains invalid configuration parameters, a client will send a DHCP Decline packet to the server to decline the configuration.

During negotiation, if a client does not respond to the DHCP Offer packets in a timely manner, servers will send DHCP NAK packets to the client and the client will reinitiate the process.

During network construction, the DHCP server has the following advantages:

- Low cost: Static IP address configuration costs more than DHCP-based address allocation configuration.
- Simplified configuration: Dynamic IP address assignment dramatically simplifies device configuration
- Centralized management: During configuration and management of multiple subnets, if there is any change on configuration parameters, you only need to change or update 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 the ping mechanism, and pushes the pool and address configuration to the client. The lease is saved locally for validity check upon lease renewal.

An address pool may carry various configuration parameters, including but not limited to the following:

- IP address range: indicates the range of IP addresses that are available.
- Gateway address: A maximum of eight gateway addresses are supported.
- DNS address: A maximum of eight DNS addresses are supported.
- Lease: Based on the lease, the device notifies clients of IP address aging and lease renewal request.

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. For an interface configured with the VRRP address and VRRP monitoring, the DHCP server only processes the DHCP clients' Request packets from a interface of the device in Master state, and discards packets from an interface of the device in backup state. If no VRRP address is configured, the DHCP server does not monitor the VRRP status, and all DHCP Request 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, Interfaces, and IP Address Ranges

After an IP address pool is deployed, the specified IP address range is assigned based on VLANs and interfaces. There are three scenarios:

1 Global configuration

2 Configuration based on VLANs, interfaces, and IP address ranges

3 Both scenarios 1 and 2: In scenario 1, addresses are assigned globally. In scenario 2, addresses in the specified IP address range are assigned only to clients of the specified VLANs and interfaces. In scenario 3, clients of the

specified VLANs and interfaces are assigned addresses in the specified IP address range, and other clients are configured with default global addresses.

Adding Trusted ARP

Trusted ARP prevents gateway-targeted ARP spoofing. Ruijie devices enabled with DHCP provide a command for delivering trusted ARP while assigning an address. After this function is enabled, the DHCP server delivers trusted ARP while assigning an IP address to the client to prevent ARP spoofing.

ARP-based Logout Detection

Ruijie devices enabled with DHCP provide a command to enable ARP-based logout detection. With this function 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 Bogus Server Detection

If a private DHCP server is deployed, a client interacts with this server while requesting an IP address and an incorrect address will be assigned to the client. This server is a bogus server. Ruijie devices enabled with DHCP provides a command to enable bogus server detection. After bogus server detection is enabled, the device will check whether DHCP packets carry Option 54 (Server Identifier Option). If the content of Option 54 is different from the actual DHCP server identifier, the IP address of the bogus server and interface receiving the packets will be recorded. Bogus server detection is only an after-event security function and cannot prevent an authorized DHCP server from assigning IP addresses to clients.

Preferentially Assigning the DNS Address Obtained from an External DHCP Server

When some interfaces on a device work in PPPoE or DHCP client mode, the interfaces can automatically obtain a DNS address from an external DHCP server and the address is configured on the local DHCP server. This eliminates the need to perform DNS configuration. When a device serves as the DHCP server, the device preferentially assigns STAs with the DNS address obtained from an external DHCP server.

ARP Check

The ARP check function is a supplement to the ping conflict detection function. If there is a STA with a static IP address is isolated at Layer 2 and the ping conflict detection function becomes ineffective (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 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 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 fails to apply for an IP address.

Related Configuration

Enabling the DHCP Server Globally

- By default, the DHCP server is disabled.

- Run the **service dhcp** command to enable the DHCP server.
- Run the **service dhcp** command globally to enable DHCP.

Configuring an Address Pool

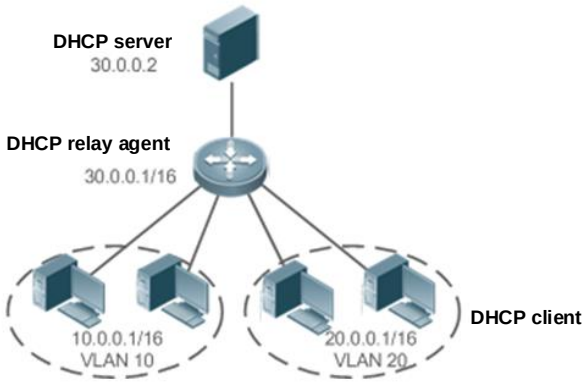
- By default, no address pool is configured.
- Run the **ip dhcp pool** command to configure an IP address range, a gateway address, and a DNS address.
- If no address pool is configured, no address will be assigned.

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 required. 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. This model achieves management of IP addresses across multiple network segments by only one DHCP server.

Figure 1-11 DHCP Relay Agent Scenario



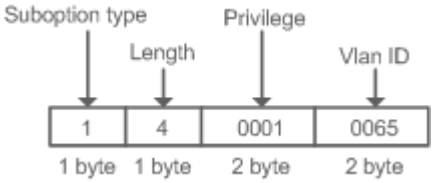
VLAN 10 and VLAN 20 correspond to segments 10.0.0.1/16 and 20.0.0.1/16 respectively. A DHCP server at 30.0.0.2 is on the network segment 30.0.0.1/16. To achieve management of dynamic IP addresses in VLAN 10 and VLAN 20 by the DHCP server, you only need to enable the DHCP relay agent on a gateway and configure IP address 30.0.0.2 for the DHCP server.

DHCP Relay Agent Information (Option 82)

As defined in RFC 3046, Option 82 can be added to indicate a DHCP client's network information when the DHCP relay agent is deployed, so that a DHCP server may assign IP addresses of various privileges based on more accurate information. The device supports the following schemes of relay agent information:

1 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. See Figure 1-12.

Figure 1-12 Option Format



2 Relay agent information option82: This scheme is used 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 Figure 1-13.

Figure 1-13 Agent Circuit ID

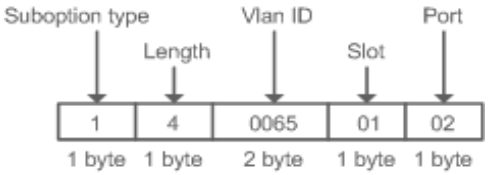
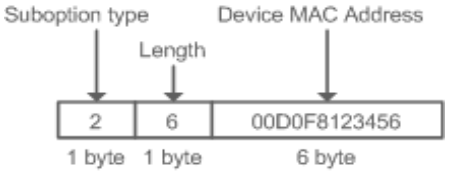


Figure 1-14 Agent Remote ID



3 Relay agent information Option 82: This scheme is used without correlation with other protocol modules. Compared with previous Option 82, the option supports the custom content, which may change. By default, a DHCP relay agent forms Option 82 based on the physical interface receiving DHCP packets, and device's MAC address and name. The option format is shown in Figure 1-15.

Figure 1-15 Option 82-circuit-id

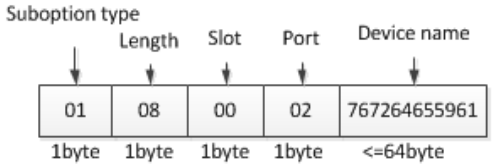
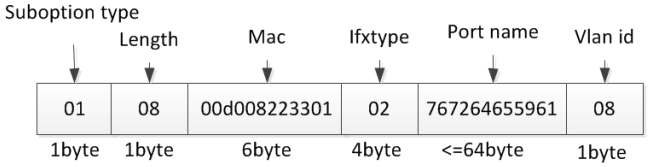


Figure 1-16 Option 82-remote-id



Server ID Check by the DHCP Relay Agent

- In DHCP scenarios, 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

the **server-id** option specifying a DHCP server. To alleviate 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 but not all DHCP servers.

Related Configuration

Enabling the DHCP Relay Agent

- By default, the DHCP relay agent is disabled.
- Run the **service dhcp** command to enable the DHCP relay agent.
- You must enable the DHCP relay agent before it works.

Configuring an IP Address for the DHCP Server

- By default, no IP address is configured for a DHCP server.
- You may run the **ip helper-address** command to configure an IP address for a DHCP server. The IP address can be configured globally or on a Layer 3 interface. A maximum of 20 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.
- Run the **ip dhcp relay information option82** command to enable DHCP Option82.

Enabling Server ID Check by the DHCP Relay Agent

- By default, server ID check by the DHCP relay agent is disabled.
- Run the **ip dhcp relay check server-id** command to enable server ID check by the DHCP relay agent.

Forcing a DHCP Relay Agent to Send Reply Packets

- By default, a DHCP relay agent is not forced to send Reply packets.
- Run the **ip dhcp relay force-send-reply-pack** command to force a DHCP relay agent to send Reply packets.

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. Then it sends lease renewal request packets in the Renew and Rebind processes of an aging period to request lease renewal.

Related Configuration

Enabling the DHCP Client on an Interface

- By default, the DHCP client is disabled.
- Run the **ip address dhcp** command in interface configuration mode to enable the DHCP client.

- You need to enable the DHCP client before enabling the DHCP service.
- The configuration takes effect on a Layer 3 interface, for example, an SVI or a routed interface.

Defining Common Option Fields on Interfaces

- In interface configuration mode, run the **ip dhcp client class-id** command to define the Option 61 field in Request packets.
- In interface configuration mode, run the **ip dhcp client client-id** command to define the Option 60 field in Request packets.
- In interface configuration mode, run the **ip dhcp client hostname** command to define the Option 12 field in Request packets.
- In interface configuration mode, run the **ip dhcp client lease** command to define the Option 51 field in Request packets.
- In interface configuration mode, run the **ip dhcp client option-list** command to define the Option 55 field in Request packets.
- The configuration takes effect on a layer 3 interface only, for example, an SVI or a routed interface.

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 AM Rule

Working Principle

An AM rule defines the range of IP addresses assigned to DHCP clients based on VLANs and interfaces. It can be used to quickly identify the VLAN and interface of a faulty DHCP client and effectively assign addresses. After an AM rule is configured, all DHCP clients from the configured VLAN and interfaces may obtain IP addresses. If no AM rule is configured but a default AM rule is configured, the client obtains an IP address from the default range. If no AM rule or default AM rule is configured, the client cannot obtain an IP address.

Related Configuration

Configuring an AM Rule in Global Configuration Mode

- In global configuration mode, run the **address-manage** command to enter the AM rule configuration mode.
- Run the **match ip default** command to configure a default AM rule.
- Run the **match ip** command to configure an AM rule based on VLANs and interfaces or interfaces.

1.3.5 Class Rule

Working Principle

When STAs apply for IP addresses from different APs, Option 82 information carried by the STAs is different. Class rules are used to match Option 82 information to assign IP addresses on 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 the 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 the DHCP Server

Configuration	Description and Command	
Configuring the DHCP Server to Dynamically Allocating IP Address	(Mandatory) It is used to enable the DHCP server to achieve dynamic IP address assignment.	
	service dhcp	Enables the 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 properties of an address pool.	
	default-router	Configures a default gateway of a client.
	lease	Configures an address lease.
	next-server	Configures a TFTP server address.
	bootfile	Configures a boot file of a client.
	domain-name	Configures a domain name of a client.
	dns-server	Configures a domain name server.
	netbios-name-server	Configures a NetBIOS WINS server.
	netbios-node-type	Configures a NetBIOS node type on a client.
	lease-threshold	Configures an alarm threshold of an address pool.
	option	Configures a user-defined option.
	pool-status	Enables or disables an address pool.
	update arp	Adds trusted ARP while assigning addresses from a pool.
	force-no-router	Configures a user-defined option.
	manage-address-pool	Enables or disables an address pool.
	user-address-pool	Cancels gateway allocation to the client.
	class	Configure class rules to be matched.

Configuration	Description and Command	
	address range	Configures assigned IP network segments after class rules are matched.
Configuring a Static IP Address	⚠ (Optional) It is used to statically assign an IP address to a client.	
	ip dhcp pool	Configures an address pool name and enters address pool configuration mode.
	host	Configures the IP address and subnet mask of a client host.
	hardware-address	Configures a client hardware address.
	client-identifier	Configures a unique client identifier.
	client-name	Configures a client name.
Configuring Global Properties of the DHCP Server	⚠ (Optional) It is used to configure properties of a DHCP server.	
	ip dhcp excluded-address	Configures an excluded IP address.
	ip dhcp force-send-nak	Configures the DHCP server to forcibly send an NAK packet.
	ip dhcp monitor-vrrp-state	Configures VRRP monitoring.
	ip dhcp ping packets	Configures the ping count.
	ip dhcp ping timeout	Configures a ping timeout.
	ip dhcp refresh arp	Configures the DHCP server to refresh trusted ARP entries.
	ip dhcp server detect	Configures bogus server detection.
Configuring AM Rules for the DHCP Server	⚠ (Optional) It is used to configure the AM rule of a DHCP server.	
	match ip default	Configures a default AM rule based on the VLAN and interface.
	match ip ip-address	Configures an AM rule based on the VLAN and interface.

Configuring the DHCP Relay Agent

Configuration	Description and Command	
Configuring Basic DHCP Relay Functions	⚠ (Mandatory) It is used to enable the DHCP relay agent.	
	service dhcp	Enables the DHCP relay agent.
	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 interface. This function cannot be used with the **dhcp option dot1x** command.	

Configuration	Description and Command	
	ip dhcp relay information option82	Enables DHCP Option 82.
Configuring Server ID Check by the DHCP Relay Agent	⚠ (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
Specifying the Source Address for DHCP Relay Packets	⚠ (Optional) It is used to specify a source address for DHCP relay packets.	
	ip dhcp relay source	Sspecifies a source address for DHCP relay packets.

Configuring the DHCP Client

Configuration	Description and Command	
Configuring the DHCP Client	⚠ (Mandatory) It is used to enable the 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 Packets 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 the DHCP Lease	⚠ (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.

1.4.1 Configuring the DHCP Server to Dynamically Allocating IP Addresses

Configuration Effect

The DHCP server provides all DHCP clients with DHCP service including assigning IP addresses and gateways.

Notes

The **service dhcp** command can be used to enable the DHCP server or DHCP relay agent, but a device cannot function both as a DHCP server and relay agent. 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 Step

↘ Enabling the DHCP Server

- Mandatory.
- It achieves dynamic IP address assignment.
- Run the **service dhcp** command in global configuration mode.

↘ Configuring an Address Pool

- Mandatory.
- It is used to create an IP address pool.
- Run the **ip dhcp pool** command in global configuration mode.

↘ Configuring the Network Number and Subnet Mask of the Address Pool

- Mandatory.
- It defines a range of dynamically assigned addresses.
- Run the **network** command in DHCP address pool configuration mode.

↘ Configuring the Default Gateway Address of Clients

- Optional.
- It is used to configure a gateway address.
- Run the **default-router** command in DHCP address pool configuration mode.

↘ Configuring the Address Lease

- Optional.
- It is used to configure an IP address lease, which is 24 hours by default.
- Run the **lease** command in DHCP address pool configuration mode.

↘ Configuring the 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 the Domain Name of Clients

- Optional.
- It is used to configure the domain name of a client.
- Run the **domain-name** command in DHCP address pool configuration mode.

Configuring the DNS Address

- Optional.
- It is used to configure a DNS address.
- Run the **dns** command in DHCP address pool configuration mode.

Configuring the NetBIOS WINS Server Address

- Optional.
- It is used to configure a NetBIOS WINS server address.
- Run the **netbios-name-server** command in DHCP address pool configuration mode.

Configuring the NetBIOS Node Type of Clients

- Optional.
- It is used to configure a NetBIOS node type.
- Run the **netbios-name-type** command in DHCP address pool configuration mode.

Configuring the Alarm Threshold of the Address Pool

- Optional.
- It is used to manage the number of leases. When a threshold (90% by default) is reached, an alarm will be generated.
- Run the **lease-threshold** command in DHCP address pool configuration mode.

Configuring the 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 the 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 trusted ARP during IP address assignment. It is disabled by default.
- Run the **update arp** command in DHCP address pool configuration mode.

Refraining from Assigning the Gateway Address

- Optional. It is used to refrain from assigning a gateway address during IP address assignment. It is disabled by default.
- Run the **force-no-router** command in DHCP address pool configuration mode.

Configuring an Address Pool Type

- It is used to identify the types of address pools, including management and user address pools.
- Run the **manage-address-pool** or **user-address-pool** command in address pool configuration mode.

Verification

Connect a DHCP client to a DHCP server.

- Check whether the client obtains configurations of the server.

Related Commands

Enabling the DHCP Server

Command	**service dhcp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Enable the DHCP server or DHCP relay agent. 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 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 DHCP address pool configuration mode.

Configuring the Network Number and Subnet Mask of the 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	DHCP address pool configuration mode

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 on the target network segment, the next address will be checked until a valid address is assigned. The device 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 on 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. If a client can connect to a server through a direct path or intermediate path, addresses may fail to be assigned. 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 the Default Gateway Address of Clients

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:* A maximum of 8 gateways can be configured. This parameter is optional.
Command Mode	DHCP address pool configuration mode
Usage Guide	Configure the address of a default gateway for 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 on the same network segment.

Configuring the Address Lease

Command	**lease** {*days* [*hours]* [*minutes*] | **infinite**}
Parameter Description	*days:* Defines a lease in the unit of days. *hours:* Defines a lease in the unit of hours, which is optional. You must define *days* before specifying *hours*. *minutes:* Defines a lease in the unit of minutes, which is optional. You must define *days* and *hours* before specifying *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 lease renewal. Otherwise, the IP address cannot be used after the lease is expired.

Configuring the Boot Server Address 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 the Boot File on Clients

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 an image file used when a client starts up. The file is usually an OS downloaded by a DHCP client.

Configuring the Domain Name of Clients

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 can 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 the DNS Address

Command	**dns-server** { *ip-address* [*ip-address2…ip-address8*] | **use-dhcp-client** *interface-type interface-number* }
Parameter Description	*ip-address:* Defines an IP address of a DNS server. You must configure at least one IP address. *ip-address2…ip-address8:* A maximum of eight DNS server addreses can be configured. This parameter is optional. **use-dhcp-client** *interface-type interface-number:* A DHCP client learns its DNS server through 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 the NetBIOS WINS Server Address

Command	**netbios-name-server** *address* [*address2…address8*]
Parameter Description	*address:* Defines an IP address of a WINS server. You must configure at least one IP address. *ip-address2…ip-address8:* A maximum of eight WINS server addresses can be configured. This parameter is optional.
Command Mode	DHCP address pool configuration mode

Usage Guide	WINS is a domain name service through which a Microsoft TCP/IP network resolves a NetBIOS 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 computers in the WINS database and on the network are consistent.

Configuring the NetBIOS Node Type of Clients

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. The 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: ● Broadcast node: For such a node, the NetBIOS name is resolved through broadcast. ● Peer-to-peer node: The client sends a resolution request to the WINS server. ● Mixed node: The client broadcasts a resolution request and sends the resolution request to the WINS server. ● 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 the Address Pool

Command	**lease-threshold** *percentage*
Parameter Description	*percentage*: Defines the alarm threshold of an address pool, in percentage. The value range is from 60 to 100.
Command Mode	DHCP address pool configuration mode
Usage Guide	Run this command to configure the alarm threshold of an address pool. 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 5 minutes.

Configuring User-Defined Options

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	DHCP allows the configuration to be transmitted to a host through 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 the 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	The device provides a command for you to enable or disable a DHCP address pool.

Adding Trusted ARP

Command	**update arp**
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	Trusted ARP is added when an address is assigned from a pool. Trusted ARP prevents ARP spoofing.

Refraining from Assigning the 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 and a gateway address, a DHCP server assigns an IP address and a gateway address to the client. Then no gateway address is sent to the client.

Configuring an Address Pool Type

Command	**manage-address-pool**
Parameter	N/A

Description	
Command Mode	DHCP address pool configuration mode
Usage Guide	Configure the address pool as a management address pool.

Command	**user-address-pool**
Parameter Description	N/A
Command Mode	DHCP address pool configuration mode
Usage Guide	Configure the address pool as a user address pool.

Configuration Example

Configuring Address Pool

Configuration Steps	• Define an address pool **net172**. • The network segment is 172.16.1.0/24. • The default gateway address is 172.16.1.254. • The address lease is 1 day. • Excluded 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 a Static IP Address

Configuration Effect

Assign specific IP addresses and push the configuration to specific DHCP clients.

Notes

N/A

Configuration Step (A)

Configuring the 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 global configuration mode.

Configuring the IP Address and Subnet Mask of Clients

- 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 the Hardware Address of Clients

- Optional.
- It is used to configure a MAC address.
- Run the **hardware** command in DHCP address pool configuration mode.

Configures the UID

- Optional.
- It is used to configure a static user identifier (UID).
- Run the **client-identifier** command in DHCP address pool configuration mode.

Configuring the 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 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.

Configuring Manual IP Address Binding

Command	**host** *ip-address* [*netmask*] **client-identifier** *unique-identifier* **client-name** *name*
Parameter	*ip-address:* Defines the IP address of a DHCP client.

Description	*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*: Defines a client name using ASCII characters, which is optional. The name excludes a domain name. For example, name a host **mary** but not **mary.rg.com**.
Command Mode	DHCP address pool configuration mode
Usage Guide	Address binding means mapping between an IP address and a client's MAC address. There are two types of address binding: ● Manual binding: Manual binding involves manually defining static mappings of IP addresses and MAC addresses in the DHCP server database. Manual binding functions as a special address pool. ● Dynamic binding: A DHCP server dynamically assigns an IP address from a pool to a client when it receives a DHCP Request packet, creating mapping between an IP address and the client's MAC address. To configure manual binding, you need to define a host address 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 but not a MAC address. For the codes of medium types, refer to *Address Resolution Protocol Parameters* in 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 numeral. Character string options: ● ethernet ● ieee802 Numeral 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 address is 20.1.1.1. ● The lease 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(config)#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 address 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 Step (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	Global configuration mode

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 the DHCP Server

Configuration Effect

Enable a server with specific functions, for example, ping and forcible NAK response.

Notes

Configuring the command may cause exceptions on other servers.

Configuration Step

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 an invalid address request with an NAK packet.
- Run the **ip dhcp force-send-nak** command in global configuration mode.

Configuring VRRP Status Monitoring

- Optional.
- When this function is configured, DHCP packets are processed by the master server.
- Run the **ip dhcp monitor-vrrp-state** command in global configuration mode.

Configuring the Ping Count

- Optional.
- Check address reachability with the **ping** command. The default value is 2.
- Run the **ip dhcp ping packet** command in global configuration mode.

Configuring Ping Timeout

- Optional.
- Check address reachability with the **ping** command. The default value is 500 ms.
- Run the **ip dhcp ping timeout** command in global configuration mode.

Refreshing Trusted ARP

- Configure a DHCP server to refresh trusted ARP entries 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 Bogus Server Detection

- Optional.
- Enable this function to log a bogus 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 an Excluded IP Address

Command	**ip dhcp excluded-address** *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address:* Indicates the start IP address. *high-ip-address:* Indicates the 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 (for example, addresses already assigned to the server or devices), you need to configure these addresses as excluded addresses. To configure a DHCP server, you are advised to configure excluded addresses to avoid address conflict and shorten detection time during address assignment.

Configuring Forcible NAK Response

Command	**ip dhcp force-send-nak**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	On 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 is on a different 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 is moved to another network, a DHCP server cannot find the lease record of the client and will not reply with a NAK packet. The client sends request packets continuously before obtaining an IP address again after timeout. Consequently, it takes a long time to obtain an IP address. This situation 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. Note that the command is disabled by default. If this function is enabled, only one DHCP server can be configured in a broadcast domain.

Configuring the Ping Count

Command	**ip dhcp ping packets** [*number*]
Parameter Description	*Number*: Indicates the ping count. The value range is from 0 to 10. The value 0 indicates the ping function is disabled. The default value is 2. This parameter is optional.
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 response, the server considers the address as idle and assigns it to a client. If there is a response, the server considers the address as occupied and assigns another address.

Configuring the Ping Timeout

Command	**ip dhcp ping timeout** *milliseconds*
Parameter Description	*milli-seconds:* Indicates the time that the DHCP server waits for a response to the ping operation, in milliseconds. The value range is from 100 to 10000.
Command Mode	Global configuration mode
Usage Guide	By default, if a DHCP server receives no response to the ping operation within 500 ms, the servers considers the IP address as available. You can run this command to change the time for a server to wait for a response.

Refreshing Trusted ARP Entries

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 ARP entris while assigning an IP address from the address pool. If a client clears the trusted ARP entries, the server will not reassign them. After this command is configured, a DHCP server may refresh trusted ARP entries according to addresses assigned from an address pool configured with **update arp**.

Configuring Bogus Server Detection

Command	**ip dhcp server detect**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, bogus server detection is disabled on a DHCP server. Run this command to enable bogus server detection.

Configuration Example

Configuring Ping Parameters

Configuration Steps	● Set the ping count to 5. ● Set the ping timeout to 800 ms.
	`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 an 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 AM Rules for the DHCP Server

Configuration Effect

Assign IP addresses according to an AM rules based on the interface and VLAN.

Notes

This function is supported on Ethernet interfaces, gigabit interfaces, as well as FR, PPP, and HDLC interfaces.

Configuration Step

Configuring Address Management

- Mandatory. Enter the address management mode.
- Run the **address-manage** command in address management configuration mode.

Configuring AM Rules

- Mandatory. Configure AM rules based on the port and VLAN.
- Run the **match ip** command in configuration mode.

Verification

Check whether clients in different VLANs and interfaces obtain valid IP addresses.

Related Commands

Configuring the Default Range

Command	**match ip default** *ip-address netmask*

Parameter Description	*ip-address:* Defines an IP address. *netmask:* Defines a subnet mask.
Command Mode	Address management mode
Usage Guide	After this command is configured, all DHCP clients without the VLAN and interface configured are assigned IP addresses from the default address range. If this command is not configured and no other VLAN or interface is configured, IP addresses are assigned according to the normal process.

Assigning Dynamic IP Address Based on the VLAN and Interface

Command	**match ip** *ip-address netmask interface-type interface-number* [**add** | **remove**] **vlan** *vlan-list*
Parameter Description	*ip-address:* Defines an IP address. *netmask:* Defines a subnet mask. *interface:* Defines an interface name. *add/remove:* Adds or deletes a specific VLAN. *vlan-list:* Indicates a VLAN index.
Command Mode	Address management mode
Usage Guide	After this command is configured, DHCP clients are assigned IP addresses from the default address range based on the VLAN and interface.

Assigning a Static IP Address Based on a VLAN

Command	**match ip** *ip-address netmask* [**add** | **remove**] **vlan** *vlan-list*
Parameter Description	*ip-address:* Defines an IP address. *netmask:* Defines a subnet mask. *add/remove:* Adds or deletes a specific VLAN. *vlan-list:* Indicates a VLAN index.
Command Mode	Address management mode
Usage Guide	In a super-VLAN, a client may be assigned a fixed static address regardless of the super-VLAN the client resides in. You do not need to configure an AM rule for this IP address based on all sub-VLANs and interfaces, but only configure an AM rule based on the VLAN. This rule takes effect for only static address assignment.

Configuration Example

Configuring an AM Rule

Configuration Steps	● Configure the default rule. ● Configure a rule based on a specific VLAN, interface, and address range. ● Configure a rule based on a specific VLAN and address range.

	`Hostname(config)# address-manage`
	`Hostname(config-address-manage)# match ip default 172.50.128.0 255.255.128.0`
	`Hostname(config-address-manage)# match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005`

	`Hostname(config-address-manage)# match ip 10.1.6.0 255.255.255.0 vlan 1006`
Verification	● Run the **show running-config** command to display the configuration.

	`Hostname# show running-config`
	`address-manage`
	`match ip default 172.50.128.0 255.255.128.0`
	`match ip 10.1.5.0 255.255.255.0 Gi5/3 vlan 1005`
	`match ip 10.1.6.0 255.255.255.0 vlan 1006`

1.4.5 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 located on different network segments.

Notes

- To enable the DHCP relay, you need to configure IPv4 unicast routing on a network.

Configuration Step

↘ Enabling the DHCP Relay

- Mandatory.
- Unless otherwise specified, you need to enable the DHCP relay on a device.

↘ Configuring an IP Address for the DHCP Server

- Mandatory.
- You need to configure an IP address for a DHCP server.

Verification

- Check whether a client obtains an IP address through the DHCP relay agent.

Related Commands

↘ Enabling the DHCP Relay

Command	**service dhcp**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

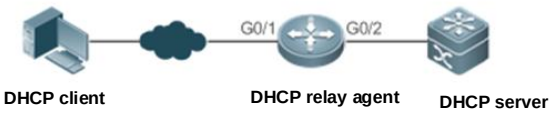
↘ Configuring an IP Address for the DHCP Server

Command	**ip helper-address** { **cycle-mode** | *A.B.C.D* }
Parameter Description	*cycle-mode*: Indicates that DHCP Request packets are forwarded to all DHCP servers. *A.B.C.D*: Indicates the IP address of a server.

Command Mode	Global configuration mode, interface configuration mode.
Usage Guide	The configured interface must be a Layer 3 interface, such as a routed interface, SVI, and loopback interface. The configured interface must be reachable through IPv4 unicast routing.

Configuration Example

Configuring the DHCP Relay in Wired Connection Mode

Scenario Figure 1-17	
Configuration Steps	● Enable a client to obtain an IP address through DHCP. ● Enable the DHCP Relay function on a DHCP relay agent. ● Configure DHCP Server.
A	Enable a client to obtain an IP address through DHCP.

B	● Enable the DHCP relay.
	`Hostname(config)# service dhcp`
	● Configure a global IP address of a DHCP server.
	`Hostname(config)# ip helper-address 172.2.2.1`
	● Configure an IP address for the interface connected to the client.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if)# ip address 192.1.1.1 255.255.255.0`
	● Configure an IP address for the interface connected to the server.
	`Hostname(config)# interface gigabitEthernet 0/2`
	`Hostname(config-if-gigabitEthernet 0/2)# ip address 172.2.2.2 255.255.255.0`

C	● Enable the DHCP server.
	`Hostname(config)# service dhcp`
	● Configure an address pool.
	`Hostname(config)# ip dhcp pool relay`
	`Ruijie (dhcp-config)#network 192.1.1.0 255.255.255.0`
	`Ruijie (dhcp-config)#default-router 192.1.1.1`
	● Configure an IP address for the interface connected to the relay agent.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-gigabitEthernet 0/2)# ip address 172.2.2.1 255.255.255.0`

Verification	Check whether the client obtains an IP address. ● Check whether the client obtains an IP address. ● Check the DHCP relay configuration.
A	● The user device obtains an IP address.
B	● After loginning to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display the DHCP relay configuration.

	Hostname# show running-config service dhcp ip helper-address 172.2.2.1 ! interface GigabitEthernet 0/1 ip address 192.1.1.1 255.255.255.0 ! interface GigabitEthernet 0/2 ip address 172.2.2.2 255.255.255.0 !

Common Errors

- The IPv4 unicast routing configuration is incorrect.
- The DHCP relay is disabled.
- No routing between DHCP relay agent and DHCP server is configured.
- No IP address is configured for the DHCP server.

1.4.6 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 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 the DHCP relay on a device.

Enables DHCP Option82

- By default, DHCP Option 82 is disabled.
- Run the **ip dhcp relay information option82** command to enable 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). The preceding three commands for adding Option 82 cannot be configured simultaneously, that is, only one command can take effect at a time. DHCP Option 82 is disabled if you delete an encapsulation format.

Configuration Example

↘ Enabling DHCP Option 82

Configuration Steps	● Enable DHCP Option 82.
	`Hostname(config)# ip dhcp relay information option82`
Verification	● After loginning to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display the DHCP relay configuration.
	`Hostname#show running-config | include ip dhcp relay` `ip dhcp relay information option82`

Common Errors

- Basic DHCP relay functions are not configured or fail to be configured.

1.4.7 Configuring Server ID Check by the DHCP Relay Agent

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, the DHCP Request packets are forwarded to all DHCP servers.

Notes

- You need to enable basic DHCP relay functions.

Configuration Steps

↘ Enabling Server ID Check by the DHCP Relay Agent

- By default, server ID check by the DHCP relay agent is disabled.
- Rrun the **ip dhcp relay check server-id** command to enable server ID check by the DHCP relay agent.

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 Server ID Check by the DHCP Relay Agent

Command	**ip dhcp relay check server-id**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Server ID Check by the DHCP Relay Agent

Configuration Steps	• Enable the DHCP relay. The configuration is not mentioned here. • Enable server ID check by the DHCP relay agent on an interface.
	`Hostname# configure terminal` `Hostname(config)# ip dhcp relay check server-id`
Verification	After loginning to the DHCP relay agent, run the **show running-config** command in privileged EXEC mode to display the DHCP relay configuration.

	`Hostname# show running-config | include check server-id`
	`ip dhcp relay check server-id`
	`Hostname#`

Common Errors

- Basic DHCP relay functions are not configured.

1.4.8 Specifying the Source Address for DHCP Relay Packets

Configuration Effect

- After you configure the **ip dhcp relay source** command on an interface, the source address of DHCP relay packets and the **Giaddr** field in DHCP packets can be specified.

Notes

- Basic DHCP relay functions must be configured.
- Only one source IP address can be specified for DHCP relay packets on an interface.
- This function must be used with Option 82 to assign a correct subnet address to the client.

Configuration Step

Specifying the Source Address for DHCP Relay Packets

No source address is specified for DHCP relay packets by default.

- Run the **ip dhcp relay source** *ip-address* command to specify the source address for DHCP relay packets.

Verification

- After a specific source address is configured on an interface, check that this source address is used as the source address of relay packets to be sent to the DHCP server and as the value of the **Giaddr** field in the DHCP packets.

Related Commands

Specifying the Source Address for DHCP Relay Packets

Command	**ip dhcp relay source** *ip-address*
Parameter Description	*ip-address*: Specifies the source IP address.
Command Mode	Interface configuration mode
Usage Guide	For a request packet sent by the DHCP relay agent, the destination address of a DHCP Reply packet sent by the DHCP server is the value of the **Giaddr** field in the Request packet. On some networks, multiple DHCP relay agents use the same interface IP address. In this case, you need to run this command on the DHCP relay agent to add another interface's IP address to the source address and **Giaddr** field of DHCP relay packets.

Configuration Example

Specifying the Source Address for DHCP Relay Packets

Configuration Steps	• Configure basic DHCP relay functions. The configuration is not mentioned here. • On a corresponding interface, specify a source address for DHCP relay packets.
	`Hostname(config-if-GigabitEthernet 0/1)# ip dhcp relay source 1.1.1.1`
Verification	• Log in to the DHCP relay agent. In privileged EXEC mode, run the **show running-config** command to display the DHCP relay configuration.

Common Errors

Basic DHCP relay functions are not configured or fail to be configured.

1.4.9 Configuring the DHCP Client

Configuration Effect

- Enable the DHCP client on a device so that it obtains IP addresses and configurations dynamically.

Notes

- The device supports the 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	• The Ethernet interface, PPP interface, FR interface, and HDLC interface can dynamically obtain IP addresses through DHCP.

Configuration Example

Configuring the DHCP Client

Configuration Steps	• Configure GigabitEthernet 0/1 to dynamically obtain an IP address through DHCP.
	`Hostname(config)# interface gigabitethernet 0/1` `Hostname(config-if-GigabitEthernet 0/1)#ip address dhcp`
Verification	• Run the **show running-config** command to display the configuration.
	`Hostname#show running-config | begin ip address dhcp` `ip address dhcp`

1.4.10 Defining Fields in Request Packets on Interfaces

Configuration Effect

- Enable the DHCP client on a device so that you can define option fields in Request packets.

Notes

- This feature is applicable to Layer 3 interfaces.

Configuration Step

Defining the Class-id Field in Request Packets

- Optional.
- Run the **ip dhcp client class-id** command to define the class-id field.

Defining the Client-id Field in Request Packets

- Optional.
- Run the **ip dhcp client client-id** command to define the client-id field.

Defining the Hostname Field in Request Packets

- Optional.

- Run the **ip dhcp client hostname** command to define the hostname field.

Defining the Lease Field in Request Packets

- Optional.
- Run the i**p dhcp client lease** command to define the lease field.

Defining the Option-list Field in Request Packets

- Optional.
- Run the **ip dhcp client option-list include** command 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 Packets

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 Packets

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 Packets

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 Packets

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 Packets

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 Packets

Configuration Steps	● Define the class-id field as **test** on GigabitEthernet 0/1.
	`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 Packets

Configuration Steps	● Define the client-id field as 0102.0304.0506 on GigabitEthernet 0/1.
	`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 Packets

Configuration Steps	● Define the hostname as **Hostname** on GigabitEthernet 0/1.
	`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 Packets

Configuration Steps	● Set the lease to 1 hour on GigabitEthernet 0/1.
	`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 Packets

Configuration Steps	● 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.

1.4.11 Releasing and Renewing the DHCP Lease

Configuration Effect

After dynamically obtaining IP addresses, DHCP clients release or renew DHCP leases.

Notes

This function applies to DHCP clients that obtain IP addresses dynamically. After interface addresses are released, run the **renew-dhcp** command to restore dynamic addresses or run the **no ip address dhcp** command to start a new IP address request.

Configuration Step

Enabling DHCP Clients to Release Dynamic IP Addresses

- Run the **release-dhcp** command in privilege EXEC mode.

Enabling DHCP Clients to Renew Dynamic IP Addresses

- Run the **renew-dhcp** command in privilege 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	Privilege 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	Privilege EXEC mode
Usage Guide	N/A

Configuration Example

Enabling DHCP Clients to Release Dynamic IP Addresses

Configuration Steps	● Release the dynamic IP addresses obtained by VLAN 100.
	`Hostname# release-dhcp vlan 100`
Verification	● Run the **show dhcp lease** command to display the configuration.

Enabling DHCP Clients to Renew Dynamic IP Addresses

Configuration Steps	● Renew the dynamic IP addresses obtained by VLAN 100.
	`Hostname# renew-dhcp vlan 100`
Verification	● Run the **show dhcp lease** command to display the configuration.

1.4.12 Configuring Class Rules of the DHCP Server

Configuration Effect

After class rules are configured, the DHCP server can assign IP addresses on different network segments to STAs based on Option 82 information carried by the STAs.

Notes

The configured class rules take effect only after they are associated with address pools.

Configuration Step

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 on different network segments need to be assigned based on option information.

Configuring 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.

Entering the Option 82 Configuration Mode

Command	**relay agent information**
Parameter Description	N/A
Command Mode	Global class configuration mode
Usage Guide	Run this command on the DHCP server to enter the Option 82 configuration mode.

Configuring Option 82 Information Matching Class Rules

Command	**relay-information hex**
Parameter Description	N/A
Command Mode	Global class configuration mode
Usage Guide	Run this command on the DHCP server to configure Option 82 information matching 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 on the DHCP server to associate configured class rules with destination address pools.

Configuring the IP Address Range Matching 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 on the DHCP server to configure the range of the IP address 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 Option 82 information sent from a specified interface as the matching rule.
	`Hostname(config-dhcp-class-relayinfo)# relay-information hex 010400100201020301020`
	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 010400100201020301020`
	`!`
	`ip dhcp pool test-pool`
	` class test-class`
	`  address range 1.1.1.10 1.1.1.20`

1.5 Monitoring

Clearing

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

Command	Description
clear ip dhcp binding { *address* | *}	Clears DHCP address binding.
clear ip dhcp conflict { *address* | *}	Clears DHCP address conflict.
clear ip dhcp history { * | *mac-address* }	Clears the address assigned by the DHCP server.
clear ip dhcp server statistics	Clears statistics on a DHCP server.
clear ip dhcp relay statistics	Clears statistics on a DHCP relay agent.
clear ip dhcp server rate	Clears statistics on DHCP server performance.
clear ip dhcp server detect	Clears information about a bogus DHCP server.

Displaying

Command	Description
show dhcp lease	Displays the DHCP lease.
show ip dhcp socket	Displays DHCP sockets.

Command	Description
show ip dhcp binding	Displays assigned IP addresses.
show ip dhcp pool	Displays created address pools.
show ip dhcp server statistic	Displays statistics on the DHCP server.
show ip dhcp relay statistic	Displays statistics on the DHCP relay agent.
show ip dhcp conflict	Displays conflicting addresses.
show ip dhcp history	Displays the DHCP lease history.
show ip dhcp identifier	Displays the address pool ID and address utilization of a DHCP server.
show ip dhcp server detect	Displays the bogus DHCP server.
show ip dhcp state ssid	Displays the address assignment status based on SSIDs.
show ip dhcp database	Displays the DHCP database backup status.

Debugging



Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug ip dhcp server agent	Debugs DHCP agent.
debug ip dhcp server ha	Debugs DHCP hot standby.
debug ip dhcp server pool	Debugs DHCP address pools.
debug ip dhcp server vrrp	Debugs VRRP.
debug ip dhcp server all	Debugs all DHCP servers.
debug ip dhcp client	Debugs DHCP packets.
debug ip dhcp relay	Debugs DHCP relay events.

1 Configuring DHCP Snooping

1.1 Overview

DHCP snooping monitors DHCP interaction packets between clients and servers to record and monitor users' IP addresses, filtering out unauthorized DHCP packets such as client requests and server responses. The valid user database created from DHCP snooping records can support security applications such as 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	On a network where multiple DHCP servers are deployed, DHCP clients are allowed to obtain network configurations only from authorized DHCP servers.
Guarding Against DHCP Packet Flooding	Malicious network users may frequently send DHCP Request packets.
Guarding Against Forged DHCP Packets	Malicious network users may send forged DHCP Request packets, for example, DHCP Release packets.
Guarding Against IP or MAC Address Spoofing	Malicious network users may send forged IP packets, for example, tampered source address fields of packets.
Preventing Private IP Addresses	Network users may use private IP addresses but not obtain them from the authorized DHCP server.
Detecting ARP Attacks	Malicious users forge ARP Reply packets to intercept packets during normal users' communication.

1.2.1 Guarding Against DHCP Service Spoofing

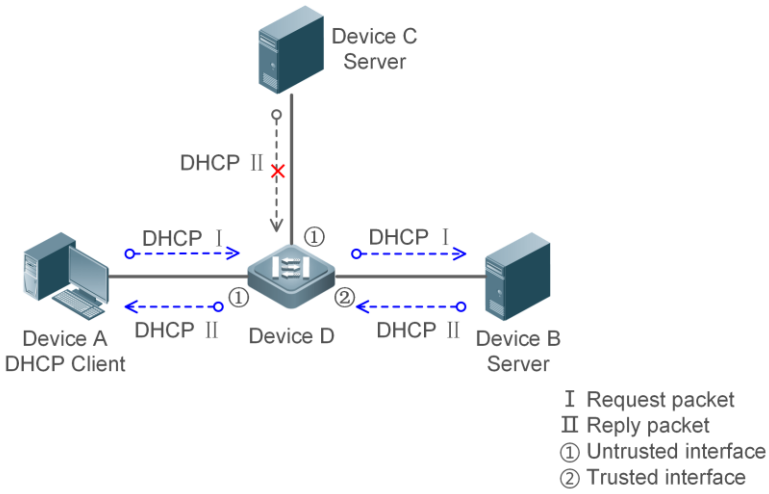
Scenario

Multiple DHCP servers may exist on a network. It is essential to ensure that user PCs obtain network configurations exclusively from the DHCP servers within a controlled area.

Figure 1-1 is used 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 Reply packets from trusted DHCP servers can be transmitted to the client.

Figure 1-1



Remarks:	Device D is an access device. Device A is a user PC. Device B is a DHCP server within the controlled area. Device C is a DHCP server out of the controlled area.

Deployment

- Enable DHCP snooping on Device D to realize DHCP packet monitoring.
- Configure the interface on Device D connecting to Device B as trusted to transfer Reply packets.
- Configure other interfaces on Device D as untrusted to filter Reply packets.

1.2.2 Guarding Against DHCP Packet Flooding

Scenario

Potential malicious DHCP clients on a network may send DHCP Request packets at high speed. As a result, authorized users cannot obtain IP addresses, and access devices are highly loaded or even break down. It is necessary to take actions to ensure network stability.

With the rate limiting function deployed, a DHCP client can only send DHCP Request packets at a rate below the limit.

- The Request packets from a DHCP client are sent at a rate below the limit.
- Packets sent at rates beyond the limit will be discarded.
- Associate DHCP snooping with ARP, and delete nonexistent entries.

Deployment

- Enable DHCP snooping on S to realize DHCP monitoring.
- Limit the rate of DHCP packets from untrusted interfaces.
- Associate DHCP snooping with ARP, and check whether users are online.

1.2.3 Guarding Against Forged DHCP Packets

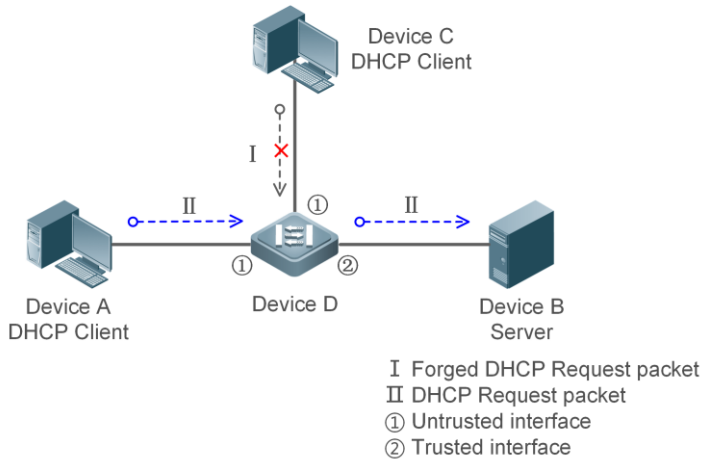
Scenario

Potential malicious clients on a network may forge DHCP Request packets, consuming available IP addresses from the servers and probably preempting IP addresses assigned to authorized users. Therefore, it is necessary to filter out unauthorized DHCP packets.

For example, as shown in Figure 1-2, DHCP Request packets sent from DHCP clients will be checked.

- The source MAC address fields of Request packets from DHCP clients must match **chaddr** fields of DHCP packets.
- Release and Decline packets from clients must match entries in the DHCP snooping binding database.

Figure 1-2



Remarks:	Device D is an access device. Device A and Device C are user PCs. Device B is a DHCP server within the controlled area.

Deployment

- Enable DHCP snooping on Device D to realize DHCP monitoring.
- Configure the interface on Device D connecting to Device B as trusted to transfer Reply packets.
- Configure other interfaces on Device D as untrusted to filter Reply packets.
- Enable source MAC address check on untrusted interfaces of Device D to filter out unauthorized packets.

1.2.4 Guarding Against IP or MAC Address Spoofing

Scenario

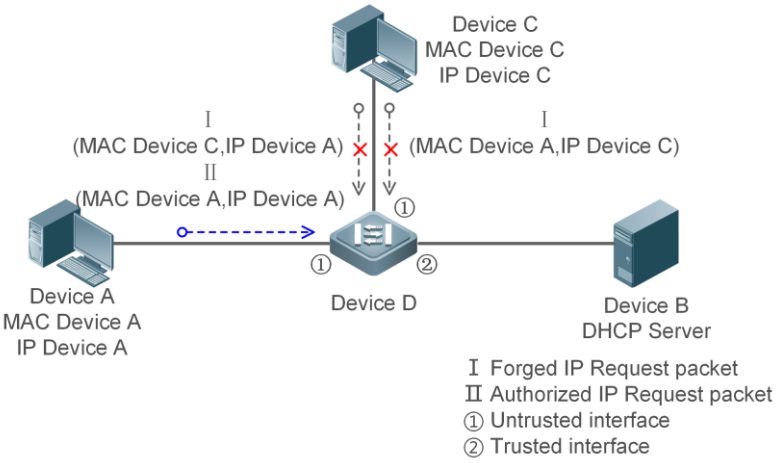
Check IP packets from untrusted interfaces to filter out forged IP packets based on IP address fields or IP and MAC address fields.

For example, in Figure 1-3, IP packets sent by DHCP clients will be checked.

- The source IP address fields of IP packets must match IP addresses assigned through 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:	Device D is an access device. Device A and Device C are user PCs. Device B is a DHCP server within the controlled area.

Deployment

- Enable DHCP snooping on Device D to realize DHCP monitoring.
- Configure all downlink interfaces on the Device D as untrusted.
- Enable IP source guard on Device D to filter IP packets.
- Enable IP source guard based on IP and MAC addresses to check source MAC and IP address fields of IP packets.

1.2.5 Preventing Private IP Addresses

Scenario

Check source addresses of IP packets from untrusted interfaces against DHCP-assigned addresses.

If the source addresses, connected interfaces, and Layer 2 source MAC addresses of interfaces in IP packets do not match DHCP snooping binding entries on the DHCP server, such packets will be discarded.

Deployment

- See Guarding Against IP or MAC Address Spoofing.

1.2.6 Detecting ARP Attacks

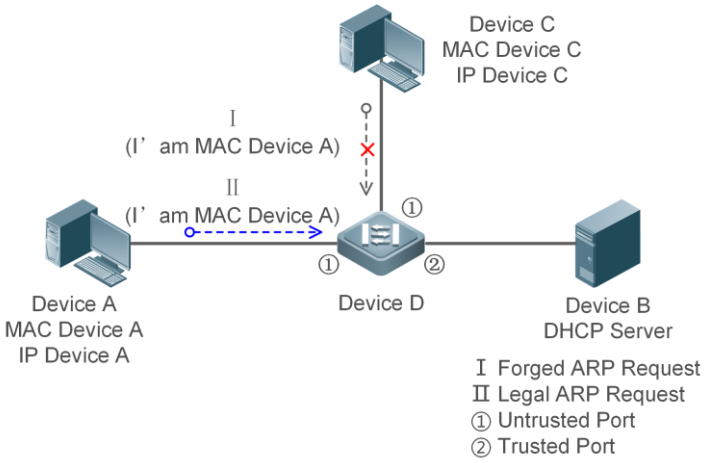
Scenario

Check ARP packets from untrusted interfaces and filter out the ARP packets that do not match DHCP snooping binding entries.

For example, in Figure 1-4, ARP packets sent from DHCP clients will be checked.

- The interfaces receiving ARP packets, Layer 2 MAC addresses, and source MAC addresses of ARP packets senders should match DHCP snooping binding entries.

Figure 1-4



Remarks:	Device D is an access device. Device A and Device C are user PCs. Device B is a DHCP server within the controlled area.

Deployment

- Enable DHCP snooping on Device D to realize DHCP monitoring.
- Configure all downlink interfaces on the Device D as untrusted.
- Enable IP source guard and ARP check on all the untrusted interfaces on Device D to realize ARP packet filtering.

All the preceding security control functions are only valid for DHCP snooping untrusted interfaces.

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 Declient packets, DHCP Release packets, and DHCP Inform packets.

DHCP Reply Packets

Reply 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 Interfaces

Interaction packets for obtaining IP addresses through DHCP are broadcast. Consequently, unauthorized DHCP services will influence normal clients' acquisition of IP addresses, leading to service spoofing and interception. To mitigate unauthorized DHCP services, DHCP snooping interfaces are classified into trusted and untrusted interfaces.

Only DHCP Reply packets received on trusted interfaces are forwarded by access devices; packets received on untrusted interfaces are discarded. This approach allows interfaces connected to authorized DHCP servers to be designated as trusted, while all others are marked as untrusted, effectively shielding against unauthorized DHCP servers.

On the device, all Layer 2 aggregate interfaces are untrusted interfaces by default. You can specify trusted interfaces. On 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 interfaces 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 interfaces 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 access controllers (ACs), all WLAN interfaces are untrusted interfaces and cannot be specified as trusted, and all the switching interfaces and Layer 2 aggregate interfaces are untrusted interfaces by default and can be specified as trusted.

DHCP Snooping Packet Suppression

To shield all the DHCP packets on a specific client, enable DHCP snooping packet suppression on its untrusted interfaces.

VLAN-based DHCP Snooping

DHCP sSnooping can work on a VLAN basis. By default, when DHCP snooping is enabled, it is valid for all the VLANs of the device. You can specify the VLAN where DHCP snooping takes effect.

DHCP Snooping Binding Database

On a DHCP network, clients may set static IP addresses randomly. This increases the difficulty in network maintenance and the possibility that authorized clients with IP addresses assigned by the DHCP server may fail to use network services normally due to address conflicts. Through snooping packets between clients and servers, the device enabled with DHCP snooping summarizes user entries including IP addresses, MAC addresses, VLAN IDs (VIDs), interfaces, and lease values to build the DHCP snooping binding database. Combined with ARP detection and ARP check, DHCP snooping controls assignment of IP addresses for authorized clients.

DHCP Snooping Rate Limiting

DHCP snooping rate limiting can be configured through the rate limiting command of Network Foundation Protection Policy (NFPP). For details about NFPP, see the *Configuring NFPP*.

DHCP Option 82

DHCP Option 82, an option for DHCP packets, is also called DHCP Relay Agent Information Option. As the option number is 82, it is known as Option 82. Option 82 is developed to enhance security of DHCP servers and improve IP address assignment. Option 82 is often configured for the DHCP relay services of a network access device such as the DHCP relay function and DHCP snooping. This option is transparent to DHCP clients, and the DHCP relay agent adds or removes the option.

Unauthorized DHCP Packets

DHCP snooping enables the device to check DHCP packets passing through a client. It discards unauthorized DHCP packets are discarded, and records user information and generates the DHCP Snooping binding database for other applications (for example, ARP detection). The following types of packets are considered unauthorized DHCP packets.

- DHCP Reply packets received on untrusted interfaces, including DHCP ACK, DHCP NAK, and DHCP Offer packets
- DHCP Request packets carrying the **giaddr** field (gateway information), which are received on untrusted interfaces
- Packets with source MAC addresses that are different from values of the **chaddr** field in DHCP packets when MAC address check is enabled
- DHCP Release packets in which the untrusted interface is inconsistent with the entry in the DHCP snooping binding database
- DHCP packets whose format is incorrect or incomplete DHCP packets

Overview

Feature	Description
Filtering Unauthorized DHCP Packets	Checks DHCP packets and discards unauthorized packet, and forwards Request packets to trusted interfaces only.
Building the Binding Database	Checks interaction between DHCP clients and the server, and generates the DHCP snooping binding database, providing the basis for other filtering modules.

1.3.1 Filtering Unauthorized DHCP Packets

Check DHCP packets from untrusted interfaces and filter out unauthorized packets to control the range in which packets are transmitted and to prevent malicious users' spoofing attacks.

Working Principle

DHCP snooping enables the device to check the receiving interfaces and other fields of packets to realize packet filtering, and to change destination interfaces of packets to control the range in which packets are transmitted.

Checking Interfaces

Upon receipt of DHCP packets, a client first determines whether the packet receiving interfaces are DHCP snooping trusted interfaces. If the receiving interface is the trusted interface, the client directly forwards the packets. If the receiving interface is the untrusted interface, the client checks the packets.

Checking Packet Encapsulation and the Length

A client checks whether packets are UDP packets and whether the destination interface is 67 or 68. It checks whether the packet length match the length field defined in protocols.

Checking Packet Fields and Types

According to the types of unauthorized packets, check **giaddr** and **chaddr** in packets and then check whetherother conditions for the type of packets are met.

Related Configuration

Enabling Global DHCP Snooping

By default, DHCP snooping is disabled.

Run the **ip dhcp snooping** command to enable DHCP snooping.

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 enabled, DHCP snooping is valid for all VLANs.

Use the [**no**] **ip dhcp snooping vlan** command to enable DHCP snooping in specified VLANs or delete VLANs from the specified VLANs. The value range of the command parameter is the actual range of VLAN IDs.

Configuring Source MAC Address Check

By default, Layer 2 MAC addresses of packets and **chaddr** fields of DHCP packets are not checked.

When the **ip dhcp snooping verify mac-address** command is used, the device checks source MAC addresses and **chaddr** fields of DHCP Request packets sent from untrusted interfaces. It discards DHCP Request packets with different MAC addresses.

1.3.2 Building the Binding Database

When the DHCP server enabled with DHCP snooping detects packets exchanged with DHCP clients, it generates DHCP snooping binding entries based on information in authorized DHCP packets. All these valid entries are provided for other security modules as the basis for filtering packets.

Working Principle

The binding database is updated in a timely manner based on types of DHCP packets.

Generating Binding Entries

When a DHCP ACK packet on a trusted interface is snooped, the client's IP address, MAC address, and lease are extracted with the interface ID (wired interface index or WLAN ID) and VLAN ID. Then a binding entry is generated.

Deleting Binding Entries

A binding entry is deleted when the recorded lease of the binding entry is due, an authorized DHCP Release or Decline packet sent by the client or a DHCP NCK packet received on a trusted interface is snooped, or the **clear** command is used.

Related Configuration

You only need to enable DHCP snooping.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	⚠ (Mandatory) It is used to enable DHCP snooping.	
	ip dhcp snooping	Enables DHCP snooping.
	ip dhcp snooping suppression	Enables DHCP snooping packet suppression.
	ip dhcp snooping vlan	Enables VLAN-based DHCP snooping.
	ip dhcp snooping verify mac-address	Configures DHCP snooping source MAC address check.

Configuration	Description and Command	
	ip dhcp snooping database write-delay	Writes the DHCP snooping binding database to the flash memory periodically.
	ip dhcp snooping database write-to-flash	Writes the DHCP snooping binding database to the flash memory manually.
	renew ip dhcp snooping database	Imports user information in the backup file to the DHCP snooping binding database.
	ip dhcp snooping database	Configures backup files of the DHCP snooping binding database.
	ip dhcp snooping trust	Configures DHCP snooping trusted interfaces.
	ip dhcp snooping bootp-bind	Enables BOOTP support.
	ip dhcp snooping check-giaddr	Enables DHCP snooping to allow the device to process relay Request packets.
	ip dhcp snooping clear-broadcast-flag	Enables the device to clear the broadcast flag bit.
Configuring Option 82	(Optional) It is used to optimize address assignment by the DHCP server.	
	ip dhcp snooping Information option	Adds Option 82 to DHCP Request packets.
	ip dhcp snooping information option format remote-id	Configures the sub-potion **remote-id** of Option 82 as a user-defined character string.
	ip dhcp snooping vlan information option format-type circuit-id string	Configures the sub-option **circuit-id** of Option 82 as a user-defined character string.

1.4.1 Configuring Basic Functions

Configuration Effect

- Enable DHCP snooping.
- Generate the DHCP snooping binding database.
- Control the transmit range of DHCP packets.
- Filter out unauthorized DHCP packets.

Notes

- The interfaces on clients connecting a trusted DHCP server must be configured as trusted.
- DHCP snooping is effective on the wired switching interfaces, Layer 2 aggregate interfaces, 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 Step

Enabling Global DHCP Snooping

- Mandatory.
- Unless otherwise noted, perfrom the configuration on access devices.

Enabling or Disabling VLAN-based DHCP Snooping

- DHCP snooping can be disabled for some VLANs if not necessary.
- Unless otherwise noted, perfrom the configuration on access devices.

Configuring DHCP Snooping Trusted Ports

- Mandatory.
- Configure the interfaces connecting a trusted DHCP server as trusted.

Enabling DHCP Snooping Source MAC Address Check

- This configuration is required if the **chaddr** fields of DHCP Request packets match Layer 2 source MAC addresses of data packets.
- Unless otherwise noted, perfrom the configuration on all the untrusted interfaces of access devices.

Writing the DHCP Snooping Binding Database to the Flash Memory Periodically

- Enable this feature to save DHCP snooping binding database information upon client restart.
- STA information is not saved.
- Unless otherwise noted, perfrom the configuration on access devices.

Enabling BOOTP Support

- Optional
- Unless otherwise noted, perfrom the configuration on access devices.

Associating DHCP Snooping with ARP

- Optional.
- Unless otherwise noted, perfrom the configuration on access devices.

Enabling DHCP Snooping to Process Relay Request Packets

- Optional.
- Unless otherwise noted, perfrom the configuration on access devices.

Enabling DHCP Snooping

- Optional.
- If DHCP snooping binding entries need to be generated on a routed interface, perfrom the configuration on a Layer 3 device.

Enabling DHCP Snooping to Clear the Broadcast Flag Bit

- Optional.
- Unless otherwise noted, perfrom the configuration 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 DHCP.

- Check whether the DHCP snooping binding database is generated with entries on the client.

Related Commands

Enabling or Disabling DHCP Snooping

Command	[**no**] **ip dhcp snooping**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After global DHCP snooping is enabled, you can check DHCP snooping using the **show ip dhcp snooping** command. After DHCP Snooping is enabled, the validity of DHCP packets is checked. DHCP response packets from untrusted ports will be discarded. To ensure the normal operation of services, configure the uplink port (that is, the port connected to the DHCP server) as a trusted port.

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*: Indicates the minimum VLAN ID. *vlan-max*: Indicates the maximum VLAN ID.
Command Mode	Global configuration mode
Usage Guide	Use this command to enable or disable DHCP snooping in 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	Interface configuration mode or WLAN security configuration mode
Usage Guide	Use this command to reject all DHCP Request packets on the interface, that is, to forbid all users on the interface to apply for addresses through DHCP.

Configuring DHCP Snooping Source MAC Address Check

Command	[**no**] **ip dhcp snooping verify mac-address**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Through source MAC address check, MAC addresses in link headers and CLIENT MAC fields in the Request packets sent by a DHCP client are checked for consistency. When source MAC address check fails, packets will be discarded.

Writing DHCP Snooping Database to the Flash Memory 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 memory.
Command Mode	Global configuration mode
Usage Guide	Use this command to write the DHCP snooping database to the flash memory. This can avoid binding information loss after device restart. Otherwise, users have to re-obtain IP addresses.

Writing the DHCP Snooping Database to the Flash Memory 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 dynamic user information in the DHCP snooping database in the flash memory in real time.

Importing Backup File Information 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 backup file information to the DHCP snooping binding database.

Configuring DHCP Snooping Trusted Interfaces

Command	[**no**] **ip dhcp snooping trust**
Parameter	N/A

Description	
Command Mode	Interface configuration mode
Usage Guide	Use this command to configure an interface connected to an authorized DHCP server as a trusted interface. The DHCP Reply packets received by trusted interfaces are forwarded, while those received by untrusted interfaces 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 Request Packets

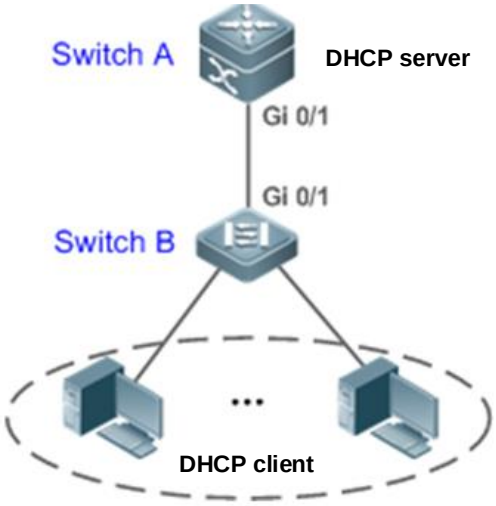
Command	[**no**] **ip dhcp snooping check-giaddr**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	After the feature is enabled, services using DHCP snooping binding entries generated based on relay Request packets, such as IP source guard or 802.1x authentication, cannot 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 request packets will be discarded. 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, the device enabled with DHCP snooping checks the broadcast flag bit for non-DHCP relay Request packets. If the flag bit is 1, it clears the flag bit. When receiving Reply packets, the device sets the flag bit to 1 and set Layer 2 and Layer 3 destination addresses as broadcast addresses.

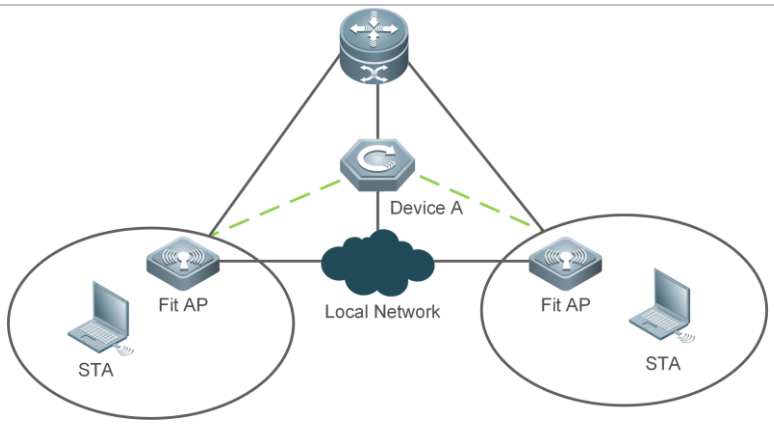
Configuration Example

DHCP Client Obtaining IP Addresses Dynamically from an Authorized DHCP Server

Scenario **Figure 1-5**	
Configuration Steps	● Enable DHCP snooping on an access device (Switch B). ● Configure the uplink interface (GigabitEthernet 0/1) as a trusted interface.
Device B	Hostname#configure terminal Hostname(config)#ip dhcp snooping Hostname(config)#interface gigabitethernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust
Verification	Check the configuration on Switch B. ● Check whether DHCP snooping is enabled, and whether the configured DHCP snooping trusted interface is the uplink interface. ● Check the DHCP snooping configuration on Switch B, and check whether the trusted interface is correct.
Device B	Hostname#show running-config ! ip dhcp snooping ! interface GigabitEthernet 0/1 B#show ip dhcp snooping Switch DHCP Snooping status : ENABLE DHCP Snooping Verification of hwaddr status : DISABLE DHCP Snooping database write-delay time : 0 seconds DHCP Snooping option 82 status : DISABLE DHCP Snooping Support BOOTP bind status : DISABLE Interface Trusted Rate limit (pps) ------------------------ ------- ---------------- GigabitEthernet 0/1 YES unlimited B#show ip dhcp snooping binding Total number of bindings: 1 MacAddress IpAddress Lease(sec) Type VLAN Interface ------------------ --------------- ------------ ------------- ----- -------------------- 0013.2049.9014 172.16.1.2 86207 DHCP-Snooping 1

	GigabitEthernet 0/11

Configuring DHCP Snooping for Wireless Fit APs in Local Forwarding Scenarios

Scenario **Figure 1-6**	
Configuration Steps	● Configure DHCP snooping basic functions on the AC.
Device A	Hostname# configure terminal Hostname(config)# ip dhcp snooping
Verification	● Check the DHCP snooping configuration.
Device A	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) ------------------------ ------- ---------------- Default No unlimited

Common Errors

- The uplink interface is not configured as a DHCP trusted interface.
- Another access security option is already configured for the uplink interface, so that a DHCP trusted interface cannot be configured.

1.4.2 Configuring Option 82

Configuration Effect

- Option 82 enables the DHCP server to obtain more information for better address assignment.
- The Option82 function is transparent to clients.

Notes

- The Option 82 function for DHCP snooping and the DHCP relay agent cannot be configured simultaneously.

Configuration Step

- To optimize address allocation, perform the configuration.
- Unless otherwise noted, enable this function on access devices with DHCP snooping enabled.

Verification

Check whether DHCP snooping options are configured successfully.

Related Commands

Adding Option 82 to DHCP Request Packets

Command	[**no**] **ip dhcp snooping information option** [**standard-format | dot1x-format**]
Parameter Description	**standard**–**format**: Indicates a standard format of Option 82. **dot1x-format**: Uses the 802.1X format for Option 82.
Command Mode	Global configuration mode
Usage Guide	Use this command to add Option 82 to DHCP Request packets so that a DHCP server assigns addresses according to such information. When the 802.1X format is used, if a DHCP relay agent is deployed on the local device and the uplink interface connected to the DHCP server is an SVI, you need to disable DHCP snooping for the VLAN corresponding to the SVI.

Configuring remote-id of Option82 as a User-defined Character String

Command	[**no**] **ip dhcp snooping information option format remote-id** { **string** *ASCII-string* | **hostname** }
Parameter Description	**string** *ASCII-string*: Indicates that the sub-option **remote-id** of Option 82 is a user-defined character string. **hostname**: Indicates that the sub-option **remote-id** of Option 82 is a host name.
Configuration mode	Global configuration mode
Usage Guide	Use this command to configure the sub-option **remote-id** of Option 82, which is added to DHCP Request packets. A DHCP server assigns addresses according to Option 82 information.

Configuring circuit -id of Option 82 as a 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 ID of the VLAN where a DHCP Request packet is transmitted. *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 Option 82, which is added to DHCP Request packets. A DHCP server assigns addresses according to Option 82 information.

Configuration Example

Configuring the Device to Add Option 82 to DHCP Request Packets

Configuration Steps	● Configuring basic functions of DHCP snooping. ● Configuring Option 82.
Device B	`Hostname# configure terminal` `Hostname(config)# ip dhcp snooping information option`
Verification	● Check the DHCP snooping configuration.

Device B	`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

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

Command	Description
clear ip dhcp snooping binding [*ip*] [*mac*] [**vlan** *vlan-id*] [**interface** *interface-id*]	Clears the DHCP snooping binding database.

Displaying

Description	Command
show ip dhcp snooping	Displays the DHCP snooping configuration.
show ip dhcp snooping binding	Displays the DHCP snooping binding database.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug snooping ipv4 event	Debugs DHCP snooping events.
no debug snooping ipv4 event	Disables debugging DHCP snooping events.
debug snooping ipv4 packet	Debugs DHCP snooping packets.
no debug snooping ipv4 packet	Disables debugging DHCP snooping packets.

1 Configuring DNS Client

1.1 Overview

A Domain Name System (DNS) is a distributed database that maps domain names to IP addresses on the Internet, enabling users to access websites without needing to remember numeric IP addresses directly used by computers. The process of translating a host name into its corresponding IP address is known as domain name resolution (or host name resolution).

Protocols and Standards

- RFC 1034: DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

1.2 Applications

Application	Description
Static Domain Name Resolution	The device resolves domain names based on mappings between domain names and IP addresses on a device.
Dynamic Domain Name Resolution	The device obtains the IP address mapped to a domain name dynamically from a DNS server on a network.

1.2.1 Static Domain Name Resolution

Scenario

- Preset mappings between domain names and IP addresses on a device.
- When you perform domain name operations (such as ping and Telnet) through applications, the system can resolve the IP address without being connected to a server on a network.

Deployment

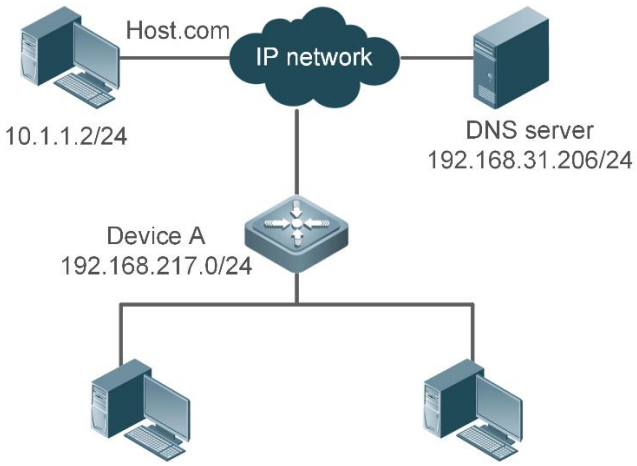
Preset mappings between domain names and IP addresses on a device.

1.2.2 Dynamic Domain Name Resolution

Scenario

- The DNS server is deployed on a network to provide the domain name service.
- The domain name host.com is deployed on the network.
- Device-A obtains domain name host.com from the DNS server.

Figure 1-1 Dynamic Domain Name Resolution



Deployment

Deploy the DNS server that provides domain name resolution for Device-A.

1.3 Features

Basic Concepts

DNS

DNS involves a resolver and a DNS server. The DNS server stores the mappings between domain names and IP addresses of all hosts on a network, and implements mutual conversion between them. Both the TCP and UDP port numbers of DNS are 53, and a UDP port is typically used.

Overview

Feature	Description
Domain Name Resolution	Obtains IP addresses based on domain names from a DNS server or a local database.
DNS Allowlist	Uses the DNS allowlist function to specify valid DNS server's IP address.

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 applications, 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 the DNS resolver of the system queries an external DNS server for the IP address mapped to the domain name when a user perform domain name operations through applications.

The procedure of dynamic domain name resolution is as follows:

1 A user application (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 in the dynamic cache does not expire, the DNS resolver returns the domain name to the application.

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.

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 an 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.

1.3.2 DNS Allowlist

Supported functions are subject to the product version.

Working Principle

The DNS allowlist function is used to specify valid DNS servers' IP addresses on a network. After this function is enabled on a device, the device checks received DNS packets and intercepts invalid DNS packets. You can enable the DNS allowlist function globally or based on the WLAN and configure a list of valid DNS servers. When the DNS allowlist function is enabled based on the WLAN, if a DNS packet received from the WLAN is not used to access the WLAN-based valid DNS server's IP address, the device discards the packet without matching the packet with the global DNS allowlist.

Related Configuration

Enabling the DNS Allowlist

- The DNS allowlist function is disabled by default.
- Run the **ip name-server white-list enable** command to enable domain name resolution.

Configuring Valid DNS Servers' IP Addresses

- No DNS server's IP address is configured by default.
- Run the **ip name-server white-list** command to configure the DNS server's IP addresses.
- Only DNS servers' IPv4 addresses are supported, and up to six DNS servers' IP addresses can be configured.

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.
Configuring DNS Allowlist	Optional.	
	ip name-server white-list enable	Enables the DNS allowlist function.
	ip name-server white-list [**wlan** *wlan-id*] *ip-address*	Configures valid DNS servers' IP addresses.

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 Step

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 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 Step

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* }&<1-6>
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 1-2**	
	Device A resolves the domain name through the DNS server (192.168.10.1) on the network.
Configuration Steps	● Set the IP address of the DNS server to 192.168.10.1 on the device. ● Set the IPv6 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)

1.4.3 Configuring DNS Allowlist

Supported functions are subject to the product version.

Configuration Effect

The system checks DNS packets received by the device and intercepts invalid DNS packets.

Configuration Step

Enabling the DNS Allowlist

- The DNS allowlist function is disabled by default.
- If this function is enabled, the device checks received DNS packets.

Configuring a DNS Server

- If no valid DNS server is configured, all DNS packets are filtered out.
- Only DNS servers' IPv4 addresses are supported.
- Up to six DNS servers' IP addresses can be configured.

Verification

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

Related Commands

Configuring the DNS Allowlist

Command	**ip name-server white-list** [**wlan** *wlan-id*] **enable**
Parameter Description	*wlan-id*: Indicates the ID of the WLAN.
Command Mode	Global configuration mode
Usage Guide	The supported configuration may vary depending on actual products.

Configuring Valid DNS Servers' IP Addresses

Command	**ip name-server white-list** [**wlan** *wlan-id*] *ip-address*
Parameter Description	*wlan-id*: Indicates the ID of the WLAN. *ip-address*: Indicates the IPv4 address of a DNS server.
Command Mode	Global configuration mode
Usage Guide	The supported configuration may vary depending on actual products.

Configuration Example

Configuring Dynamic Domain Name Resolution

Configuration Steps	• Enable the DNS allowlist function on the device. • Set the DNS server's IP address to 192.168.10.1 on the device.

	`Hostname# configure terminal`
	`Hostname(config)# ip name-server white-list enable`
	`Hostname(config)# ip name-server white-list 192.168.10.1`
	`Hostname(config)# exit`

Verification	Run the **show ip name-server white-list** command to display the DNS allowlist configuration.

	`Hostname# show ip name-server white-list`
	`white-list check: enable`
	`white-list name-server:`
	`192.168.10.1`

1.5 Monitoring

Clearing

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

Command	Description
clear host [*host-name*]	Clears the dynamic host name cache table.

Displaying

Command	Description
show hosts [*host-name*]	Displays DNS parameters.

Displaying the DNS Allowlist

Command	Description
show ip name-server white-list [**wlan** *wlan-id*]	Displays the DNS allowlist configuration.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug ip dns	Debugs the DNS function.

1 Configuring DNS Snooping

1.1 Overview

DNS snooping monitors domain name server (DNS) packets exchanged between clients and servers to record mapping table entries of domain names and IP addresses. It also filters out unauthorized DNS packets, including request packets from clients and response packets from servers.

DNS snooping provides authentication-free uniform resource locators (URLs), that is, domain name-based direct addresses.

Protocols and Standards

- RFC 1034：DOMAIN NAMES - CONCEPTS AND FACILITIES
- RFC 1035：DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

1.2 Applications

Application	Description
Applying Authentication-free URLs	Unauthenticated clients cannot access a network normally when web-based authentication is enabled on the AC. With the authentication-free URL function enabled, clients are allowed to access specific URLs without authentication.

1.2.1 Applying Authentication-free URLs

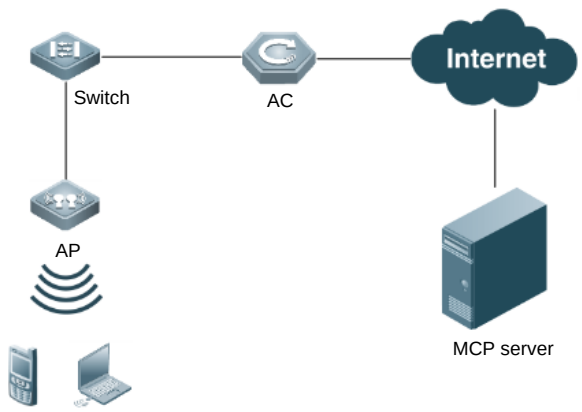
Scenario

In Figure 1-1, the AC interacts with the MCP server, to control the network access right of unauthenticated downlink clients as well as their authentication through authentication over WeChat following.

Unauthenticated clients can access only WeChat, and can pass authentication by following the WeChat public account.

Authenticated clients have unrestricted network access rights.

Figure 1-1



Remarks:	The AC indicates an access controller. The AP indicates an access point. The MCP server is a cloud server.

Deployment

- Enable authentication over WeChat following on the AC for interaction with the MCP server.

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

The CPE WAN Management Protocol (CWMP), initiated by the Digital Subscriber Line (DSL) forum and designated as TR-069, is commonly referred to as the TR-069 protocol. It provides the universal framework, message specification, and method and data model for managing and configuring home network devices on next-generation networks.

Implementation of the 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	Prevents unauthenticated clients from accessing a 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 matches 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 an Authentication-free URL	(Mandatory) It is used to configure authentication-free apps in global configuration mode.	
	free-url	Configures the authentication-free URL. Only WeChat, Sina App, certain iPhone apps, and designated URLs are supported.
	ip dns snooping enable	Enables DNS snooping.

1.4.1 Configuring an 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 Step

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 an Authentication-free URL

- Mandatory.
- Configure an authentication-free URL on the AC.

Command	**free-url** { **weixin | sina | iphone** | **url** *url* } [**wlan** *wlan-id*]
Parameter Description	**weixin**: Indicates WeChat. **sina**: Indicates a Sina app. **iphone**: Indicates an iPhone app. *url*: Indicates a designated URL. **wlan**: Indicates a WLAN.
Defaults	No authentication-free URL is configured by default.
Command Mode	Global configuration mode
Usage	You can configure multiple authentication-free URLs.

Guide	

Verification

- Run the **show free-url** command to check the configuration.
- Check whether unauthenticated clients can access authentication-free URLs directly when the web-based authentication function is enabled on the AC.

Configuration Example

↘ Configuring WeChat as Authentication-free URL on the 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 authentication-free URLs.

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
                                  240e:ff:e020:932:0:ff:b04a:7a63      2024
                                  240e:ff:e020:9d1:0:ff:b055:d090      2024
==========================================================================
====
```

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show free-url	Displays authentication-free URLs.
clear free-url	Clears authentication-free URLs.
show dns s nooping statistics	Displays DNS packet statistics.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug dns-snooping	Debugs DNS snooping.

1 Configuring Bonjour Gateway

1.1 Overview

The Bonjour gateway is used to manage clients and servers supporting the Bonjour protocol, to implement Bonjour applications on large-scale networks.

The Bonjour gateway provides the following functions:

- Controls traffic of multicast Domain Network Service (mDNS) packets on a network to decrease excessive mDNS packets.
- Configures Bonjour policies and rules to manage available services on the client.
- Forwards mDNS packets of clients and servers across VLANs to enhance ease of use for networks.

Protocols and Standards

- RFC 1034: Domain Names - Concepts and Facilities
- RFC 1035: Domain Names - Implementation and Specification
- RFC 6762: Multicast DNS

1.2 Applications

Application	Description
Query Proxy and Response Forwarding	In some scenarios, the Bonjour gateway receives query packets from a client, but its service resource entries show that it does not obtain the specified service requested by the client. In this case, the Bonjour gateway needs to perform query proxy and response forwarding on the specified service. When the Bonjour gateway forwards the query packets and receives response packets about the service, it adds information about the service to Bonjour service resource entries, and forwards the response packets to the client. Then the Bonjour gateway can perform response proxy for the server.
Preemption Prohibition of the Multimedia Gateway	When different terminals use the screen projection function of Apple TV simultaneously, they may preempt resources if the Bonjour gateway is not enabled. When the Bonjour gateway is enabled, preemption is prohibited.
Automatic Server Renaming of the Multimedia Gateway	To differentiate between multiple Apple TVs on a network with the same projector name displayed on the terminals, the device provides automatic naming based on the name and IP address. This helps identify different servers.
Accurate Screen Projection of the Multimedia Gateway	If multiple Apple TVs exist on a network, multiple projector names may be displayed on the terminals, which can lead to incorrect screen projection. After the accurate screen projection function of the multimedia gateway is enabled, iPad needs to scan the QR code on the Apple TV to bind to the TV, and to detect the devices bound to the iPad. Otherwise, the iPad cannot discover any projectors.

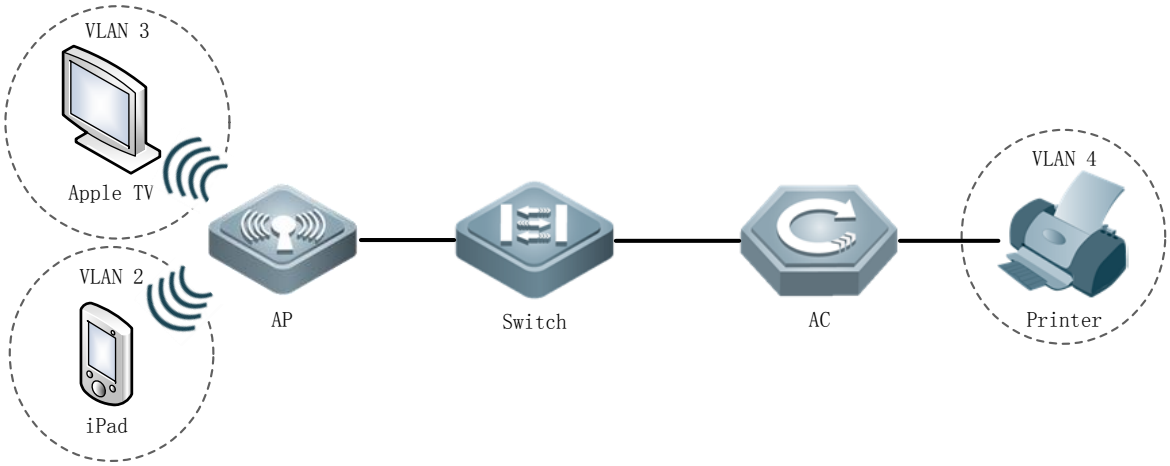
Application	Description
Server Location Control of the Multimedia Gateway	If multiple Apple TVs exist on the network and they are connected to different APs, multiple mirroring devices may be displayed on the client. This may cause inaccurate screen mirroring. After the server location control function of the multimedia gateway is enabled, the location where an iPad goes online needs to match the location where the Apple TV server can provide services so as to discover the corresponding mirroring device.

1.2.1 Query Proxy and Response Forwarding

Scenario

As shown in Figure 1-1, iPad, Apple TV, and printer are located in different VLANs. iPad needs to obtain the IP addresses of Apple TV and printer through the Bonjour gateway to communicate with them.

Figure 1-1 Bonjour Gateway Topology



Deployment

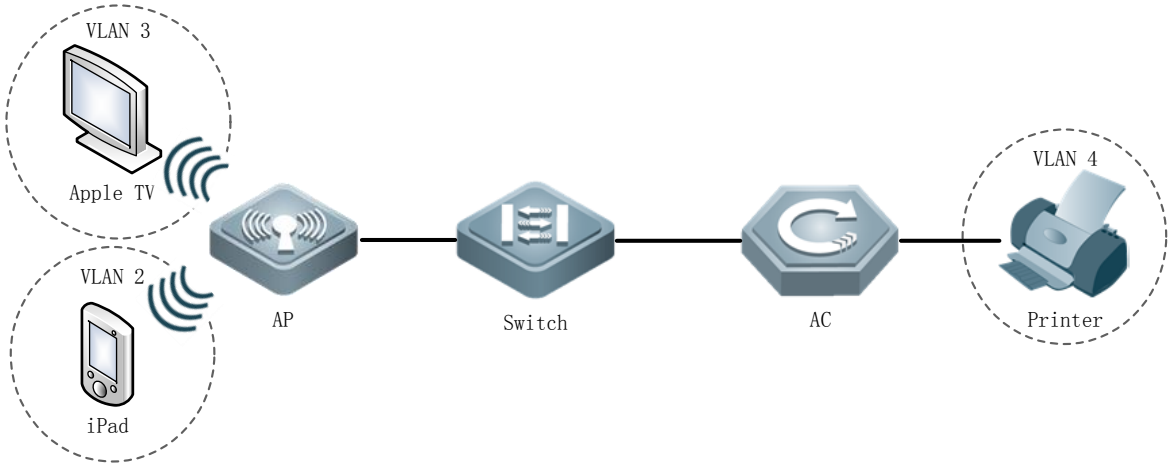
- Enable the Bonjour gateway globally to process multicast DNS request packets received on the interface.

1.2.2 Preemption Prohibition of the Multimedia Gateway

Scenario

As shown in Figure 1-2, iPad, Apple TV, and printer are located in different VLANs. iPad needs to obtain the IP addresses of Apple TV and printer through the Bonjour gateway to communicate with them. When different clients use the screen projection function of Apple TV simultaneously, they may preempt resources if the Bonjour gateway is not enabled. When the Bonjour gateway is enabled, preemption prohibition can be implemented.

Figure 1-2 Bonjour Gateway Topology



Deployment

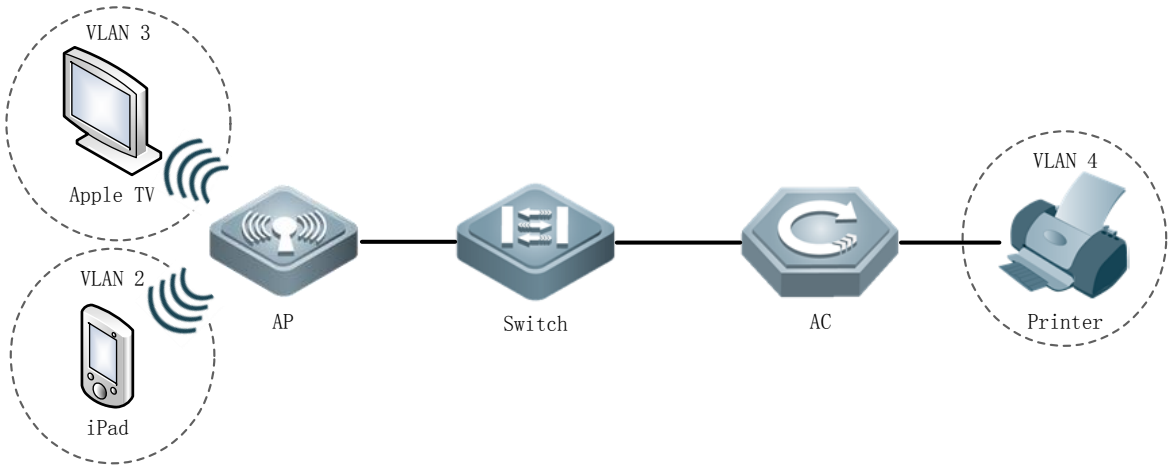
- Enable the Bonjour gateway globally to process multicast DNS request packets received on the interface and enable preemption prohibition. Preemption prohibition is forcibly enabled, and cannot be disabled.

1.2.3 Automatic Server Renaming of the Multimedia Gateway

Scenario

As shown in Figure 1-3, iPad, Apple TV, and printer are located in different VLANs. iPad needs to obtain the IP addresses of Apple TV and printer through the Bonjour gateway to communicate with them. If multiple Apple TVs exist on the network, the same name may be displayed for the projectors on the clients. The device provides automatic server renaming based on names and IP addresses to differentiate them.

Figure 1-3 Bonjour Gateway Topology



Deployment

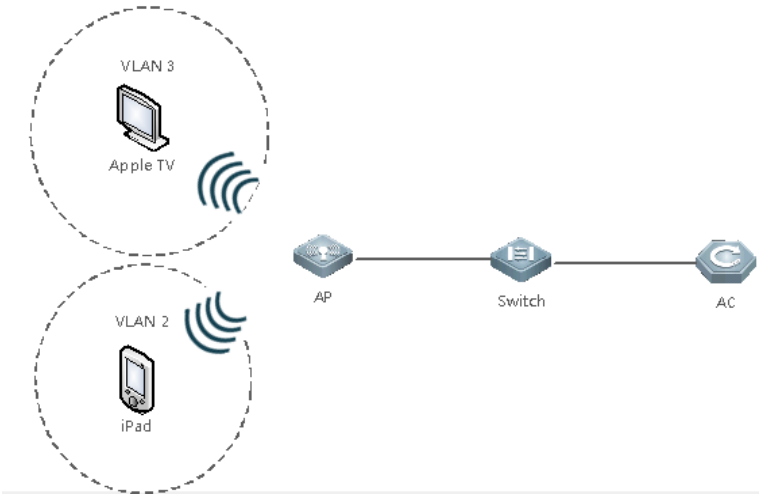
- Enable the Bonjour gateway globally to process multicast DNS request packets received on the interface and automatically rename the discovered servers.

1.2.4 Accurate Screen Projection of the Multimedia Gateway

Scenario

As shown in Figure 1-4, the iPad and the Apple TV reside in different VLANs, and the AC is connected to the EG. The iPad needs to obtain the IP address of the Apple TV through the Bonjour gateway to communicate with the Apple TV. If multiple Apple TVs exist on the network, multiple projector names may be displayed on the terminals, which can lead to incorrect screen projection. After the accurate screen projection function of the multimedia gateway is enabled, iPad needs to scan the QR code on the Apple TV to bind to the TV and to detect the devices bound to the iPad. Otherwise, the iPad cannot discover any projectors.

Figure 1-4 Bonjour Gateway Topology



Deployment

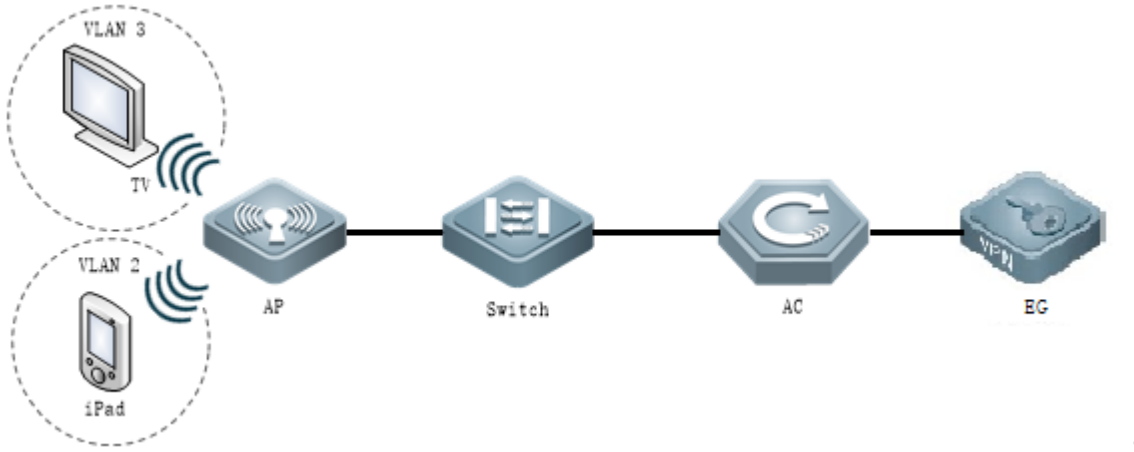
- Enable the Bonjour gateway globally and then enable accurate screen projection. The terminals need to scan the QR code and bind to the Apple TV to detect and use the Bonjour screen projection service.

1.2.5 Server Location Control of the Multimedia Gateway

Scenario

As shown in the following figure, the iPad and the Apple TV are on different VLANs, and the AC is connected to the EG. The iPad needs to obtain the IP address of the Apple TV through the Bonjour gateway to communicate with the Apple TV. If there are multiple Apple TVs on the network and they are connected to different APs, multiple mirroring devices may be displayed on the client. This may cause inaccurate screen mirroring. After the server location control function of the multimedia gateway is enabled, the location where an iPad goes online needs to match the location where the Apple TV server can provide services so as to discover the corresponding mirroring device.

Figure 1 – 5 Bonjour Gateway Topology



Deployment

Enable the Bonjour gateway globally and configure the MAC address of the specified server providing the Bonjour service and the location where services are available. The iPad can discover and use the Bonjour screen mirroring service only when it is in the same location as the configured Apple TV server.

1.3 Features

Basic Concepts

↘ Bonjour

Bonjour is Apple's multicast DNS-based, zero-configuration network standard. Devices using Bonjour automatically broadcast their own service information and listen for services from other devices, much like exchanging greetings. This allows Bonjour to make systems and services on a LAN easily discoverable, even without a network administrator. It displays the names of devices and applications supporting the multicast domain name protocol on the LAN and uses multicast DNS to resolve device naming conflicts.

↘ Bonjour Gateway

The Bonjour gateway is used to manage clients and servers supporting the Bonjour protocol, to implement Bonjour applications on large-scale networks.

Overview

Feature	Description
Bonjour Gateway	The Bonjour gateway is used to manage the clients and servers supporting the Bonjour protocol, to implement Bonjour applications on large-scale networks.

1.3.1 Bonjour Gateway

Working Principle

The Bonjour gateway is used to manage clients and servers supporting the Bonjour protocol, to implement Bonjour applications on large-scale networks.

The Bonjour gateway provides the following functions.

Response Proxy

Servers send Bonjour response packets on a network to advertise the services they support. After receiving the response packets, the Bonjour gateway establishes Bonjour service resource entries, and directly sends response packets to the clients that query services contained in the entries.

Query Proxy and Response Forwarding

In some cases, the Bonjour gateway receives query packets from a client, but its service resource entries show that it does not obtain the specified service requested by the client. In this case, the Bonjour gateway needs to perform query proxy and response forwarding on the specified service. When the Bonjour gateway forwards the query packets and receives response packets about the service, it adds information about the service to the Bonjour service resource entries, and forwards the response packets to the client. Then the Bonjour gateway can perform response proxy for the server.

Screen Preemption Prohibition

When different clients use the screen projection function of Apple TV simultaneously, they may preempt resources if the Bonjour gateway is not enabled. When the Bonjour gateway is enabled, preemption prohibition can be implemented.

Automatic Renaming of Servers

If multiple Apple TVs exist on a network, the same name may be displayed for the projectors on the clients. This function enables automatic server renaming based on names and IP addresses to differentiate them.

Accurate Screen Projection

If multiple Apple TVs exist on a network, multiple projector names may be displayed on the terminals. After the accurate screen projection function of the multimedia gateway is enabled, the terminals need to scan the QR code on the Apple TV to bind to the TV to discover bound TV devices.

1.4 Configuration

Configuration	Description and Command	
Enabling the Bonjour Gateway	(Mandatory) It is used to create the Bonjour gateway service.	
	bonjour-gateway enable	Enables the Bonjour gateway.
	Optional.	
Configuring Bonjour Policies and Rules	Optional.	
	bonjour-gateway global-strategy	Applies a specified Bonjour policy globally.
	bonjour-gateway strategy	Applies a specified Bonjour policy on interfaces.
	bonjour-gateway strategy-mode	Creates a Bonjour policy.
	service type	Configures a service rule.
	service vlan range	Configures a VLAN that allows forwarding query and response packets.

Configuration	Description and Command	
Configuring Preemption Prohibition and Automatic Renaming	**service wired/wireless**	Enables service discovery in wired or wireless mode.
	bonjour-gateway airplay-preemption disable	Disables preemption prohibition.
	bonjour-gateway airplay-rename disable	Disables automatic renaming.
Active Query of Bonjour Services	⚠ Optional.	
	bonjour-gateway query enable	Enables the active query of Bonjour services.
	bonjour-gateway query interval	Configures the interval for actively querying Bonjour services.
Accurate Screen Projection	⚠ Optional.	
	bonjour-gateway airplay-fixed enable	Enables Bonjour accurate screen projection.
	bonjour-gateway airplay-fixed mac-map	Adds the MAC address binding entry for a device.
Server Location Control	⚠ (Optional)	
	bonjour-gateway service-mac	Configures server location and service scope control.

1.4.1 Enabling the Bonjour Gateway

Configuration Effect

- Implement Bonjour applications on large-scale networks after the Bonjour gateway is enabled.

Notes

- The Bonjour gateway must be enabled on Layer 3 interfaces.

Configuration Step

↘ Enabling the Bonjour Gateway

- Mandatory.

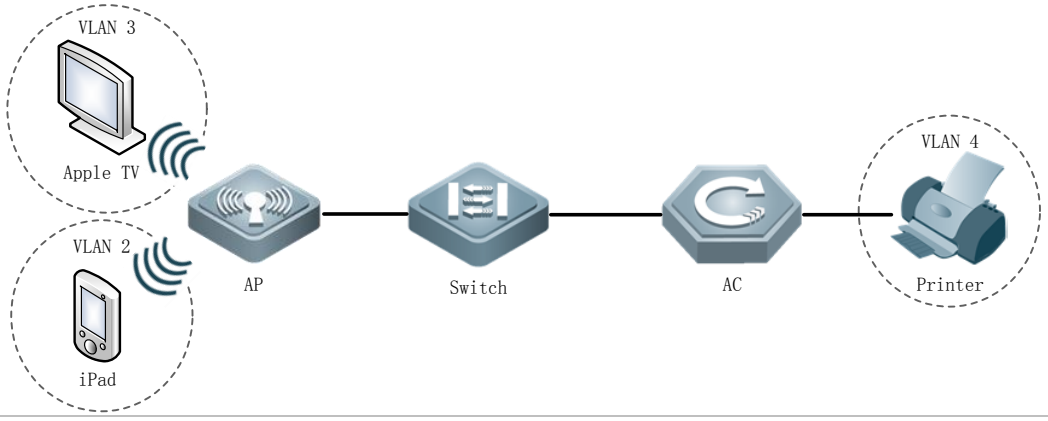
Command	**bonjour-gateway enable**
Parameter Description	N/A
Defaults	The Bonjour gateway is disabled by default.
Command Mode	Global configuration mode or interface configuration mode
Usage Guide	After this function is configured, multicast is enabled on all or specified Layer 3 interfaces to forward multicast packets. The global Bonjour gateway must be enabled before the Bonjour gateway is enabled on a specified interface.

Verification

- Run the **show run** command to display the Bonjour gateway configuration.

Configuration Example

Enabling the Bonjour Gateway

Scenario **Figure 1-5**	● iPad, Apple TV, and printer are located in different VLANs. iPad needs to obtain the IP addresses of Apple TV and printer through the Bonjour gateway to communicate with them.
	
Configuration Steps	● Enable the Bonjour gateway.

	`Hostname#configure terminal`
	`Hostname(config)#`
	`Hostname(config)#interface vlan 2`
	`Hostname(config-if-vlan 2 )#bonjour-gateway enable`

Verification	● Check whether the Bonjour gateway is enabled.
	`Hostname#show run | begin interface vlan 2`
	`Current configuration : 491 bytes`
	
	`interface vlan 2`
	` bonjour-gateway enable`
	`!`

1.4.2 Configuring Bonjour Policies and Rules

Configuration Effect

- Configure Bonjour policies and rules to manage available services on the client.

Configuration Step

Creating a Bonjour Policy

- Optional.
- Run the **bonjour-gateway strategy-mode** command to create a Bonjour policy.

Command	**bonjour-gateway strategy-mode** *name*
Parameter	*name*: Indicates the name of a Bonjour policy.

Description	
Defaults	No Bonjour policy is created by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway strategy-mode** command is used to create a Bonjour policy. The **no bonjour-gateway strategy-mode** command is used to delete a Bonjour policy. By default, no Bonjour policy is created. A maximum of 100 Bonjour policies can be created on the device.

Configuring a Service Discovery Rule

- Optional.
- Run the **service { wired | wireless } disable** command to configure a service discovery rule.

Command	**service { wired | wireless } disable**
Parameter Description	N/A
Defaults	Services can be discovered in both wired and wireless modes by default.
Command Mode	Bonjour gateway mode
Usage Guide	The **service { wired | wireless } disable** command is used to configure a service discovery rule. The **no service { wired | wireless } disable** command is used to delete a service discovery rule. By default, service discovery is allowed in both wired and wireless modes.

Configuring a Service Instance

- Optional.
- Run the **service type** command to create a service rule.

Command	**service type** *type* **{ instance** *name* | **disable }**
Parameter Description	*type*: Indicates the type of a service that can be found by the client. *name*: Indicate the instance name of a service that needs to be searched for by the client.
Defaults	The client can find all services by default.
Command Mode	Bonjour gateway mode
Usage Guide	The **service type** command is used to set a service rule. The **no service type** command is used to delete a service rule. By default, the client can find all services. After the **no service type** command is configured, the corresponding service cannot be found.

Configuring a Service VLAN

- Optional.
- Run the **service vlan range** command to configure a VLAN that allows forwarding query and response packets when a specified Bonjour policy is applied.

Command	**service vlan { range** *vlan-id-list* **| access-vlan }**
Parameter Description	*vlan-id-list*: Indicates the VLAN list. **access-vlan**: Allows forwarding query and response packets in the VLAN to which connected clients belong.

Defaults	All query and response packets are forwarded by default.
Command Mode	Bonjour gateway mode
Usage Guide	The **service vlan range** command is used to configure a VLAN that allows forwarding query and response packets, and discard the query and response packets outside the VLAN. The **no service vlan** command is used to delete the settings. By default, all query and response packets are forwarded.

Applying a Specified Bonjour Policy Globally

- Optional.
- Run the **bonjour-gateway global-strategy** command to apply a specified Bonjour policy globally.

Command	**bonjour-gateway global-strategy** *name*
Parameter Description	*name*: Indicates the name of a Bonjour policy.
Defaults	No Bonjour policy is applied globally by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway global-strategy** command is used to apply a specified Bonjour policy globally. The **no bonjour-gateway global-strategy** command is used to cancel the applied Bonjour policy. By default, no Bonjour policy is applied globally. That is, when the Bonjour gateway is enabled, only the default service type is supported by default, and services can be found in both wired and wireless modes.

Applying a Specified Bonjour Policy

- Optional.
- Run the **bonjour-gateway strategy** command to apply a specified Bonjour policy on Layer 3 interfaces.

Command	**bonjour-gateway strategy** *name*
Parameter Description	*name*: Indicates the name of a Bonjour policy.
Defaults	No Bonjour policy is applied to Layer 3 interfaces by default.
Command Mode	Interface configuration mode
Usage Guide	The **bonjour-gateway strategy** command is used to apply a specified Bonjour policy to Layer 3 interfaces. The **no bonjour-gateway strategy** command is used to cancel the applied Bonjour policy. By default, no Bonjour policy is applied to Layer 3 interfaces.

Verification

- Run the **show run** command to display the Bonjour gateway configuration.

Configuration Example

Configuring a Bonjour Policy

Scenario	See Figure 1-2.

Configuration Steps	● Configure a Bonjour policy.

	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# bonjour-gateway strategy-mode teacher`
	`Hostname(config-bonjour-gateway)#service type ftp ip 10.0.0.5`
	`Hostname(config-bonjour-gateway)#service vlan range 5`
	`Hostname(config-bonjour-gateway)#service vlan access-vlan`
	`Hostname(config-bonjour-gateway)#exit`
	`Hostname(config)#`
	`Hostname(config)#interface vlan 2`
	`Hostname(config-if-vlan 1)#bonjour-gateway enable`
	`Hostname(config-if-vlan 1)# bonjour-gateway strategy teacher`

Verification	● Check whether the Bonjour gateway is enabled.
	`Hostname#show run | begin interface VLAN 1`
	`Current configuration : 491 bytes`
	
	`interface VLAN 2`
	` bonjour-gateway enable`
	` bonjour-gateway strategy teacher`
	`!`
	● Check whether a Bonjour policy is configured.
	`Hostname#show run | begin bonjour-gateway`
	`Current configuration : 491 bytes`
	
	`bonjour-gateway strategy-mode teacher`
	` service type ftp ip 10.0.0.5`
	` service vlan range 5`
	` service vlan access-vlan`
	`!`

1.4.3 Configuring Preemption Prohibition and Automatic Renaming

Configuration Effect

- Configure preemption prohibition and automatic renaming.

Configuration Step

↘ Disabling Preemption Prohibition

- Optional.
- Run the **bonjour-gateway airplay-preemption disable** command to disable preemption prohibition.

Command	**bonjour-gateway airplay-preemption disable**
Parameter Description	N/A

Defaults	Preemption prohibition is enabled by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway airplay-preemption disable** command is used to disable preemption prohibition.

Disabling Automatic Renaming

- Optional.
- Run the **bonjour-gateway airplay-rename disable** command to disable automatic renaming.

Command	**bonjour-gateway airplay-rename disable**
Parameter Description	N/A
Defaults	Automatic renaming is enabled by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway airplay-rename disable** command is used to disable automatic renaming.

Verification

- Run the **show run** command to display the Bonjour gateway configuration.

Configuration Example

Disabling Automatic Renaming

Scenario	See Figure 1-2.
Configuration Steps	• Disable automatic renaming.

	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# bonjour-gateway airplay-rename disable`

Verification	• Check whether automatic renaming is disabled.
	`Hostname#show run | begin bonjour-gateway`
	`Current configuration : 491 bytes`
	
	`bonjour-gateway airplay-rename disable!`

Common Errors

N/A

1.4.4 Active Query of Bonjour Services

Configuration Effect

- To implement response proxy, the Bonjour gateway needs to maintain Bonjour service resource entries. When the active query of Bonjour services is enabled, the Bonjour gateway can guarantee real-timeliness of Bonjour service resource entries.

Configuration Step

Enabling Active Query of Bonjour Services

- Optional.
- Run the **bonjour-gateway query enable** command to enable active query of Bonjour services.

Command	bonjour-gateway query enable
Parameter Description	N/A
Defaults	Active query of Bonjour services is disabled by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway query enable** command is used to enable active query of Bonjour services. The **no bonjour-gateway query enable** command is used to disable active query of Bonjour services. By default, active query of Bonjour services is disabled.

Configuring the Interval for Sending Query Packets to a Discovered Service

- Optional.
- Run the **bonjour-gateway query interval** command to configure the interval for sending query packets to a discovered service.

Command	**bonjour-gateway query interval** *number*
Parameter Description	*number*: Indicates the interval for sending query packets to a discovered service, in seconds. The value range is from 5 to 600.
Defaults	The interval for sending query packets to a discovered service is 15s by default.
Command Mode	Global configuration mode
Usage Guide	The **bonjour-gateway query interval** command is used to configure the interval for sending query packets to a discovered service. The **no bonjour-gateway query interval** command is used to restore the default settings. By default, the interval for sending query packets to a discovered service is 15s.

Verification

- Run the **show run** command to display the Bonjour gateway configuration.

Configuration Example

Enabling Active Query of Bonjour Services

Scenario	See Figure 1-2.
Configuration Steps	• Enable active query of Bonjour services.

	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#bonjour-gateway query enable`
	`Hostname(config)#bonjour-gateway query interval 20`

Verification	● Check whether active query of Bonjour services is enabled.
	`Hostname#show run | begin bonjour-gateway`
	`Current configuration : 491 bytes`
	
	`bonjour-gateway query enable`
	`bonjour-gateway query interval 20`
	`!`

1.4.5 Accurate Screen Projection

Configuration Effect

- With the Bonjour accurate screen projection function enabled, the device responds to the terminals according to the binding relationship. Run the **bonjour-gateway airplay-fixed enable** command to enable this function.

Notes

- The Bonjour gateway must be enabled first.

Configuration Step

↘ Enabling Accurate Screen Projection

- Mandatory.

Command	**bonjour-gateway airplay-fixed enable**
Parameter Description	N/A
Defaults	Accurate screen projection is disabled by default.
Command Mode	Global configuration mode
Usage Guide	After accurate screen projection is enabled, the device returns a unicast response to a specified terminal based on MAC address binding, instead of providing the multicast response service to the terminal. This command is used to enable accurate screen projection.

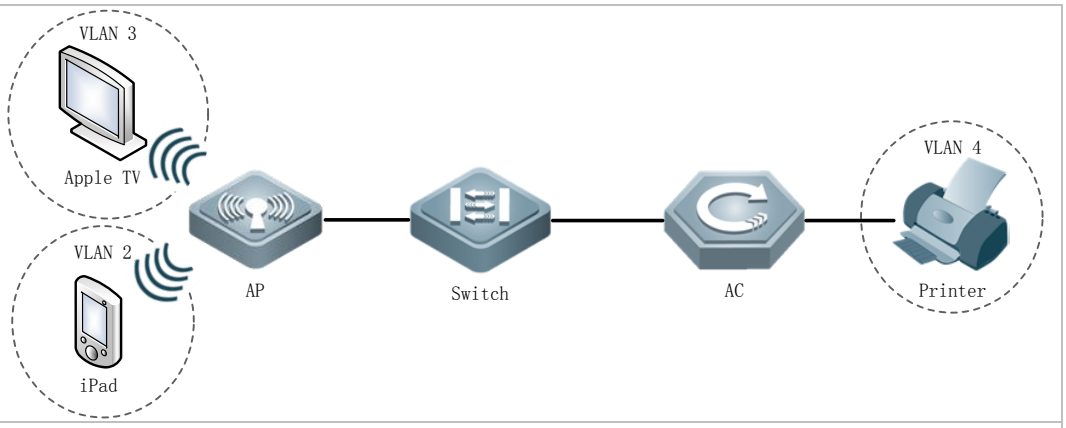
Verification

- Run the **show run** command to display the Bonjour accurate screen projection configuration.

Configuration Example

↘ Enabling Accurate Screen Projection

Scenario **Figure 1-1**	● As shown in the following figure, iPad, Apple TV, and printer reside in different VLANs. iPad needs to obtain the IP address of Apple TV through the Bonjour gateway to communicate with Apple TV and printer.

	
Configuration Steps	● Enable accurate screen projection.

	`Hostname#configure terminal`
	`Hostname(config)#`
	`Hostname(config)#bonjour-gateway airplay-fixed enable`

Verification	● Check whether the Bonjour accurate screen projection is enabled.
	`Hostname#show run | include fixed`
	`bonjour-gateway airplay-fixed enable`
	`Hostname#`

Common Errors

N/A

Adding the Binding Entry of the STA's and TV's MAC Addresses on a Device

- Optional.
- Run the **bonjour-gateway airplay-fixed mac-map stamac** *mac1* **tvmac** *mac2* [**ttl** *number*] command to add the binding entry of the STA's and TV's MAC addresses.

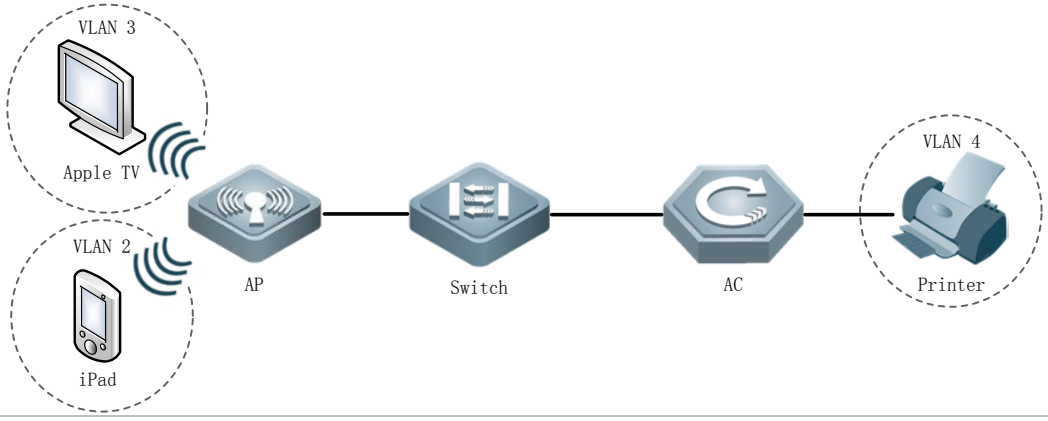
Command	**bonjour-gateway airplay-fixed mac-map stamac** *mac1* **tvmac** *mac2* **tvname** *name* [**ttl** *number*]
Parameter Description	*mac1:* Indicates the MAC address of the STA. *mac2:* Indicates the MAC address of the TV. *name*: Indicates the name of the TV. *number*: Indicate the time to live (TTL) of MAC address binding entries, in minutes. The default value is 1440 minutes (1 day).
Defaults	No binding entry is configured by default.
Command Mode	Global configuration mode
Usage Guide	Run the **bonjour-gateway airplay-fixed enable** command to enable accurate screen projection before you configure binding entries. The **bonjour-gateway airplay-fixed mac-map stamac** *mac1* **tvmac** *mac2* **tvname** *name* [**ttl** *number*] command is used to add the binding entry of STA's and TV's MAC addresses. The default TTL of the entry is 1440 minutes (that is, 1 day) and can be configured as required. The **no bonjour-gateway airplay-fixed mac-map stamac** *mac1* command is used to delete a binding entry. No binding entry is configured on the device by default.

Verification

- This command is an action command. The configuration of this command cannot be displayed by the **show run** command. Run the **show bonjour-gateway mac-map info** command to display the added entries.

Configuration Example

Adding the MAC Address Binding Entry for a Device

Scenario **Figure 1-7**	• As shown in the following figure, iPad, Apple TV, and printer reside in different VLANs. iPad needs to obtain the IP address of Apple TV through the Bonjour gateway to communicate with Apple TV and printer.
	
Configuration Steps	• Add the binding entry of the STA's and TV's MAC addresses on a device.

	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#bonjour-gateway airplay-fixed enable`
	`Hostname(config)#bonjour-gateway airplay-fixed mac-map stamac fe80.4c4e.0708 tvmac 509a.3a5b.6048 tvname sta1 ttl 2`

Verification	• Check whether the MAC address binding entry have been added.
	`Hostname#show bonjour-gateway mac-map info`
	`Map Number: 2`
	
	`STA MAC  TV MAC  TIME TO LIVE  TV NAME`
	`----------  ----------  ----------  ----------`
	`fe80.4c4e.a7b8  509a.3a5b.6048  86400  sta1`
	`fe80.4c4e.0708  509a.3a5b.6048  120  sta2`
	`Hostname#`

Configuring the Upper Limit for MAC Address Binding Entries

- Mandatory.

Command	**bonjour-gateway airplay-fixed mac-map limit** *num*
Parameter Description	*num:* Indicates the upper limit for binding entries. The value range is from 1 to 2000.
Defaults	The upper limit for binding entries is not configured by default.
Command	Global configuration mode

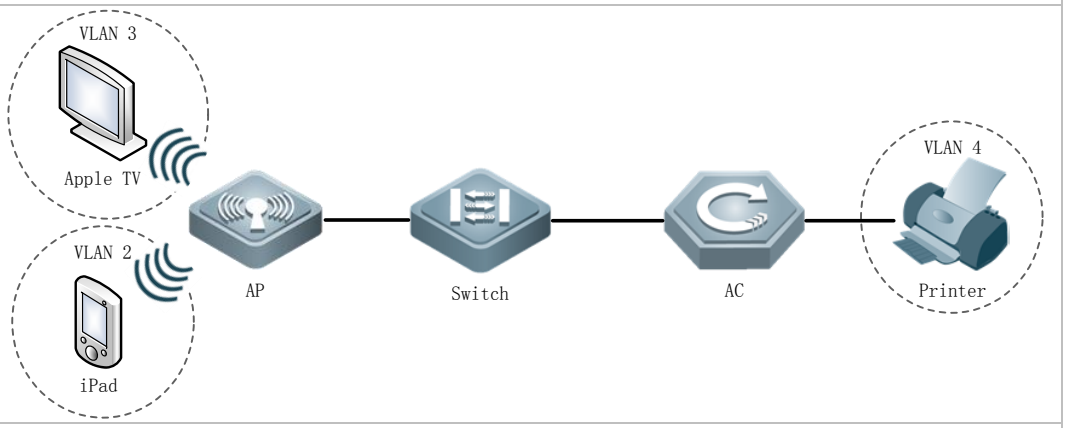
Mode	
Usage Guide	After this command is configured, if the number of MAC address binding entries for accurate screen projection exceeds the configured upper limit, new binding entries cannot be added and a prompt is displayed.

Verification

- Run the **show run** command to display the upper limit for binding entries.

Configuration Example

Configuring the Upper Limit for MAC Address Binding Entries

Scenario **Figure 1-8**	• As shown in the following figure, iPad, Apple TV, and printer reside in different VLANs. iPad needs to obtain the IP address of Apple TV through the Bonjour gateway to communicate with Apple TV and printer.
	
Configuration Steps	• Configure the upper limit for MAC address binding entries.

	`Hostname#configure terminal`
	`Hostname(config)#`
	`Hostname(config)#bonjour-gateway airplay-fixed mac-map limit 200`

Verification	• Check the upper limit for MAC address binding entries.
	`Hostname#sh run | include fixed`
	`bonjour-gateway airplay-fixed mac-map limit 200`
	`Hostname#`

Common Errors

N/A

1.4.6 Server Location Control

Configuration Effect

- After Bonjour server location control is configured, the Bonjour gateway responds to clients based on the server location matching relationship.

Notes

- The Bonjour gateway must be enabled first.

Configuration Steps

Configuring Server Location Control

- Mandatory.

Command	**bonjour-gateway service-mac** *mac-address* **location-type** { **ap-location** | **ap-name** | **ap-group** } **match** { *string* | **same** }
Parameter Description	*mac-address*: Indicates the MAC address of the server that provides services. **ap-location**: Matches against the AP location. **ap-name**: Matches against the AP name. **ap-group**: Matches against the AP group. *string*: Indicates the AP location, AP name, and AP group name when combined with **ap-location**/**ap-name**/**ap-group**. **same**: Indicates that the connected AP shares the same AP location, AP name, AP group with the server when combined with **ap-location**/**ap-name**/**ap-group**.
Defaults	Bonjour server location control is disabled.
Command Mode	Global configuration mode
Usage Guide	This command is used to specify the MAC address of a server that can provide services, and the server can provide services at the configured location. When the server access the Internet through a wired connection instead of being connected to an AP. Therefore, the **same** parameter is invalid. You can directly specify the location, name, and AP group name of the AP that provides services. After this command is run, only the configured server can respond to requests, and the unconfigured server cannot provide services for the device. When the **same** or *string* parameter is used for accurate screen mirroring control, and a roaming client is still connected to the original AP rather than the AP connected to the server in the conference room, the roaming client needs to be disconnected and then reconnected.

Verification

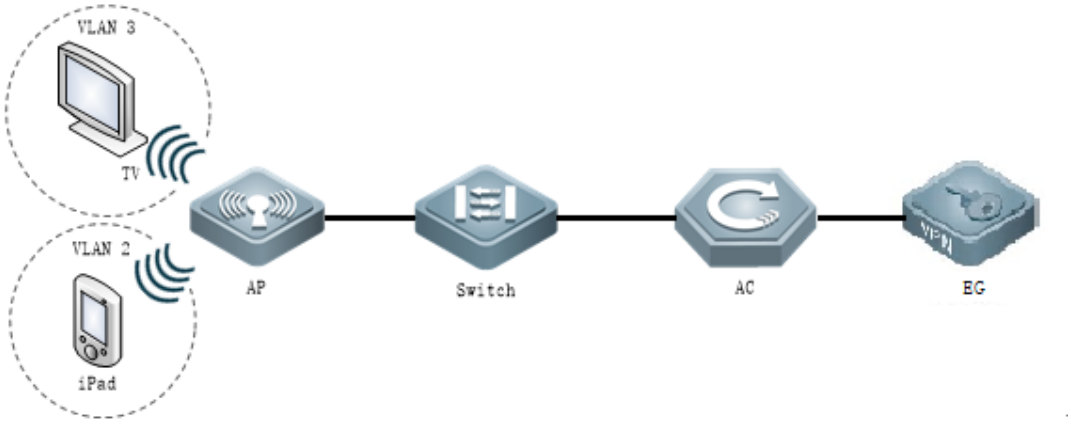
Run the **show running-config** command to check whether the configuration is successful.

Run the **show bonjour-gateway location info** command to check whether the configuration is successful.

Configuration Examples

Enabling Bonjour AP Name-based Location Control on the Server Connected to the AP to Provide Screen Mirroring Service

Scenario Figure1 -7	As shown in the following figure, the iPad and Apple TV are on different VLANs. The iPad needs to obtain the IP address of the Apple TV through the Bonjour gateway to communicate with the Apple TV. The MAC address of the Apple TV is f46d.3fe9.69d4. The iPad can obtain the screen mirroring service only when connected to the AP820-AR.

	
Configuration Steps	In global configuration mode on the AC, specify the server whose MAC address is f46d.3fe9.69d4 to provide services only for clients connected to the AP820-AR.

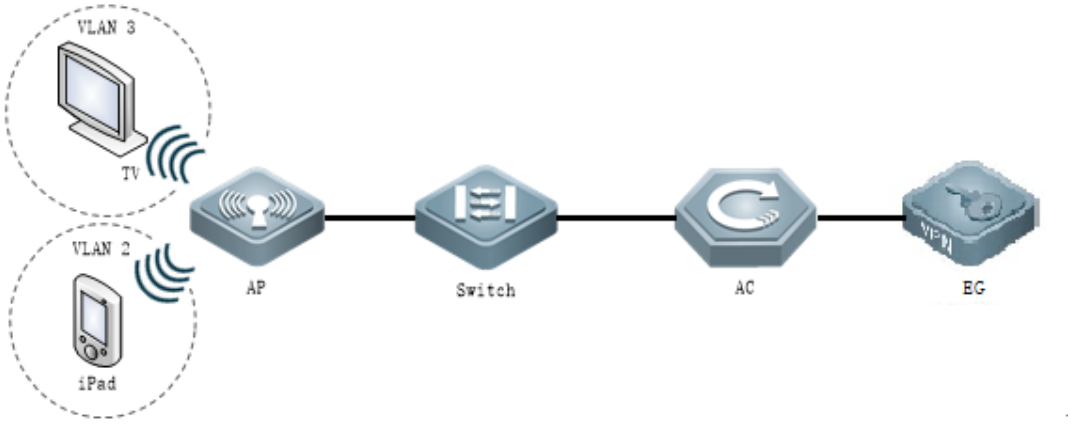
	`Hostname(config)#ap-config 7085.c487.fda2`
	`You are going to config AP(7085.c487.fda2), which is online now.`
	`Hostname(config-ap)#ap-name ap820-ar`
	`Hostnameconfig-ap)#exit`
	`Hostname(config)# bonjour-gateway service-mac f46d.3fe9.69d4 location-type ap-name match ap820-ar`

Verification	● Run the **show running-config** command on the AC to check whether the Bonjour server location control is configured.
	`Hostname# show running-config | include location-type`
	`bonjour-gateway service-mac f46d.3fe9.69d4 location-type ap-name match ap820-ar`

	● Run the **show bonjour-gateway location info** command on the AC to check whether the configuration is successful.
	`Hostname#show bonjour-gateway location info`
	`Total number of config service mac: 1`
	`SERVICE MAC SERVICE_AP MAC LOCATION TYPE MATCH NAME`
	`---------- ---------- ---------- ----------`
	`f46d.3fe9.69d4 7085.c487.fda2 ap-name name ap820-ar`

Enabling Bonjour AP Group-based Location Control on the Server Connected to the AP to Provide Screen Mirroring Service

Scenario Figure1 -8	As shown in the following figure, the iPad and Apple TV are on different VLANs. The iPad needs to obtain the IP address of the Apple TV through the Bonjour gateway to communicate with the Apple TV. The MAC address of the Apple TV is f46d.3fe9.69d4. The iPad can obtain the screen mirroring service only when it goes online by associating with the AP in the AP group where the Apple TV is online.

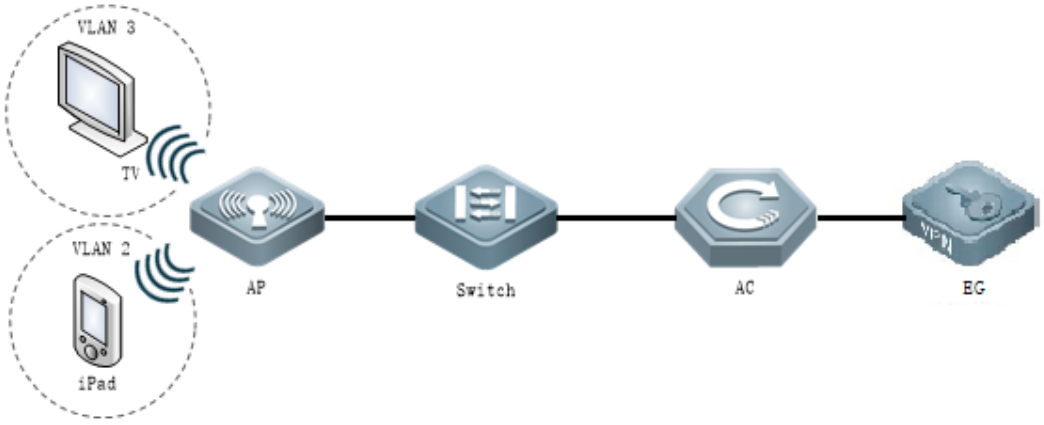
	
Configuration Steps	In global configuration mode on the AC, specify the server whose MAC address is f46d.3fe9.69d4 to provide services only for clients connected to the AP in the AP group where the server is online.
	`Hostname(config)# bonjour-gateway service-mac f46d.3fe9.69d4 location-type ap-group match same`

Verification	● Run the **show running-config** command on the AC to check whether the Bonjour server location control is configured.
	`Hostname# show running-config | include location-type`
	`bonjour-gateway service-mac f46d.3fe9.69d4 location-type ap-group match same`

	● Run the **show bonjour-gateway location info** command on the AC to check whether the configuration is successful.
	`Hostname#show bonjour-gateway location info`
	`Total number of config service mac: 1`
	`SERVICE MAC SERVICE_AP MAC LOCATION TYPE MATCH NAME`
	`---------- ---------- ---------- ----------`
	`f46d.3fe9.69d4 7085.c487.fda2 ap-group same group1`

Enabling Bonjour AP Location-based Location Control on the Server Connected to the AP to Provide Screen Mirroring Service

Scenario Figure1 -9	As shown in the following figure, the iPad and Apple TV are on different VLANs. The iPad needs to obtain the IP address of the Apple TV through the Bonjour gateway to communicate with the Apple TV. The MAC address of the Apple TV is f46d.3fe9.69d4. The iPad that go online at the same AP location can obtain the screen mirroring service provided by the Apple TV.

	
Configuration Steps	In global configuration mode on the AC, specify the server whose MAC address is f46d.3fe9.69d4 to provide services only for the iPad that goes online with the AP location set to test. Regardless of whether the iPad is connected to AP 1 or AP 2, the iPad can obtain the service provided by the Apple TV.

	`Hostname(config)#ap-config AP1`
	`Hostname(config-ap)#location test`
	`Hostname(config-ap)#exit`
	`Hostname(config)#ap-config AP2`
	`Hostname(config-ap)#location test`
	`Hostname(config-ap)#exit`
	`Hostname(config)# bonjour-gateway service-mac f46d.3fe9.69d4 location-type ap-location match test`

Verification	● Run the **show running-config** command on the AC to check whether the Bonjour server location control is configured.
	`Hostname# show running-config | include location-type`
	`bonjour-gateway service-mac f46d.3fe9.69d4 location-type ap-location match any`

	● Run the **show bonjour-gateway location info** command on the AC to check whether the configuration is successful.
	`Hostname#show bonjour-gateway location info`
	`Total number of config service mac: 1`
	`SERVICE MAC SERVICE_AP MAC LOCATION TYPE MATCH NAME`
	`---------- ---------- ---------- ----------`
	`f46d.3fe9.69d4 7085.c487.fda2 ap-location name test`

Enabling Bonjour Location Control on the Server Connected to a Wired Network to Provide Screen Mirroring Service

Scenario	The Apple TV access the Internet through a wired connection instead of being connected to an AP. The iPad needs to obtain the IP address of the Apple TV through the Bonjour gateway to communicate with the Apple TV. The MAC address of the Apple TV is f46d.3fe9.69d4. The iPad can only obtain the screen mirroring service when connected to the AP at location_1.

Configuration Steps	The Apple TV is not directly connect to APs. Therefore, the **same** keyword cannot be used. You can precisely configure the AP location, AP name, and AP group name that can be matched to provide services. The server with the MAC address of f46d.3fe9.69d4 can only provide services for clients connected to the AP at location_1.

	`Hostname(config)#ap-config 7085.c487.fda2`
	`You are going to config AP(7085.c487.fda2), which is online now.`
	`Hostname(config-ap)#location location_1`
	`Hostname(config-ap)#exit`
	`Hostname(config)# bonjour-gateway service-mac f46d.3fe9.69d4 location-type ap-location match location_1`

Verification	● Run the **show running-config** command on the AC to check whether the Bonjour server location control is configured.
	`Hostname# show running-config | include location-type`
	`bonjour-gateway service-mac f46d.3fe9.69d4 location-type ap-location match location_1`

	● Run the **show bonjour-gateway location info** command on the AC to check whether the configuration is successful.
	`Hostname#show bonjour-gateway location info`
	`Total number of config service mac: 1`
	`SERVICE MAC SERVICE_AP MAC LOCATION TYPE MATCH NAME`
	`---------- ---------- ---------- ----------`
	`f46d.3fe9.69d4 -- ap-location name location_1`

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show bonjour-gateway service-database	Displays information about the discovered Bonjour service.
show bonjour-gateway service-database ip *address*	Displays information about the discovered Bonjour service of a specified IP address.
show bonjour-gateway strategy-mode	Displays Bonjour policy information.
show bonjour-gateway mac-map info [json]	Displays MAC address binding entry information.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description

debug bonjour error	Debugs the Bonjour gateway error.
debug bonjour stamng	Debugs preemption of the Bonjour gateway.

1 Configuring IPv6 Basics

1.1 Overview

As the Internet evolves rapidly and IPv4 address space becomes increasingly scarce, IPv4 limitations become obvious. Extensive research and development have been focused on the next-generation Internet Protocol (IPng). The IPng working group of the Internet Engineering Task Force (IETF) has developed a new protocol called IP Version 6 (IPv6), as outlined 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 the intranet subnet.

↘ Simpler Packet Header Format

To minimize the packet header overhead, the design principle of the IPv6 packet header involves moving some non-essential and optional fields to the extended header. As a result, although an IPv6 address is four times longer than an IPv4 address, the IPv6 packet header is only twice as large as its IPv4 counterpart. This design makes device forwarding more efficient. For instance, the absence of a checksum in the IPv6 packet header means that devices don't need to process fragments, as fragmentation is handled 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 services for PnP. Particularly, IPv6 offers two types of auto-configuration: stateful and stateless auto-configuration. In IPv4, the 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 calls 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 configuration.

↘ Security

Internet Protocol Security (IPsec), which is an optional extension for IPv4, is integrated into IPv6 to provide security for IPv6 packets. IPv6 includes two mechanisms for this purpose: Authentication Header (AH) and Encapsulated Security

Payload (ESP). AH ensures data integrity and authenticates the source of IP packets to verify that they originate from the nodes specified by source addresses. Meanwhile, ESP provides data encryption to enable end-to-end confidentiality.

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 and allow users to specify QoS requirements. A device can identify all packets belonging to a specific data stream based on this field and process these packets according to user requirements.

NDP 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 but not 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
- RFC8106 - IPv6 Router Advertisement Options for DNS Configuration

1.2 Applications

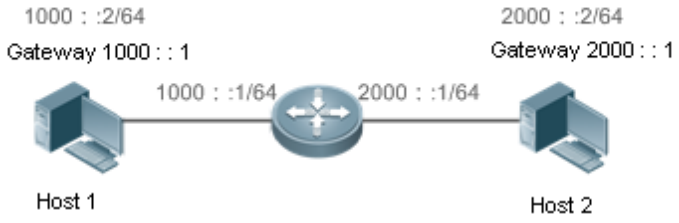
Application	Description
Communication Based on IPv6 Addresses	Two PCs communicate with each other using IPv6 addresses.

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 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 a more flexible representation.
IPv6 Address Type	IPv6 identifies network applications based on addresses.
IPv6 Packet Header Format	IPv6 simplifies 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 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 (similar to ARP), next-hop determination, Neighbor Unreachability Detection (NUD), Duplicate Address Detection (DAD), and redirection.
Configuring the Interface to Generate a Default Route Based on the RA Packet ● By default, no default route is generated based on the RA packet. ● Run the **ipv6 nd ra default route** command in interface configuration mode to generate a default route based on the RA packet. IPv6 Source Routing	This feature is used to specify the intermediate nodes that a packet passes through along the path to the destination address. It is similar to the IPv4 loose source routing option and loose record routing option.
Limiting the Rate for Sending ICMPv6 Error Messages	This feature prevents DoS attacks.

Feature	Description
IPv6 Hop Limit	This feature prevents useless unicast packets from being unlimitedly transmitted on the network and wasting network bandwidth.
Enabling Suppression of Broadcasting NS Packets to Authentication VLANs	In gateway authentication mode, the device is suppressed from broadcasting NS packets to authentication VLANs.
Configuring the Device Enabled with IPv6 ND to Allocate Different Prefixes to Different Users	Different IPv6 prefixes can be allocated to different users.
Enabling ND Packet Rate Statistics Collection	You can count the number of ND packets sent and received on all IPv6 interfaces, and their corresponding rates.
Binding the DNS Address Pool to the IPv6 Interface	The DNS address pool is bound to the IPv6 interface to carry the DNS address information in the DNS address pool when the interface announces router advertisement (RA) information.

1.3.1 IPv6 Address Format

An IPv6 address is represented in 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 4 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 leading zeros in each integer. If an IPv6 address contains a string of zeros (as shown in the preceding second and third examples), 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 expanded to a full 128-bit format. This notation can only be used when the 16-bit groups being replaced are all zeros, and a double colon can appear only once in an IPv6 address.

In environments with both IPv4 and IPv6, an IPv6 address can include an IPv4 address in its least significant 32 bits. This mixed representation is formatted as X:X:X:X:X:X:d.d.d.d, where X represents hexadecimal values and d represents 8-bit decimal values. For example, the IPv6 address 0:0:0:0:0:0:192.168.20.1 can be abbreviated to ::192.168.20.1. Common uses include IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. IPv4-compatible addresses, such as ::1.1.1.1, are now obsolete, while IPv4-mapped addresses, such as ::FFFF:1.1.1.1, are used to represent IPv4 addresses within an IPv6 format.

An IPv6 address is divided into two parts: subnet prefix and interface ID. It can be expressed with an additional value based on an address allocation method such as Classless Inter-Domain Routing (CIDR). This additional value shows how many bits of the address represent the network part. Essentially, the IPv6 address includes the prefix length, which is separated from the address by a slash. For example, in 12AB::CD30:0:0:0:0/60, the prefix length 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.
- 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 (interfaces 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. 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 abbreviated to ::. It has two purposes:

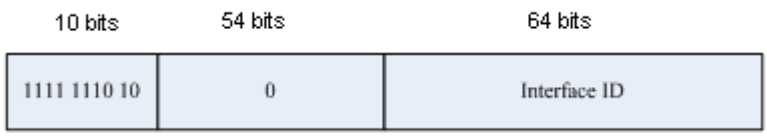
1. If a host has no unicast address upon startup, it uses the unspecified address as the source address to send an RS packet to obtain prefix information from the gateway and thereby generate a unicast address.
2. When an IPv6 address is configured for a host, the device detects whether the address conflicts with addresses of other hosts on 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 often used by a node to send itself packets.

- Link-local address

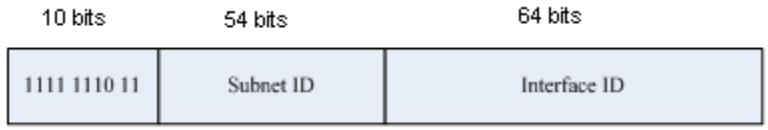
Figure 1-2 Format of a Link-local Address



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 does not forward 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 to (2^{64}-1) hosts.

- Site-local address

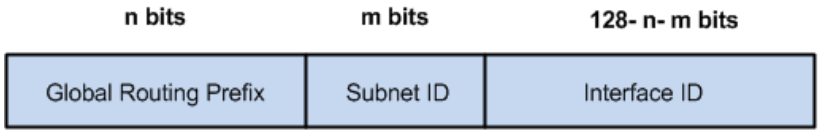
Figure 1-3 Format of a Site-local Address



A site-local address is used to transmit data within a site. A device does not forward 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). The 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

Figure 1-4 Format of a Global Unicast Address



Among global unicast addresses, there is a type of IPv4-embedded IPv6 addresses, including IPv4-compatible IPv6 addresses and IPv4-mapped IPv6 addresses. They are used for interconnection between IPv4 and IPv6 nodes.

Figure 1-5 Format of an IPv4-compatible IPv6 Address

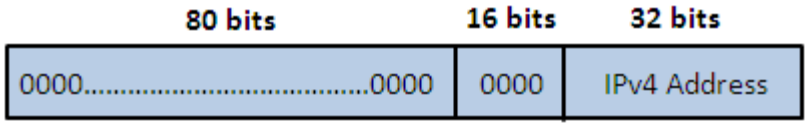
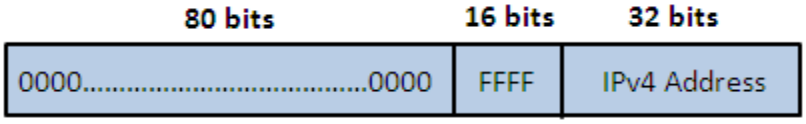


Figure 1-6 Format of an IPv4-mapped IPv6 Address



IPv4-compatible IPv6 addresses are mainly used on automatic tunnels. Nodes on automatic tunnels support both IPv4 and IPv6. Using these addresses, IPv4 devices transmit IPv6 packets over tunnels. IPv4-compatible IPv6 addresses have been abolished; IPv4-mapped IPv6 addresses are used by IPv6 nodes to access IPv4-only nodes. For example, if an IPv6 application on an IPv4/IPv6 host requests to resolve the name of an IPv4-only host, the name server dynamically generates an IPv4-mapped IPv6 address and returns it to the IPv6 application.

↘ 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 4 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 4 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:

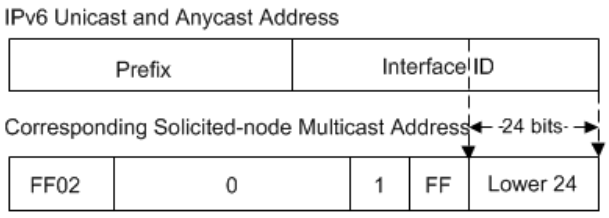
1. Multicast address for all nodes on the local link, that is, FF02::1
2. Solicited-node multicast address, prefixed with FF02:0:0:0:0:1:FF00:0000/104

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.

Figure 1-7 Format of an Solicited-node Multicast Address



Anycast Addresses

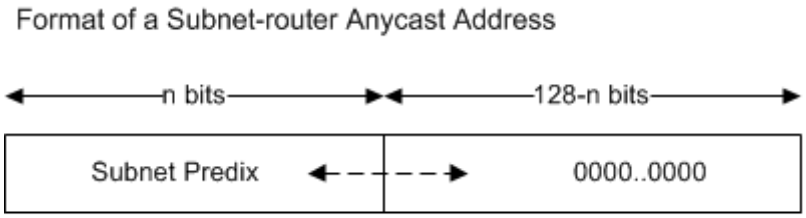
Similar to a multicast address, an anycast address can also be shared by multiple nodes. The difference is that only one node in the anycast address receives data packets, while all nodes in a multicast address receive data packets. Anycast addresses are allocated within the standard IPv6 unicast address space, so they share the same formats as unicast addresses. Each node that is part of an anycast address must be explicitly configured for proper identification.

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 followed by 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



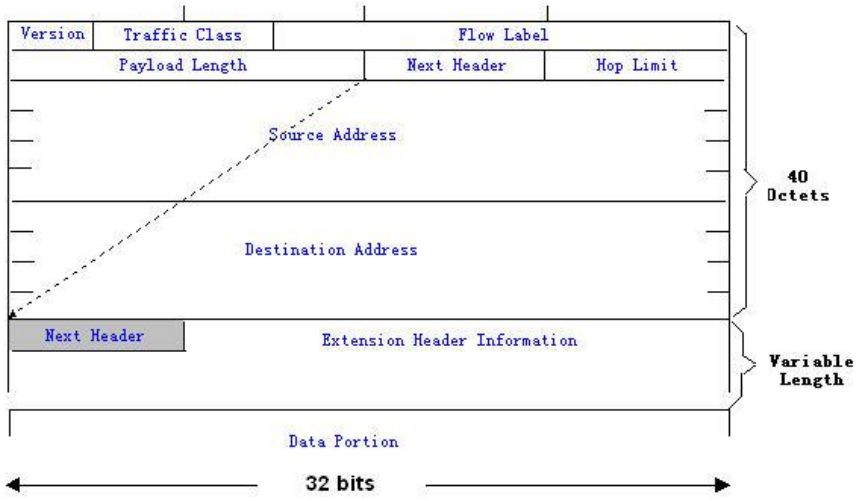
Related Configuration

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 Format of the IPv6 Packet Header



The IPv4 packet header is expressed in the unit of 4 bytes. The IPv6 packet header consists of 40 bytes, in the unit of 8 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. It 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 signal the presence of the IPv6 extension header.

- Hop Limit

This field consists of 8 bits. Each time a device forwards a packet, the field value is 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.

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 passerby nodes. The initial destination address in the IPv6 packet header is the first address among 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, 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. The Destination Options field can only be filled with integral multiples of 64 bits (8 bytes) if required. This extension header can be used to carry information to be checked by the destination node.

- Upper-layer header

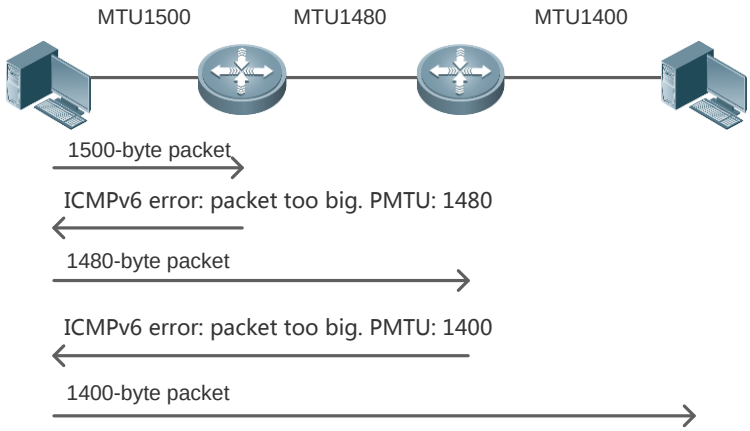
This extension header indicates the protocol used at the upper layer, such as TCP (6) and UDP (17).

Another two extension headers of AH and ESP will be described in *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 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 fragments packets. 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 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 change the IPv6 MTU of an interface.

Configuring a Static PMTU

- Run the **ipv6 path-mtu** command to configure a static PMTU.

Configuring the Aging Time for a Dynamic PMTU

- The default aging time is 10 minutes.
- Run the **ipv6 path-mtu age** command to configure the aging time of the dynamic PMTU.

1.3.5 IPv6 Neighbor Discovery

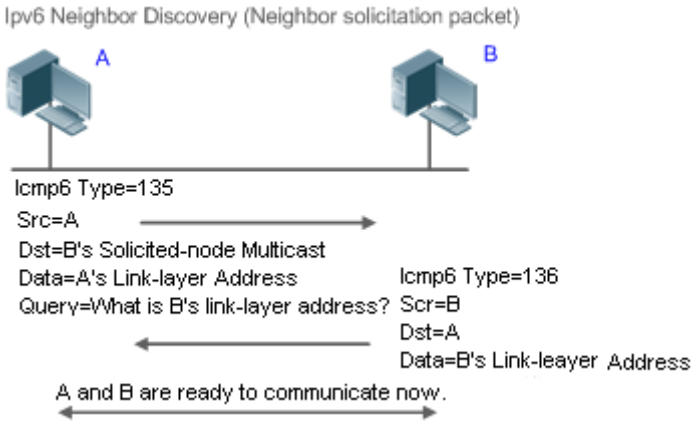
NDP is a basic part of IPv6. Its main functions include router discovery, prefix discovery, parameter discovery, address auto-configuration, address resolution (similar to ARP), next-hop determination, NUD, DAD, and redirection. NDP defines five ICMP packets: RS (ICMP type: 133), RA (ICMP type: 134), NS (similar to ARP request, ICMP type: 135), NA (similar to ARP reply, ICMP type: 136), and ICMP Redirect (ICMP type: 137).

All the preceding ICMP packets carry one or more options, which may be optional in some cases but crucial in other cases. NDP defines five main 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, link-layer address of the solicited node. After receiving the NA packet, the source node can communicate with the destination node.

Figure 1-11 Address Resolution Process



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

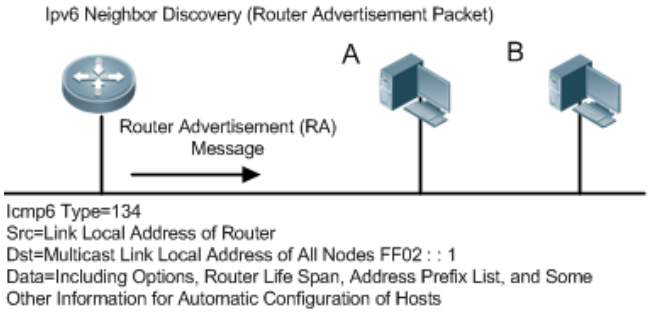
To know whether the IPv6 address configured for a host is unique, the device needs to perform DAD by sending an NS packet in which the source IPv6 address is the unspecified address.

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 RA Packet Sending Process



An RA packet usually contains the following content:

- One or more IPv6 address prefixes (used for on-link determination or stateless address auto-configuration)
- Validity of the IPv6 address prefix
- Host auto-configuration mode (stateful or stateless)
- Default device information (whether the device acts as the default device; interval for acting as the default device if the device is used as the default one)
- Other information provided for host configuration, such as the hop limit, MTU, and NS retransmission interval
- Route priority

RA packets can be also used as replies to the RS packets sent by a host. Using RS packets, a host can obtain the auto-configured information immediately upon startup, without waiting for the RA packets sent by the device. If no unicast address is configured for a newly started host, the host uses the unspecified address (0:0:0:0:0:0:0:0) as the source address in the RS packet. Otherwise, the host uses the configured unicast address as the source address and the multicast address of all local routing devices (FF02::2) as the destination address in the RS packet. As a reply to the RS packet, the RA packet uses the source address of the RS packet as the destination address (if the source address is the unspecified address, it uses the multicast address of all local nodes (FF02::1).

In an RA packet, the following parameters can be configured:

- Ra-interval: Interval for sending the RA packet.
- Ra-lifetime: Lifetime of a router, that is, whether the device acts as the default router on the local link and the interval for acting as the default router.
- Prefix: Prefix of an IPv6 address on the local link. It is used for on-link determination or stateless address auto-configuration, including other parameter configurations related to the prefix.
- Ns-interval: NS packet retransmission interval.
- Reachabletime: Period when the device regards a neighbor reachable after detecting a Confirm Neighbor Reachability event.
- Ra-hoplimit: Number of hop of the RA packet, which is used to set the hop limit for a host to send a unicast packet.
- Ra-mtu: MTU of the RA packet.
- Managed-config-flag: Whether a host receiving this RA packet obtains the address through stateful auto-configuration.
- Other-config-flag: Whether a host receiving this RA packet uses DHCPv6 to obtain other information except the IPv6 address for auto-configuration.

- RDNSS and DNSSL options: Provide IPv6 terminals with the address of the DNS recursive query server and a search list of DNS domain names.

Configure the preceding parameters when configuring IPv6 interface attributes.

Redirection

If a router receiving an IPv6 packet finds a better next hop, it sends the ICMP Redirect packet to inform the host of the better next hop. The host will directly send the IPv6 packet to the better next hop next time.

Maximum Number of Unresolved ND Entries

- To prevent malicious scanning of network segments that generates a large number of unresolved neighbor entries and consumes excessive memory, you can configure a limit on the maximum number of unresolved neighbor entries.

Maximum Number of ND Options

- To prevent forged ND packets from carrying an excessive number of ND options that can overwhelm the device's CPU, you can configure the maximum number of ND options.

Maximum Number of Neighbor Learning Entries on an Interface

- To prevent neighbor learning attacks that consume device neighbor table entries, use up memory, and impact forwarding performance, you can configure the maximum number of interface neighbor learning entries.

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. The 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 60s.
- Run the **ipv6 nd dad retry** value command in global configuration mode to configure the DAD interval. The 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 change 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 change 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 or Disabling RA Packet 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 packet suppression.

Configuring the Maximum Number of Unresolved ND Entries

- The default value is 0, indicating that unresolved ND entries are not limited. It depends on 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 proactively 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 that neighbors learned on an interface are not limited.

Configuring the Interface to Generate a Default Route Based on the RA Packet

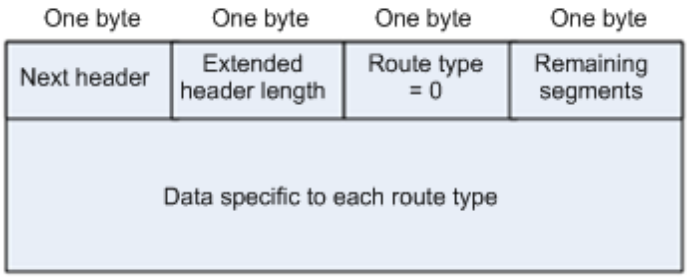
- By default, no default route is generated based on the RA packet.
- Run the **ipv6 nd ra default route** command in interface configuration mode to generate a default route based on the RA packet.

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.

Figure 1-13 Format of the IPv6 Routing Header



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.

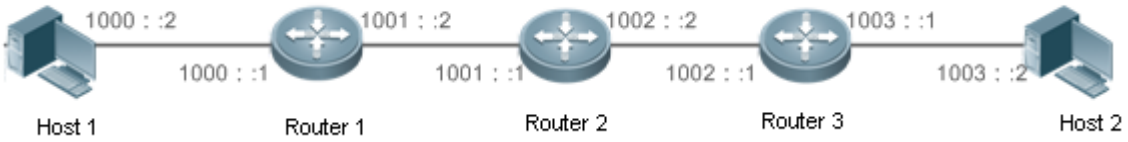
Two routing types are defined: Type 0 and Type 2. The Type 2 routing header is used for mobile communication. RFC 2460 defines the Type 0 routing header (similar to the loose source routing option of IPv4).

Figure 1-14 Format of the Type 0 Routing Header



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 forwarding.

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.

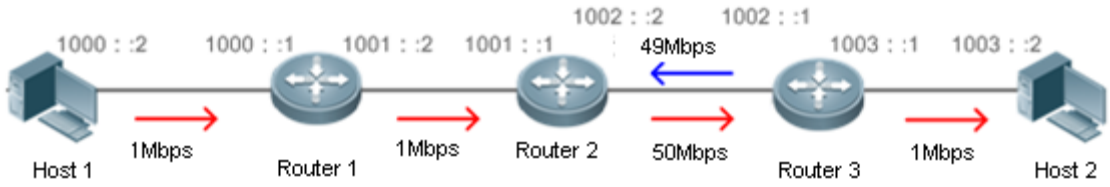
2 Router 1 forwards this packet to Router 2.

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. Then 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. Then 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 this time point, 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." Considering security, 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 Limiting the Rate for Sending 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. When attacks of invalid IPv6 packets occur, the device may continuously reply to ICMPv6 error messages till device resources are exhausted and thereby fail to provide services. To solve this problem, you can restrict the rate for sending 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 for IPv6 PMTUD. If the rate for sending ICMPv6 error messages is limited due to excessive other ICMPv6 error messages, ICMPv6 Packet Too Big messages may be filtered, causing a failure of IPv6 PMTUD. Therefore, you are advised to separately limit the rates for sending ICMPv6 Packet Too Big messages and other ICMPv6 error messages.

ICMPv6 Redirect messages are not ICMPv6 error messages, and the rates of ICMPv6 Redirect messages and other ICMPv6 error message are limited together.

Related Configuration

Configuring the Rate for Sending 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 rate for sending ICMPv6 Packet Too Big messages.

Configuring the Rate for Sending Other ICMPv6 Error Messages

- The default rate is 10 per 100 ms.
- Run the **ipv6 icmp error-interval** command to configure the rate for sending 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 each time the packet passes through a router. When the hop limit decreases to 0, the router discards the packet to prevent the 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 Enabling Suppression of Broadcasting NS Packets to Authentication VLANs

Working Principle

In gateway authentication mode, all sub-VLANs in a super-VLAN are authenticated VLANs by default. Users in an authenticated VLAN can access a network only after being authenticated. After a user is authenticated, a static ND entry is generated on the device. Therefore, when accessing an authenticated user, the device does not need to send NS packets to the authenticated VLAN to which the authenticated user belongs.

In gateway authentication mode, the device is enabled with suppression of broadcasting NS packets to authentication VLANs by default. If the device needs to access non-authenticated users in an authenticated VLAN, disable the suppression function.

Related Configuration

Enabling Suppression of Broadcasting NS Packets to Authentication VLANs

- In interface configuration mode, run the **ipv6 nd suppress-auth-vlan-ns** command to enable suppression of broadcasting NS packets to authentication VLANs.
- The device is enabled with suppression of broadcasting NS packets to authentication VLANs by default.
- This function can be configured only on SVIs and takes effect only in gateway authentication mode.

1.3.10 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.

1.3.11 Enabling ND Packet Rate Statistics Collection

Working Principle

The device counts the number of ND (RS/RA/NS/NA) packet 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.

1.3.12 Binding the DNS Address Pool to the IPv6 Interface

Working Principle

The DNS address pool is bound to the IPv6 interface to carry the DNS address information in the DNS address pool when the interface announces router advertisement (RA) information.

Related Configuration

Configuring the IPv6 Interface to Bind the DNS Address Pool

- In interface configuration mode, run the **ipv6 nd ra dns import-rdnss** *pool-name* command to configure the name of the DNS address pool to be bound to the IPv6 interface.
- By default, no DNS address pool is bound to the IPv6 interface.

1.4 Configuration

Configuration	Description and Command
Configuring an IPv6	(Mandatory) It is used to configure IPv6 addresses and enable IPv6.

Configuration	Description and Command	
Address	**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 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 reachable-time	Configures the reachable time of a neighbor.
	ipv6 nd prefix	Configures the address prefix to be advertised in an RA packet.
	ipv6 nd suppress-ra	Enables RA packet suppression on an interface.
	ipv6 nd managed-config-flag	Configures the **managed address configuration** flag bit of the RA packet.
	ipv6 nd ra-hoplimit	Configures the hop count of an RA packet.
	ipv6 nd ra-interval	Configures the interval for sending RA packets.
	ipv6 nd ra-lifetime	Configures the device lifetime of the RA packet sent on the interface.
	ipv6 nd ra-mtu	Configures the MTU of RA packets.
	ipv6 nd resolve vlan	Configures the device to proactively send NS packets to specific sub-VLANs in the super-VLAN.
	ipv6 nd stale-time	Configures the period for the neighbor to maintain the state.
	ipv6 ns-linklocal-src	Configures the local address of the link as the source IP address for sending neighbor requests.
	(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 ND packet option fields.	
	ipv6 nd max-opt	Configures the maximum number of ND packet option fields.
	(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.
	(Optional) It is used to configure the interval for the interface to retransmitting	

Configuration	Description and Command	
	Neighbor Solicitation (NS) packets.	
	ipv6 nd ns-interval	Configures the interval for the interface to retransmitting NS packets.
	⚠ (Optional) It is used to configure the interface to generate a default route based on the received RA.	
	ipv6 nd ra default route	Configures the interface to generate a default route based on the received RA.

Configuring the NS Retransmission Interval of the Interface
Configuration Steps
Set the Neighbor Solicitation (NS) retransmission interval to 2 seconds.
`Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ns-interval 2000`
Verification
Run the **show running-config** command to check whether the configuration takes effect.
`Hostname#show running-config`
`!`
`interface GigabitEthernet 0/1`
`ipv6 nd ns-interval 2000`
`!`
	⚠ (Optional) It is used to restrict the MTU of IPv6 packets sent on an interface.	

	ipv6 mtu	Configures the IPv6 MTU.

Configuration	Description and Command	

↘ **Configuring the Interface to Generate a Default Route Based on the Received RA**
 	
Configuration Steps Configure the VLAN 1 interface to generate a default route based on the RA.
`Hostname(config)#interface VLAN 1`
`Hostname(config-if-VLAN 1)#ipv6 nd ra default route`
Verification Run the **show running-config** command to check whether the configuration takes effect.
`Hostname#show running-config`
`!`
`interface VLAN 1`
`ipv6 nd ra default route`
`!`
Enabling PMTUD		

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 Rate for	⚠ Optional.	

Configuration	Description and Command	
Sending ICMPv6 Error Messages	**ipv6 icmp error-interval too-big**	Configures the rate for sending ICMPv6 Packet Too Big messages.
	ipv6 icmp error-interval	Configures the rates for sending 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.
Enabling Suppression of Broadcasting NS Packets to Authentication VLANs	⚠ (Optional) It is used in gateway authentication mode to enable suppression of broadcasting NS packets to authentication-free VLANs.	
	ipv6 nd suppress-auth-vlan-ns	Enables suppression of broadcasting NS packets to authentication VLANs.
Configuration Effect	⚠ (Optional) It is used to carry the DNS address information in the DNS address pool when the interface announces the RA information.	
	ipv6 nd ra dns import-rdnss *pool-name*	Binds the DNS address pool to the IPv6 interface.

1.4.1 Configuring an IPv6 Address

Configuration Effect

Configure the IPv6 address of an interface to implement IPv6 network communication.

Configuration Step

↘ 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 running the **ipv6 enable** command in interface configuration

	mode or 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 comply with the format defined in RFC 4291. *eui-64*: Indicates the created IPv6 address that consists 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: 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 *Configuring DHCPv6*). The sub prefix and host bits are specified by *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 colon hexadecimal notation as defined 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.

Configuring an Interface to Borrow the IPv6 Unicast Address of Another Interface

Command	**ipv6 unnumbered** *interface-id*
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Borrowing the address of another interface can save IPv6 address resources. This command is only supported on PPP interfaces. If the **ipv6 unnumbered** command is configured on an interface, the IPv6 function is enabled automatically on the interface. You cannot disable IPv6 on the interface even by running the **no ipv6 enable** command.

Configuration Example

Configuring an IPv6 Address on an Interface

Configuration Steps	● Enable IPv6 on GigabitEthernet 0/1 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 GigabitEthernet 0/1.

	`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 packet 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 Step

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 disable DAD for IPv6 addresses on an interface or change 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 change 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 or Disabling RA Packet 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 and affecting device performance.

Configuring the Interval for Retransmitting NS Packets on an Interface

- Optional.
- If a large number of IPv6 hosts are deployed on a network, prolong the interval for transmitting NS packets. When the status of many interfaces change, frequent NS packet handling consumes the memory and affect device performance, resulting in exceptions. This function addresses this issue.

Configuring the Interface to Generate a Default Route Based on the Received RA

- Optional.
- Only in case of DHCPv6 stateful address auto-configuration, run the **ipv6 nd ra default route** command to automatically generate a default route.
- 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-info**: Check whether the prefix and other information configured for RA packets are correct.

Related Commands

Enabling IPv6 Redirection on an Interface

Command	**ipv6 redirects**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	All ICMPv6 error messages are transmitted at a limited rate. By default, a maximum number of 10 ICMPv6 error messages are transmitted per second (10 pps).

Configuring the Number of Consecutive NS Packets Sent During DAD

Command	**ipv6 nd dad attempts** *value*
Parameter Description	*value*: Indicates the number of NS packets.
Command	Interface configuration mode

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. In this case, you must configure a new address and restart the interface to re-enable DAD. When an interface changes from Down to Up, 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 value is 60s. The value 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, in milliseconds. The value range is from 0 to 3600000. 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 this also increases network bandwidth and device resource usage. Therefore, do not set a small value. 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 the default value is recommended.

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* }]] [**off-link** | **no-autoconfig**] * | **no-advertise** }
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, which is followed by the prefix. *valid-lifetime*: Indicates the period when a host receiving the prefix of an RA packet regards the prefix valid. The value range is from 0 to 4294967295. 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 range is from 0 to 4294967295. 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 by specifying a fixed time for each prefix in an RA packet or specifying the deadline. If the deadline is specified, the valid date of the prefix in each RA packet decreases till it becomes 0.

Enabling or Disabling RA Packet Suppression on an Interface

Command	**ipv6 nd suppress-ra**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	To enable RA packet suppression on an interface, run the **ipv6 suppress-ra** command.

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 not used.

Configuring the Hop Count of RA Packets

Command	**ipv6 nd ra-hoplimit** *value*
Parameter Description	*value*: Specifies the hop count of RA packets. The value range is from 0 to 255 and the default value is 64.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Interval for Sending RA Packets

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 600s. **min-max**: Indicates the maximum and minimum interval for sending RA packets, in seconds. *min_value*: Indicates the minimum interval for sending RA packets, in seconds. *max_value*: Indicates the maximum interval for sending RA packets, in seconds.
Command Mode	Interface configuration mode
Usage Guide	If the device serves as the default device, the interval cannot be longer than the lifetime of the device. To ensure that other devices along the link occupies network bandwidth while sending RA packets, the actual interval for sending RA packets will vary by 20% around the set value. If **min-max** is specified, the actual interval for sending RA packets will be selected between the minimum value and maximum value.

Configuring the Device Lifetime of RA Packets 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 range is from 0 to 9000 and the default value is 64.
Command Mode	Interface configuration mode
Usage Guide	The router lifetime field is available in each RA packet. 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 must be larger than or equal to the interval for sending RA packets (ra-interval).

Configuring the MTU of RA Packets

Command	**ipv6 nd ra-mtu** *value*
Parameter Description	*value*: Indicates the MTU. The value range is from 0 to 1500. The default value is the same as the IPv6 MTU.
Command Mode	Interface configuration mode
Usage Guide	If it is specified as 0, RA packets will not carry 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 seconds. The value range is from 0 to 86400. The default value is 3,600.
Command Mode	Global 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. Moreover, more network bandwidth and device resources are consumed. Therefore, do not use a small value.

Configuring the Local Link Address as the Source Address for Sending Neighbor Requests

Command	**ipv6 ns-linklocal-src**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

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	Global configuration mode

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. The configured value must be greater than or equal to the number of ND entries learned by the interface. Otherwise, the configuration does not take effect. The value depends on the ND entry capacity supported by the device.

Configuring the Interval for the Interface to Retransmit NS Packets

Command	**ipv6 nd ns-interval** *milliseconds*
Parameter Description	*milliseconds*: Indicates the interval for retransmitting NS packets.
Command Mode	Interface configuration mode
Usage Guide	The configured value will be advertised through RA packets and will be used by the device itself. You are not advised to set a short interval.

Configuring the Interface to Generate a Default Route Based on the Received RA

Command	**ipv6 nd ra default route**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Only in case of DHCPv6 stateful address auto-configuration, run the **ipv6 nd ra default route** command to automatically generate a default route. The **ipv6 address autoconfig default** command also generates a default route, so you can only configure the **ipv6 address autoconfig default** or **ipv6 nd ra default route** command at only one

layer-3 interface for one device.

If the interface is bound to a multi-protocol VRF with no IPv6 address family configured, you cannot enable the feature of generating a default route on the interface. To enable the feature, configure an IPv6 address family for the multi-protocol VRF first.

Configuration Example

Enabling IPv6 Redirection on an Interface

Configuration Steps	● Enable IPv6 redirection on 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):`
	`  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 GigabitEthernet 0/0.
	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): 0/0/0, RS(input): 0 Link-layer address: 00:00:00:00:00:00 Physical MTU: 1500 ND router advertisements live for 1800 seconds ND router advertisements are sent every 200 seconds<160--240> Flags: !M!O, Adv MTU: 1500 ND advertised reachable time is 0 milliseconds ND advertised retransmit time is 0 milliseconds ND advertised CurHopLimit is 64 Prefixes: <total: 1> 1234::/64(Def, CFG, vltime: 2592000, pltime: 604800, flags: LA)

Configuring 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 running-config** command to check whether the configuration takes effect.
	Hostname#show running-config 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 running-config** command to check whether the configuration takes effect.

	`Hostname#show running-config`
	
	`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 running-config** command to check whether the configuration takes effect.

	`Hostname#show running-config`
	`!`
	`interface GigabitEthernet 0/1`
	`ipv6 nd cache interface-limit 100`
	`!`

Configuring the NS Retransmission Interval of the Interface

Configuration Steps Set the Neighbor Solicitation (NS) retransmission interval to 2 seconds.

```
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ns-interval 2000
```

Verification Run the **show running-config** command to check whether the configuration takes effect.

```
Hostname#show running-config
!
interface GigabitEthernet 0/1
 ipv6 nd ns-interval 2000
!
```

Configuring the Interface to Generate a Default Route Based on the Received RA

Configuration Steps Configure the VLAN 1 interface to generate a default route based on the RA.

```
Hostname(config)#interface VLAN 1
Hostname(config-if-VLAN 1)# ipv6 nd ra default route
```

Verification Run the **show running-config** command to check whether the configuration takes effect.

```
Hostname#show running-config
!
interface VLAN 1
 ipv6 nd ra default route
!
```

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 Step

Configuring the IPv6 MTU of an Interface

- Optional.

Configuring a Static PMTU

- Optional.

Configuring the Aging Time for a Dynamic PMTU

- Optional.

Verification

- Run the **show running-config** 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.
- Obtain the locally sent IPv6 packets of which the length exceeds the PMTU. The packet obtaining 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, in bytes. The value range is from 1280 to 1500.
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 GigabitEthernet 0/1 to 1300.
	`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 0/1 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. Devices do not support the Type 0 routing header by default. The **ipv6 source-route** command can be used in global configuration mode to enable IPv6 source routing.

Configuration Step

↘ 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	Because 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 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 Rate for Sending ICMPv6 Error Messages

Configuration Effect

Configure the rate for sending ICMPv6 error messages.

Configuration Step

Configuring the Rate for Sending 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 rate for sending error messages.

Configuring the Rate for Sending Other ICMPv6 Error Messages

- Optional.
- If a device receives many invalid IPv6 packets and thereby generates many ICMPv6 error messages, run the **ipv6 icmp error-interval** command to restrict the rate for sending ICMPv6 error messages. This command does not affect the rate for sending ICMPv6 Packet Too Big messages.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

Configuring the Rate for Sending 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, in milliseconds. The value range is from 0 to 2147483647. The default value is 100. If the value is 0, the rate for sending ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket. The value range is 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 rate for sending 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 for IPv6 PMTUD. If there are excess other ICMPv6 error messages, ICMPv6 Packet Too Big messages cannot be sent, causing a failure of IPv6 PMTUD. Therefore, you are advised to separately restrict the rates for sending ICMPv6 Packet Too Big messages and other ICMPv6 error messages. Because the precision of the timer is 10 milliseconds, you are advised 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. 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.

Configuring the Rate for Sending Other ICMPv6 Error Messages

Command	**ipv6 icmp error-interval** *milliseconds* [*bucket-size*]
Parameter Description	*milliseconds*: Indicates the refresh period of a token bucket, in milliseconds. The value range is from 0 to 2147483,647. The default value is 100. If the value is 0, the rate for sending ICMPv6 error messages is not restricted. *bucket-size*: Indicates the number of tokens in a token bucket. The value range is 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 Rate for Sending ICMPv6 Error Messages

Configuration Steps	● Set the rate for sending ICMPv6 Packet Too Big messages 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 Step

Configuring the IPv6 Hop Limit

- Optional.
- To change 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.
- Obtain IPv6 unicast packets sent by a host. The packet obtaining 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 range is 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

Common Errors

N/A

1.4.7 Enabling Suppression of Broadcasting NS Packets to Authentication VLANs

Configuration Effect

Enable suppression of broadcasting NS packets to authentication VLANs on an SVI.

Notes

This function can be configured only on SVIs and takes effect only in gateway authentication mode.

Configuration Step

Enabling Suppression of Broadcasting NS Packets to Authentication VLANs

- Optional.
- In gateway authentication mode, you can use this command to enable suppression of broadcasting NS packets to authentication VLANs.

Verification

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

Related Commands

Enabling Suppression of Broadcasting NS Packets to Authentication VLANs

Command	**ipv6 nd suppress-auth-vlan-ns**
Parameter Description	-
Command Mode	Interface configuration mode
Usage Guide	Use the **no** form of this command to disable this function.

Configuration Example

Disabling Suppression of Broadcasting NS Packets to Authentication VLANs

Configuration Steps	• Disable suppression of broadcasting NS packets to authentication VLANs.
	`Hostname(config-if-VLAN 2)# no ipv6 nd suppress-auth-vlan-ns`
Verification	• Run the **show running-config interface vlan 2** command to display the configuration.
	`Hostname# show running-config interface vlan 2` `no ipv6 nd suppress-auth-vlan-ns`

Common Errors

N/A

1.4.8 Binding the DNS Address Pool to the IPv6 Interface

1.4.9 Configuration Effect

Bind the DNS address pool to the IPv6 interface to carry the DNS address information in the DNS address pool when the interface announces RA information.

Notes

N/A

Configuration Steps

↘ Configuring the Interface Binding Prefix

- Optional.
- In interface configuration mode, run the **ipv6 nd ra dns import-rdnss** *pool-name* command to configure the name of the DNS address pool to be bound to the IPv6 interface.

Verification

- Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

↘ Configuring the Name of the DNS Address Pool to Be Bound to the IPv6 Interface

Command	**ipv6 nd ra dns import-rdnss** *pool-name*
Parameter Description	*pool-name*: Indicates the name of the DNS address pool.
Command Mode	Interface configuration mode
Usage Guide	DHCPv6 sends the DNS address pool information of the server to TCP/IP. If a DNS address pool name is bound to the interface, the announced RA route information carries the DNS address information in the DNS address pool.

Configuration Example

↘ Binding the DNS Address Pool to the IPv6 Interface

Configuration Steps Bind the ruijie DNS address pool to the GigabitEthernet 0/1 interface.

```
Hostname(config)# interfaceGigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ipv6 dhcp client pd ruijie
Hostname(config-if-GigabitEthernet 0/1)# ipv6 nd ra dns import-rdnss ruijie
```

Verification Run the **show running-configinterface** GigabitEthernet 0/1 command to check whether the configuration takes effect.

```
Hostname#show running-config interface GigabitEthernet 0/1
ipv6 nd ra dns import-rdnss ruijie
```

Common Errors

N/A

1.5 Monitoring

Clearing

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

Command	Description
clear ipv6 neighbors [*interface-type interface-number*]	Clears dynamically learned neighbors.

Displaying

Command	Description
show ipv6 address [*interface-name*]	Displays IPv6 addresses.
show ipv6 general-prefix	Displays information about the general prefix.
show ipv6 interface [[*interface-id*] [ra-info]] [brief [*interface-id*]]	Displays IPv6 information about an interface.
show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]	Displays neighbor information.
show ipv6 neighbors statistics	Displays statistics on IPv6 neighbor tables.
show ipv6 neighbor statistics per-mac [*interface-name*] [*mac-address*]	Displays the number of ND entries corresponding to each MAC address.
show ipv6 nd-packet [**interface** *interface-name*] **statistics**	Displays statistics on ND packets.
show ipv6 raw-socket [*num*]	Displays all IPv6 raw sockets.
show ipv6 routers [*interface-type interface-number*]	Displays information about neighbor routers and RA packets.
show ipv6 sockets	Displays all IPv6 sockets.
show ipv6 udp [**local-port** *num*] [**peer-port** *num*]	Displays all IPv6 UDP sockets.
show ipv6 udp statistics	Displays statistics on IPv6 UDP sockets.
show ipv6 nd ra received rdnss [**interface** *interface-name*]	Displays the rdnss information.
show ipv6 nd ra received dnssl [**interface** *interface-name*]	Displays the dnssl information.
show ipv6 nd ra dns server	Displays the server address information of the DNS recursive resolution service provided by the RDNSS option in the RA packet as well as the suppression status of the RDNSS option and the interface information.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug ipv6 nd	Debugs ND entry learning.

1 Configuring DHCPv6

1.1 Overview

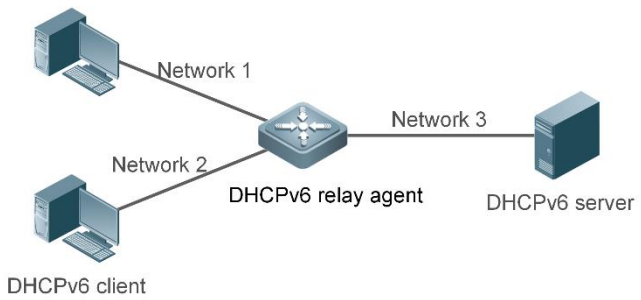
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) allows a DHCP server to transfer configurations (such as IPv6 addresses) to IPv6 nodes.

Compared with other IPv6 address allocation methods, such as manual configuration and stateless automatic address configuration, DHCPv6 provides address allocation, prefix delegation, and configuration parameter allocation.

- DHCPv6 is a stateful protocol for automatically configuring addresses and flexibly adding and reusing network addresses. It records allocated addresses and enhances network manageability.
- Using prefix delegation of DHCPv6, uplink network devices can allocate address prefixes to downlink network devices, enabling flexible station-level automatic configuration and control of station address space.
- The DHCPv6 configuration parameter allocation addresses the issue of obtaining parameters through a stateless automatic address configuration protocol, allocating DNS server addresses and domain names to hosts.
- DHCPv6 works on the client/server model. A DHCPv6 client requests configurations, while a DHCPv6 server provides them. If the DHCPv6 client and DHCPv6 server are on different network links, they can interact with each other through using a DHCPv6 relay agent.

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. This may complicate management and upgrade, resulting in extra deployments (a DHCPv6 server is deployed for each subnet). The DHCPv6 relay agent can solve these problem by enabling a DHCPv6 client to send messages to a DHCPv6 server on a different link. The DHCP relay agent is often deployed within the link where a DHCPv6 client resides and is used to relay interaction messages between the DHCPv6 client and DHCPv6 server. The DHCP relay agent is transparent to the DHCPv6 client.

Figure 1-1



Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol for IPv6
- RFC 3633: IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6
- RFC 3646: DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3736: Stateless DHCP Service for IPv6

- RFC 5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

1.2 Applications

Application	Description
Requesting/Allocating Addresses and Configuration Parameters	A DHCPv6 client requests addresses from a DHCPv6 server. The DHCPv6 server allocates addresses and configuration parameters to the DHCPv6 client.
Requesting/Allocating Prefixes	The DHCPv6 client requests a prefix from the DHCPv6 server. The DHCPv6 server allocates a prefix to the DHCPv6 client and then the DHCPv6 client configures IPv6 addresses by using this prefix.
Relay Service	The DHCPv6 relay is used to enable communication between the DHCPv6 client and DHCPv6 server on different links.

1.2.1 Requesting/Allocating Addresses and Configuration Parameters

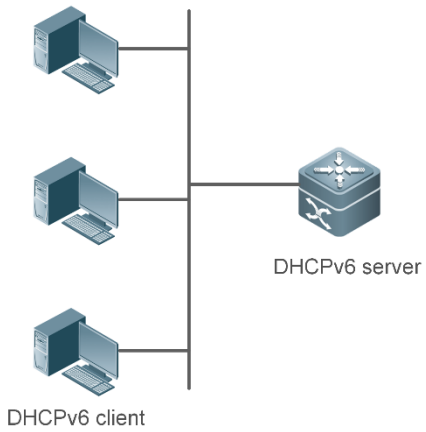
Scenario

On a subnet, a DHCPv6 client requests addresses from a DHCPv6 server. The DHCPv6 server allocates addresses and configuration parameters to the DHCPv6 client.

In Figure 1-2:

- The DHCPv6 server is configured with IPv6 addresses, DNS servers, domain names, and other configuration parameters to be allocated.
- A host works as a DHCPv6 client to request an IPv6 address from the DHCPv6 server. After receiving the request, the DHCPv6 server selects an available address and allocates the address to the host.
- The host can also request a DNS server, a domain name, and other configuration parameters from the DHCPv6 server.

Figure 1-2



Deployment

- Run the DHCPv6 client on a host in the subnet to obtain an IPv6 address and other parameters.

- Run the DHCPv6 server on a device and configure the IPv6 address and other parameters to allocate the IPv6 address and parameters.

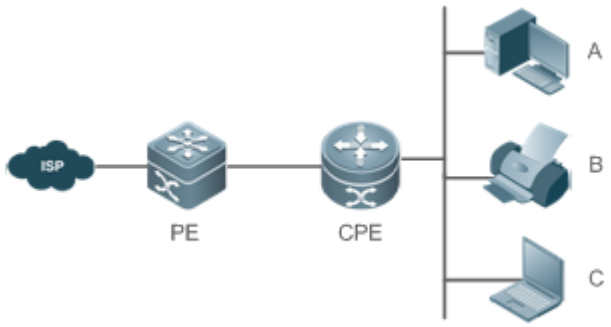
1.2.2 Requesting/Allocating Prefixes

Scenario

As shown in Figure 1-3, an uplink device (PE) allocates an IPv6 address prefix to a downlink device (CPE). The CPE generates a new address prefix for the internal subnet based on the obtained prefix. Hosts on the internal subnet of the CPE are configured with addresses through Router Advertisement (RA) messages by using the new address prefix.

- The PE used aa a DHCPv6 server provides the prefix delegation service.
- The CPE used aa a DHCPv6 client requests an address prefix from the PE. After obtaining the address prefix, the CPE generates a new address prefix for the internal subnet and sends an RA messages to hosts on the internal subnet.
- The hosts on the internal subnet where the CPE resides configure their addresses based on the RA message sent by the CPE.

Figure 1-3



Remarks	● The Provider Edge (PE) works as a DHCPv6 server for providing prefixes and is also called a delegating router. ● The Customer Premises Equipment (CPE) works as a DHCPv6 client for requesting prefixes and is also called a requesting router. ● A, B, and C are hosts.

Deployment

- Run the DHCPv6 server on the PE to implement the prefix delegation service.
- Run the DHCPv6 client on the CPE to obtain address prefixes.
- Deploy IPv6 ND between the CPE and the hosts to configure the host addresses on the subnet through RA messages.

1.2.3 Relay Service

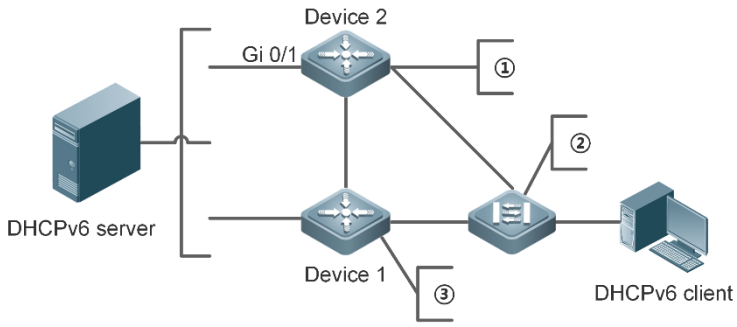
Scenario

The DHCPv6 relay agent provides the relay service for the DHCPv6 client ad DHCPv6 server on different links to enable communication between them.

In Figure 1-4:

- Device 1 is enabled with the DHCPv6 relay agent and destined to 3001::2.
- Device 2 wants to forward messages to other servers through a next-level relay service. Enable the DHCPv6 relay agent on Device 2, set the destination address to FF02::1:2 (all servers and relay multicast addresses), and specify the egress interface as the Layer 3 interface gi 0/1.

Figure 1-4



①Layer 3 gateway enabled with the DHCPv6 relay agent

②Layer 2 access device enabled with LDRA

③Layer 3 gateway enabled with the DHCPv6 relay agent

Deployment

- Enable the DHCPv6 relay agent on device 1 and specify the address as 3000::1.
- Enable the DHCPv6 relay agent on device 2 and specify the address as FF02::1:2.

1.3 Features

Basic Concept

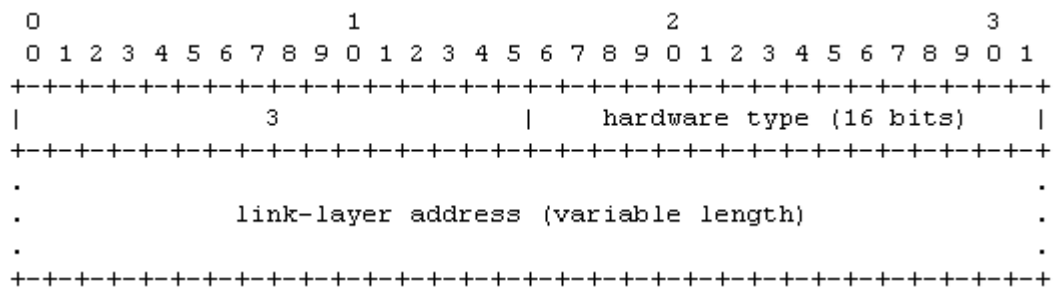
DUID

The DHCP Unique Identifier (DUID) identifies a DHCPv6 device. As defined in RFC 3315, each DHCPv6 device (DHCPv6 client, relay, or server) must have a DUID, which is used for mutual authentication during DHCPv6 message exchange.

RFC 3315 defines three types of DUIDs:

- DUID Based on Link-Layer address plus Time (DUID-LLT)
- DUID Assigned by Vendor Based on Enterprise Number (DUID-EN)
- Link-Layer address (DUID-LL)

DHCPv6 devices use DUID-LLs. The format 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 device's MAC address respectively.

IA

A DHCPv6 server allocates Identity Associations (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). The DHCPv6 server supports only IA_NA and IA_PD.

Binding

DHCPv6 binding data on a DHCPv6 server records the IA and other configurations allocated to each 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 the DUID as the index.

DHCPv6 Conflict

When an address allocated by a DHCPv6 client is in conflict, the client sends a Decline message 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 query and clearing of address information in the address conflict queue.

Message Type

RFC 3315 stipulates that DHCPv6 uses UDP ports 546 and 547 for message exchange. In particular, a DHCPv6 client uses port 546 for receiving messages, while a DHCPv6 server and DHCPv6 relay agent use port 547 for receiving messages. RFC 3315 defines the following types of messages that can be exchanged among the DHCPv6 server, client, and relay agent:

- Messages that may be sent by a DHCPv6 client to a DHCPv6 server include Solicit, Request, Confirm, Renew, Rebind, Release, Decline, and Information-request messages.
- Messages that may be sent by a DHCPv6 server to a DHCPv6 client include Advertise, Reply, and Reconfigure messages.

- Messages that may be sent by a DHCPv6 relay agent to another DHCPv6 relay agent or a DHCPv6 server include Relay-forward messages.
- Messages that may be sent by a DHCPv6 relay agent to another DHCPv6 relay agent or a DHCPv6 server include Relay-reply messages.

The DHCPv6 server does not support the Reconfigure message.

The DHCPv6 client does not support the Confirm and Reconfigure messages.

Overview

Feature	Description
Requesting or Allocating Addresses	Dynamically obtains or allocates IPv6 addresses on a network in the client/server model.
Requesting or Allocating Prefixes	Dynamically obtains or allocates IPv6 prefixes on a network in the client/server model.
Stateless Service	Provides stateless configuration service for hosts on a network.
Relay Service	Provides the DHCPv6 server service for hosts on different networks by using the relay service.

1.3.1 Requesting or Allocating Addresses

A DHCPv6 client can request an IPv6 address from a DHCPv6 server.

After being configured with available addresses, a DHCPv6 server can provide IPv6 addresses to hosts on a network, record allocated addresses and improve the network manageability.

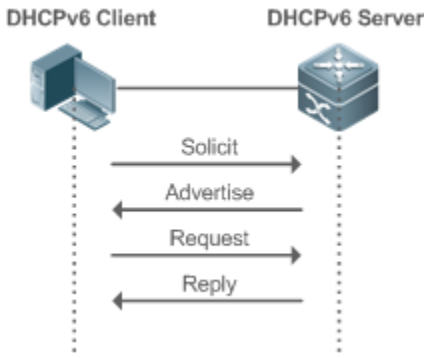
Working Principle

Network hosts serve as DHCPv6 clients to communicate with the DHCPv6 server to implement address allocation, update, confirmation, release, and other operations through message exchange.

Four-Message Exchange

Figure 1-5 shows the four-message exchange process.

Figure 1-5



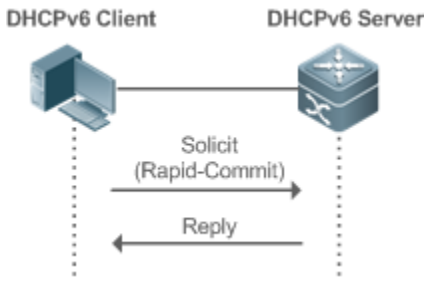
- A DHCPv6 client sends a Solicit message whose destination address is FF02::1:2 and destination port number is 547 within the local link to request address, prefix, and configuration parameter allocation. All DHCPv6 servers or DHCPv6 relay agents within the link will receive the Solicit message.

- 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 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 1-6

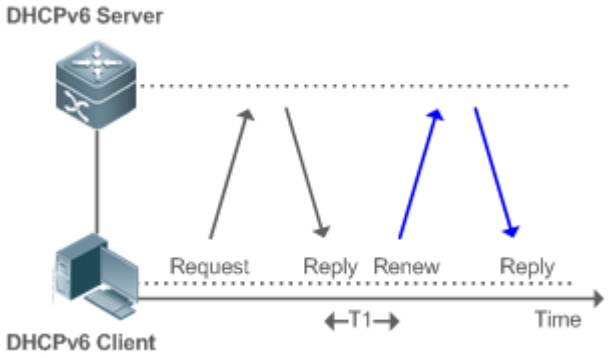


- A DHCPv6 client sends a Solicit message whose destination address is FF02::1:2 and destination port number is 547 within the local link to request address, prefix, and configuration parameter allocation. The Solicit message contains Rapid Commit.
- If a DHCPv6 server supports the Rapid Commit option, the DHCPv6 server creates a binding locally and sends a Reply message in 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

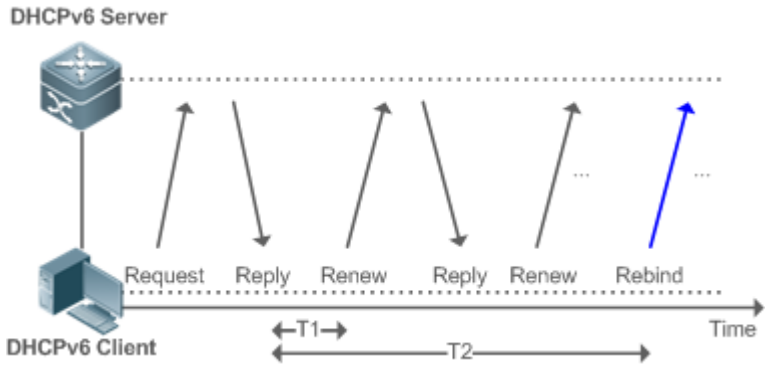
The DHCPv6 server provides the control address and the updated T1 and T2 in the IA of the message sent to the DHCPv6 client.

Figure 1-7



- The DHCPv6 client will multicast a Renew 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 so, the DHCPv6 server updates the local binding and sends a Reply message in unicast mode. The Reply message contains the new T1 and other parameters.

Figure 1-8



- If no response is received after the DHCPv6 client sends a Renew message to the DHCPv6 server, the DHCPv6 client will multicast a Rebind 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 1-9



- 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 1-10

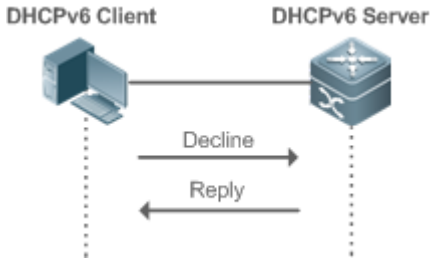


- After receiving the Confirm message, the DHCPv6 server performs confirmation based on the address information in the Confirm message, and sends a Reply message carrying the state option to the DHCPv6 client. If the confirmation fails, the DHCPv6 client may initiate a new address allocation request.

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 1-11



- The DHCPv6 client adds IA information of the conflicted addresses to 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 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 an address pool.
- You can run the **iana-address** command to configure addresses to be allocated and values of **preferred lifetime** and **valid lifetime**.

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 or Allocating Prefixes

Configure available prefixes on the DHCPv6 server. By using prefix delegation of DHCPv6, uplink network devices can allocate address prefixes to downlink network devices, which implements flexible station-level automatic configuration and 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- or 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 prefix delegation, see Requesting or 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 the DHCPv6 server function for the interface.

The DHCPv6 server function is effective only on a layer-3 interface.

Configuring 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 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

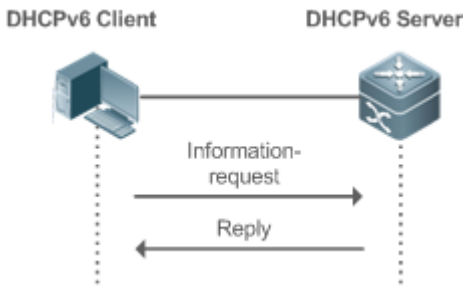
When a DHCPv6 client needs only configuration parameters, the DHCPv6 stateless service can be used to obtain related configuration parameters which cannot be obtained through a stateless automatic address configuration protocol, such as the DNS server address.

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 1-12



- 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 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 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.

1.3.4 Relay Service

When the DHCPv6 client and DHCPv6 server are on different links, the DHCPv6 client can relay related messages to the DHCPv6 server through the DHCPv6 relay agent. The DHCPv6 server also relays the response to the DHCPv6 client through the relay agent.

Working Principle

When receiving a message from the DHCPv6 client, the DHCPv6 relay agent creates a Relay-forward message. This message contains the original message from the DHCPv6 client and some options added by the relay agent. Then the relay agent sends the Relay-forward message to a specified DHCPv6 server or a specified multicast address FF05::1:3.

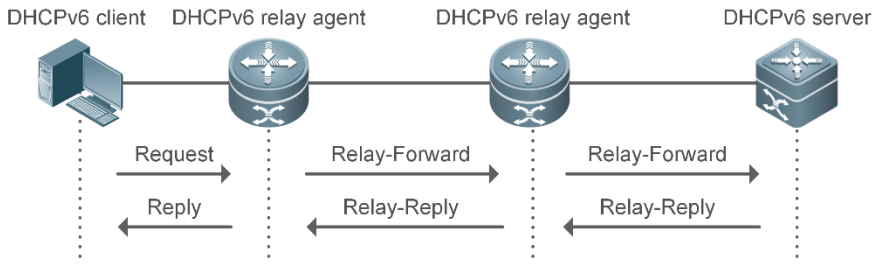
After receiving the Relay-forward message, the DHCPv6 server extracts the original message from the DHCPv6 client for processing. Then the DHCPv6 server constructs a response to the original message, encapsulates the response in a Relay-reply message, and then sends the Relay-reply message to the DHCPv6 relay agent.

After receiving the Relay-reply message, the DHCPv6 relay agent extracts the original message from the DHCPv6 server for processing, and forwards the message to the DHCPv6 client.

Multi-level relay agents are allowed between the DHCPv6 client and DHCPv6 server.

DHCPv6 Relay Agent

Figure 1-13



- The DHCPv6 relay agent performs message encapsulation and decapsulation between the DHCPv6 client and DHCPv6 server to enable communication between the DHCPv6 client and DHCPv6 server on different links.

1.4 Configuration

Configuration	Description and Command	
Configuring the DHCPv6 Server	(Mandatory) It is used to create a DHCPv6 server configuratio pool.	
	ipv6 dhcp pool	Configures an address pool for the 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.
	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	Configures excluded addresses on the DHCPv6 server.
	(Mandatory) It is used to enable the DHCPv6 server.	
	ipv6 dhcp server	Enables the DHCPv6 server on an interface.
Configuring the DHCPv6 Relay	(Mandatory) It is used to enable the DHCPv6 relay agent.	
	ipv6 dhcp relay destination	Configures the DHCPv6 relay agent.
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, you must specify an address pool.
- Do not use the long name of the address pool.
- When enabling the DHCPv6 server, you must specify a pool.
- Only the Switch Virtual Interface (SVI), routed interface, and Layer 3 aggregate interface support this configuration.

Configuration Step

Configuring a DHCPv6 Server Pool

- Mandatory.
- Unless otherwise specified, you should configure a pool on all devices that need to provide the DHCPv6 server.

Configuring Address Prefixes to Be Allocated on the DHCPv6 Server

- Optional.
- To provide the address allocation service, configure address prefixes to be allocated on all devices that need to provide the DHCPv6 server.

Configuring Prefixes of Static Addresses on the DHCPv6 Server

- Optional.
- To provide the prefix delegation service for statically bound addresses, configure prefixes of statically bound addresses on all devices that need to provide the DHCPv6 server.

Configuring the DHCPv6 Server to Allocate Prefixes from a Local Prefix Pool

- Optional.
- To provide the prefix delegation service, specify a local prefix pool on all devices that need to provide the DHCPv6 server.

Configuring a Local IPv6 Prefix Pool

- Optional.
- To provide the prefix delegation service through a prefix pool, specify a local prefix pool on all devices that need to provide the DHCPv6 server.

Configuring the DNS Server on the DHCPv6 Server

- Optional.
- To allocate DNS servers, configure the DNS server on all devices that need to provide the DHCPv6 server.

Configuring Domain Names on the DHCPv6 Server

- Optional.
- To allocate domain names, configure domain names on all devices that need to provide the DHCPv6 server.

Configuring the IPv6 Address of the CAPWAP AC on the DHCPv6 Server

- Optional.
- To allocate CAPWAP AC information, configure the IPv6 address of the CAPWAP AC on all devices that need to provide the DHCPv6 server.

Enabling the DHCPv6 Server

- Mandatory.
- Unless otherwise specified, you should enable the DHCPv6 server on specific interfaces of all devices that need to provide the DHCPv6 server.

Verification

The DHCPv6 server allocates addresses, prefixes, or configuration parameters to DHCPv6 clients.

- The DHCPv6 client obtains 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 pool. After configuring this command, you enter the DHCPv6 pool configuration mode, in which you can configure pool parameters such as the prefix and DNS server. After creating a DHCPv6 server pool, you can run the **ipv6 dhcp server** command to associate the pool with the DHCPv6 server on an interface.

Configuring Prefixes of Statically Bound Addresses on the DHCPv6 Server

Command	**prefix-delegation** *ipv6-prefix/prefix-length client-DUID*[**lifetime** { *valid-lifetime* | *preferred-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 valid time of the prefix allocated to a client. This keyword must be configured 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	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 so, 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*
Parameter Description	*poolname*: Indicates the name of a user-defined local prefix pool.
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. Then 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 multiple CAPWAP ACs. A new CAPWAP AC IPv6 address will not overwrite old IPv6 addresses.

Enabling the DHCPv6 Server

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. The value range is 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 server 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 cannot be configured on an interface simultaneously.

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 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 long.
- The number of pools exceeds the limit (256).
- The configuration is not performed on the SVI, routed interface, or Layer 3 aggregate interface.
- The number of interfaces configured with the DHCPv6 server exceeds the 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 limit (20).
- When prefixes of statically bound addresses are configured, the specified DUIDs are 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 than that of **preferred lifetime**.
- The number of DNS servers exceeds the limit (10).
- The number of domain names exceeds the limit (10).
- The number of Option 52 addresses exceeds the limit (10).

1.4.2 Configuring the DHCPv6 Relay Agent

Configuration Effect

- A DHCPv6 relay agent can be configured to implement communication between the DHCPv6 client and server on different links for address allocation, prefix delegation, and parameter allocation.

Notes

- A destination address must be specified. If the destination address is a multicast address (such as FF05::1:3), you also need to specify an egress interface.

Configuration Step

Configuring the DHCPv6 Relay Agent

- Mandatory.
- Unless otherwise specified, you should configure the DHCPv6 relay agent on all devices that need to provide the DHCPv6 relay agent.

Verification

- The DHCPv6 client and DHCPv6 server exchange messages through the relay agent.
- Check whether the interface is enabled with the DHCPv6 relay agent.
- Check whether the DHCPv6 relay agent can receive and send messages.

Related Commands

Configuring the DHCPv6 Relay Agent

Command	**ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]
Parameter Description	*ipv6-address*: Specifies the destination address of the relay agent. *interface-type*: Specifies the type of the destination interface (optional). *interface-number*: Specifies the number of the destination interface (optional).
Command Mode	Interface configuration mode
Usage Guide	All DHCPv6 messages from clients received by an interface enabled with the DHCPv6 relay agent will be encapsulated and sent to a specified destination address (or multiple destination addresses) through a specified interface (optional).

Configuration Example

Configuring the DHCPv6 Relay Agent

Configuration Steps	● Specify an interface enabled with the relay agent to forward received DHCPv6 client messages to a specified destination address through the specified interface (optional).

	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#interface vlan 1`
	`Hostname(config-if)#ipv6 dhcp relay destination 3001::2`
	`Hostname(config-if)#ipv6 dhcp relay destination ff02::1:2 vlan 2`

Verification	● Run the **show ipv6 dhcp relay destination all** command to display the configured destination addresses.

	Interface:VLAN 1 Destination address(es) Output Interface 3001::2 ff02::1:2 VLAN 2

Common Errors

- The configuration is not performed on the SVI, routed interface, or Layer 3 aggregate interface.

1.4.3 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 function 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 an 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 the 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 RA messages.

	`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 check 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 agent 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 agent or DHCPV6 server.

1.5 Monitoring

Clearing

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

Command	Description
clear ipv6 dhcp binding [*ipv6-address*]	Clears DHCPv6 bindings.
clear ipv6 dhcp server statistics	Clears DHCPv6 server statistics.
clear ipv6 dhcp conflict { *ipv6-address* | * }	Clears conflicted addresses on the DHCPv6 server.
clear ipv6 dhcp relay statistics	Clears statistics on sent and received messages after the DHCPv6 relay agent is enabled on the device.
clear ipv6 dhcp client *interface-type interface-number*	Restarts the DHCPv6 client.

Displaying

Command	Description
show ipv6 dhcp	Displays the DUID of a device.
show ipv6 dhcp binding [*ipv6-address*]	Displays address bindings on the DHCPv6 server.
show ipv6 dhcp interface [*interface-name*]	Displays the DHCPv6 interface.
show ipv6 dhcp pool [*poolname*]	Displays the DHCPv6 pool.
show ipv6 dhcp conflict	Displays conflicted DHCPv6 addresses.
show ipv6 dhcp server statistics	Displays statistics on the DHCPv6 server.
show ipv6 dhcp relay destination { **all** | *interface-type interface-number* }	Displays the destination address of the DHCPv6 relay agent.
show ipv6 dhcp relay statistics	Displays the statistics on sent and received messages after the DHCPv6 relay is enabled on a device.
show ipv6 local pool [*poolname*]	Displays the local IPv6 prefix pool.

Debugging



Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug ipv6 dhcp [**detail**]	Debugs DHCPv6.

1 Configuring DHCPv6 Snooping

1.1 Overview

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) snooping records and monitors the user IP address usage by intercepting DHCPv6 packets between a DHCPv6 server and the DHCPv6 clients. It can also filter invalid DHCPv6 packets, including DHCPv6 request packets from the clients and DHCPv6 response packets from the server. The user data entries generated by DHCPv6 snooping can be used by security applications such as IPv6 source guard.

The following section describes DHCPv6 snooping.

Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol for IPv6
- RFC 5007: DHCPv6 Leasequery
- RFC 5460: DHCPv6 Bulk Leasequery

1.2 Applications

Application	Description
Defense Against DHCPv6 Spoofing Attacks	Allows DHCPv6 clients to obtain network configuration parameters only from the valid DHCPv6 server when multiple DHCPv6 servers exist on the network.
Defense Against Bogus DHCPv6 Packet Attacks	Defends against malicious users who send bogus DHCPv6 request packets, such as DHCPv6-Release packets.
Defense Against IPv6/MAC Spoofing Attacks	Defends against malicious users who send bogus IPv6 packets, for example, with the source address field tampered.
Defense Against Untrusted IPv6 Addresses	Detects network users who use untrusted IPv6 addresses, instead of the IPv6 addresses obtained from the DHCPv6 server.

1.2.1 Defense Against DHCPv6 Spoofing Attacks

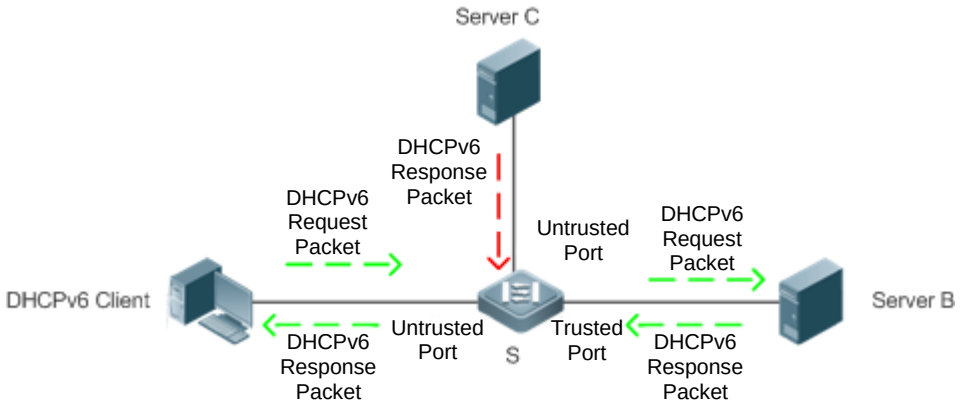
Scenario

Multiple DHCPv6 servers may exist on the network. User PCs can obtain network configuration parameters only from DHCPv6 servers within the specified range.

As shown in the following figure, the DHCPv6 client can communicate with only the trusted DHCPv6 server.

- The request packets of the DHCPv6 client can be transmitted only to the trusted DHCPv6 server.
- Only the response packets of the trusted DHCPv6 server can be transmitted to the DHCPv6 client.

Figure 1-1



Notes	S is the access device. DHCPv6 Client is a user PC. Server B is a trusted DHCPv6 server. Server C is an untrusted DHCPv6 server.

Deployment

- Enable DHCPv6 snooping on the access device S to monitor DHCPv6 packets.
- Configure the port connecting the access device S to DHCPv6 Server B as a DHCPv6 trusted port to forward response packets.
- Configure other ports of the access device S as DHCPv6 untrusted ports to filter response packets.

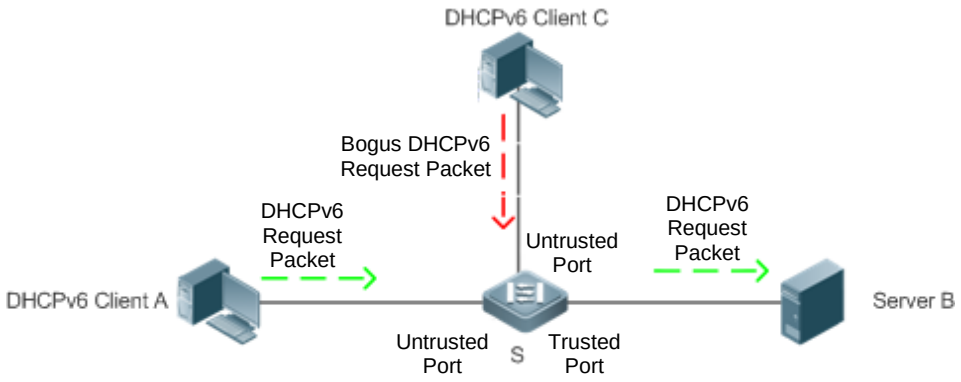
1.2.2 Defense Against Bogus DHCPv6 Packet Attacks

Scenario

Malicious users may exist on the network and they send bogus DHCPv6 request packets. These packets consume available IPv6 addresses of DHCPv6 servers and preempt IPv6 addresses of valid users. Therefore, invalid DHCPv6 packets on the access network must be filtered.

As shown in the following figure, the access device checks DHCPv6 request packets sent by DHCPv6 clients. The Release and Decline packets of the clients can be forwarded only if they match the records in the internal snooping database.

Figure 1-2



Notes	S is the access device. A and C are user PCs. B is a DHCPv6 server within the specified range.

Deployment

- Enable DHCPv6 snooping on the access device S to monitor DHCPv6 packets.
- Configure the port connecting the access device S to DHCPv6 Server B as a DHCPv6 trusted port to forward response packets.
- Configure other ports of the access device S as DHCPv6 untrusted ports to filter DHCPv6 packets.

1.2.3 Defense Against IPv6/MAC Spoofing Attacks

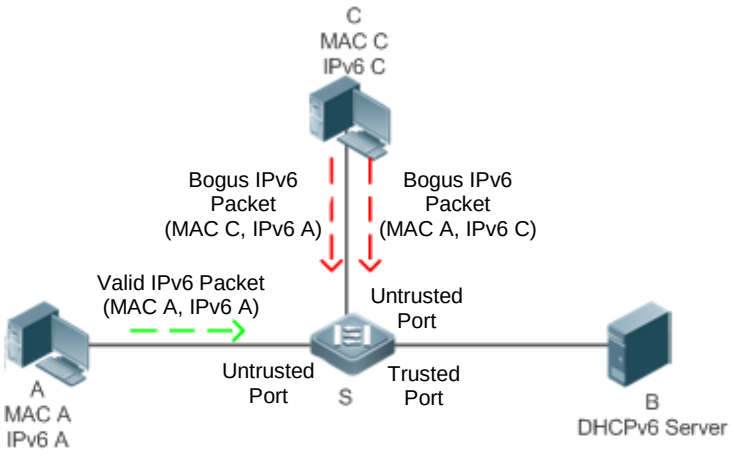
Scenario

When the access device checks IPv6 packets from untrusted ports to filter bogus IPv6 packets, it can check only the IP field or both the IP and MAC fields.

As shown in the following figure, the access device checks IPv6 packets sent by DHCPv6 clients.

- The source address field in an IPv6 packet must be the same as the IPv6 address allocated by the DHCPv6 server.
- The source MAC address of a Layer 2 packet must be the same as the user MAC address in the DHCPv6 request packet of the client.

Figure 1-3



Notes	S is the access device. A and C are user PCs. B is a DHCPv6 server within the specified range.

Deployment

- Enable DHCPv6 snooping on the access device S to monitor DHCPv6 packets.
- Configure all the downlink ports of the access device S as DHCPv6 untrusted ports.
- Enable IPv6 source guard on the access device S to filter IPv6 packets.
- Set the matching mode of IPv6 source guard on the access device S to IPv6+MAC to check both the MAC and IPv6 fields of IPv6 packets.

1.2.4 Defense Against Untrusted IPv6 Addresses

Scenario

The access device checks whether the source IPv6 addresses of IPv6 packets from untrusted ports are the same as those allocated by the DHCPv6 server.

If the source IPv6 address, port number, or Layer 2 source MAC address of an IPv6 packet does not match the record allocated by the DHCPv6 server to which the access device connects, the access device discards the IPv6 packet.

The operating process of the access device in this scenario is the same as that in the previous section.

Deployment

Same as those in the "Defense Against IPv6/MAC Spoofing Attacks" section.

1.3 Features

Basic Concepts

DHCPv6 Request Packets

DHCPv6 request packets are sent by DHCPv6 clients to the DHCPv6 server, including the following types:

- DHCPv6-Solicit: Detects available DHCPv6 servers.
- DHCPv6-Request: Requests the IP address or other configuration information.
- DHCPv6-Confirm: Confirms whether the obtained IP address is still valid.
- DHCPv6-Rebind: Rebinds an IP address when the client fails to communicate with the previous server.
- DHCPv6-Release: Releases the currently released IP address.
- DHCPv6-Decline: Rejects the IP address allocated by the server.
- DHCPv6-Renew: Requests to renew the currently allocated IP address.
- DHCPv6-Inform_Req: Requests extra configuration information, not involving IP address allocation.
- DHCPv6-Leasequery: Queries the lease information of clients.

DHCPv6 Response Packet

DHCPv6 response packets are sent by DHCPv6 servers to DHCPv6 clients to respond to requests from the clients. The packet types are the same as those of DHCPv6 request packets.

DHCPv6 Snooping Trust Port

DHCPv6 exchange packets for obtaining the IPv6 address or prefix are broadcast. Therefore, if an invalid DHCPv6 server exists on the network, users may fail to obtain IPv6 addresses or user information may be stolen through the invalid DHCPv6 server. To prevent this problem, DHCPv6 snooping divides ports into trusted ports and untrusted ports. A device forwards only DHCPv6 packets from the trusted ports and discards DHCPv6 packets from all the untrusted ports. This ensures that only response packets from valid DHCPv6 servers can be forwarded to clients, preventing impact of invalid DHCPv6 servers on clients.

- On a switch, all the switch ports and Layer 2 aggregate ports are untrusted ports by default, and you can specify a designated port as the trusted port.
- On an Access Point (AP), all the WLAN ports are untrusted ports, and you cannot specify a designated port as the trusted port.
- When an AP works in FAT mode, all the Layer 2 switch ports and Layer 2 encapsulation sub-interfaces are untrusted ports by default, and you can specify a designated port as the trusted port.
- When an AP works in FIT mode, all the Layer 2 switch ports are untrusted ports by default, and you can specify a designated port as the trusted port. All the Layer 2 encapsulation sub-interfaces are trusted ports, and you cannot specify a designated port as the untrusted port.

- On an Access Controller (AC), all the WLAN ports are untrusted ports, and you cannot specify a designated port as the trusted port. All the switch ports and Layer 2 aggregate ports are untrusted ports by default, and you can specify a designated port as the trusted port.

DHCPv6 Snooping Request Packet Filtering

If DHCPv6 packets are prohibited for a specific user, all the DHCPv6 packets sent by the user device must be masked. The DHCPv6 request packet filtering feature can be configured on an untrusted port to filter all the DHCPv6 request packets received by this port.

VLAN-based DHCPv6 Snooping

The DHCPv6 snooping feature is applied to VLANs. By default, if DHCPv6 snooping is enabled on a device, this feature takes effect in all the VLANs of the device. You can enable or disable DHCPv6 snooping in a specific VLAN to implement refined management.

DHCPv6 Snooping User Database

It is common that users on the DHCPv6 network randomly configure static IPv6 addresses. This increases the network maintenance difficulty and may lead to network access failures of users who obtain IPv6 addresses from valid DHCPv6 servers due to address conflicts. To resolve this problem, the DHCPv6 snooping feature monitors packets exchanged between clients and servers to collect the IPv6 addresses obtained by users as well as the MAC address, VLAN ID, port, and lease time of users. The information is integrated into user data entries to build the DHCPv6 snooping user database. In this way, DHCPv6 snooping can effectively control valid IPv6 address usage by users to ensure network stability and security.

DHCPv6 Options 18 and 37

The network administrator wants to allocate IP addresses based on the information of connected network devices when managing IP addresses. To achieve this purpose, when a network device performs DHCPv6 snooping, it adds device information of users to DHCP request packets in DHCPv6 Option fields.

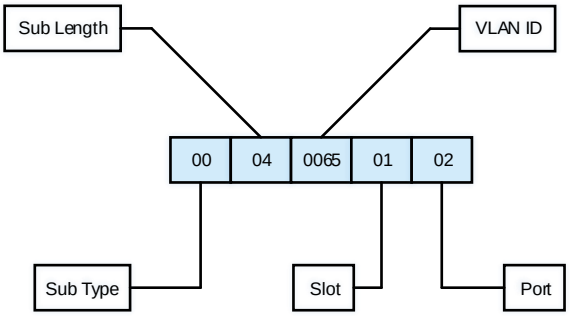
- RFC 3315 defines the DHCPv6 protocol, which uses Option 18 to carry the user device information.
- RFC 4649 defines the DHCPv6 Relay Agent options, among which Option 37 carries the user device information.

Option 18: Interface ID

- Default content: VLAN ID of the port that receives request packets from DHCPv6 clients and the port index. (The value of the port index is the combination of the slot ID and port number.) For wireless access, all the fields are set to 0.
- Extended content: custom strings, applicable to wired interfaces (such as switch ports, Layer 2 aggregate ports, and Layer 2 encapsulation sub-interfaces).
- Applicable scope: The default and custom content is applicable to wired interfaces, such as switch ports, Layer 2 aggregate ports, and Layer 2 encapsulation sub-interfaces.

Two formats are available for filling the **Interface ID** field: standard format and extended format. Only one format can be used on a network. When the standard format is used, only the default content can be filled into sub-options of the **Interface ID** field, as shown in the following figure.

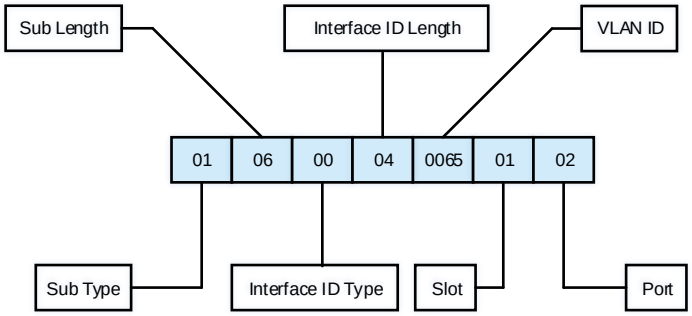
Figure 1-4



If custom content is required, use the extended format. In extended format, both custom content and extended content can be filled in. To distinguish the content, the one-byte **Interface ID Type** field and the one-byte **Interface ID Length** field are added next to the **Sub Length** field. For the **Interface ID Type** field, the value 0 indicates default content and the value 1 indicates extended content.

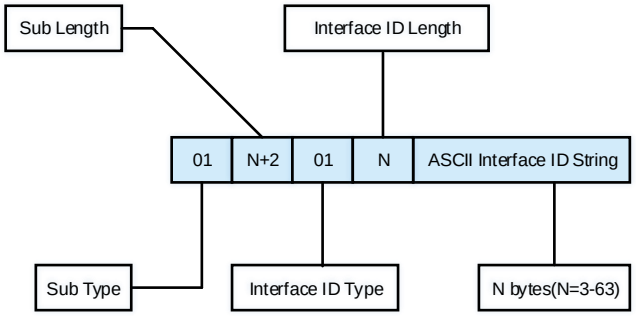
Format of Filling Default Content

Figure 1-5



Format of Filling Extended Content

Figure 1-6

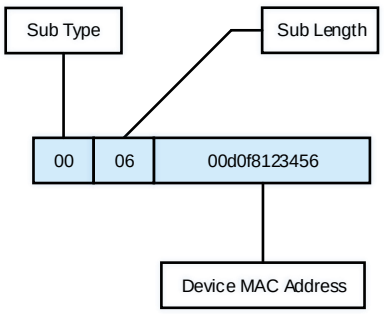


Option 37: Remote ID

- Default content: bridge MAC address of the DHCPv6 relay that receives DHCPv6 clients' request packets
- Extended content: custom strings

Two formats are available for filling the **Remote ID** field: standard format and extended format. Only one format can be used on a network. When the standard format is used, only the default content can be filled into sub-options of the **Remote ID** field, as shown in the following figure.

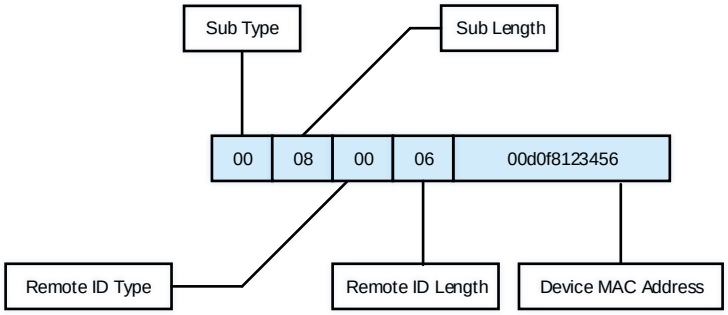
Figure 1-7



If custom content is required, use the extended format. In extended format, both custom content and extended content can be filled in. To distinguish the content, the one-byte **Remote ID Type** field and the one-byte **Remote ID Length** field are added next to the **Sub Length** field. If the **Remote ID Type** field is set to 0, default content is filled. If the **Remote ID Type** field is set to 1, extended content is filled.

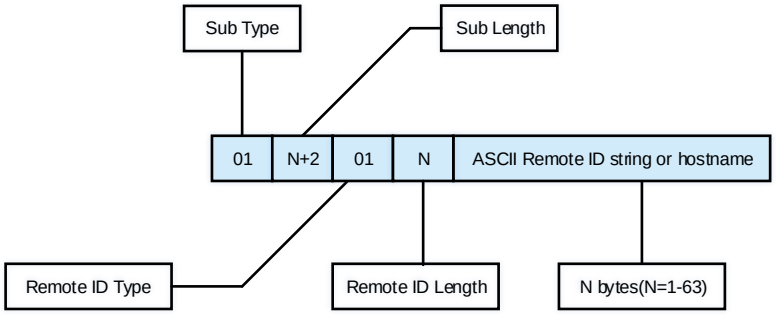
Format of Filling Default Content

Figure 1-8



Format of Filling Extended Content

Figure 1-9



Notes:

Option 18: the **Interface ID** field, the port index is the combination of the slot ID and the port number. The port type can be wired interfaces, such as switch ports, Layer 2 aggregate ports, and Layer 2 encapsulation sub-interfaces. The port number indicates the sequence of the port in a slot. For Layer 2 aggregate ports, the port number is the aggregate port ID. For example, the port number of Fa0/10 is 10, the port number of AP 11 is 11, and the port number of WLAN 1 is 1.

The slot ID indicates the sequence of the slot in a device. A stacking device is numbered as a single device. The slot ID starts from 0, and an aggregate port locates in the last slot. You can run the **show slots** command to view the slot ID.

Example 1:

```
Ruijie#show slots (Only the information of the Dev and Slot columns is displayed.)
  Dev Slot
  --- ----
  1   0    ------>The slot ID is 0.
  1   1    ------>The slot ID is 1.
  1   2    ------>The slot ID is 2.
```

The slot ID of the aggregate port is 3.

Example 2:

```
Ruijie#show slots (Only the information of the Dev and Slot columns is displayed.)
  Dev Slot
  --- ----
  1   0    ------>The slot ID is 0.
  1   1    ------>The slot ID is 1.
  1   2    ------>The slot ID is 2.
  2   0    ------>The slot ID is 3.
  2   1    ------>The slot ID is 4.
  2   2    ------>The slot ID is 5.
```

The slot ID of the aggregate port is 6.

Invalid DHCPv6 Packet

DHCPv6 snooping checks the validity of DHCPv6 packets passing through the device, discards invalid DHCPv6 packets, records user information, and generates a DHCPv6 snooping binding database for query by other features. The following types of packets are regarded as invalid DHCPv6 packets:

- DHCPv6 response packets received by untrusted ports. For details, see "DHCPv6 Response Packets" in the "Basic Concepts" section.
- DHCPv6 packets received by untrusted ports that pass through the DHCPv6 relay, including the DHCPv6-Relay-Forw and DHCPv6-Relay-Reply packets.
- DHCPv6-Relay-Reply packets received by trusted ports, whose outbound interfaces are untrusted ports in the corresponding table.

- DHCPv6-Release packets, for which no user is found in the DHCPv6 snooping user database based on the Layer 2 source MAC address and VID.
- DHCPv6-Release packets whose IPv6 addresses or prefixes do not exist in the DHCPv6 snooping user database.
- DHCPv6-Release packets whose IPv6 addresses or prefixes exist in the DHCPv6 snooping user database, but the untrusted ports receiving these packets different from those stored in the DHCPv6 snooping user database.
- DHCPv6 packets of incorrect format or incomplete packets.

Overview

Feature	Description
Invalid DHCPv6 Packet Filtering	Checks the validity of exchanged DHCPv6 packets, discards invalid packets, and forwards only valid request packets to trusted ports.
User Database Establishment	Monitors packets exchanged between DHCPv6 clients and DHCPv6 servers and generates a DHCPv6 snooping user database to provide basis for other security modules to filter packets.

1.3.1 Invalid DHCPv6 Packet Filtering

This feature checks the validity of DHCPv6 packets from untrusted ports and filters invalid packets. This feature also controls the transmission range of DHCPv6 packets to prevent spoofing by malicious users.

Working Principle

During the monitoring process, the device checks the ports receiving packets and the fields in the packets to filter packets. The device also modifies the destination ports of packets to control the transmission range of DHCPv6 packets.

↘ Checking the Port

After receiving a DHCPv6 packet, the device checks whether the port receiving the DHCPv6 packet is a trusted port. If yes, the device directly forwards the packet without checking its validity or generating a binding or prefix record. If no, the device checks the packet validity.

↘ Checking Packet Encapsulation and Integrity

The device checks whether the packet is a UDP packet and whether the destination port is 546 or 547. The device checks whether the actual length of the packet is the same as that of the **Length** field defined in the protocol.

↘ Checking the Packet Type and Fields in the DHCPv6 Packet

The device checks whether the packet passes through a relay based on the description of invalid packet types in the "Basic Concepts" section. Then, the device checks whether the packet type meets the restriction conditions specific for this type.

1.3.2 User Database Establishment

The device monitors packets exchanged between DHCPv6 clients and DHCPv6 servers and generates DHCPv6 snooping binding entries and prefix entries based on the valid DHCPv6 packet information. All these entries are provided to other security

modules of the device as a valid user information table for filtering network packets. After the DHCPv6 snooping feature is enabled, the device automatically creates and updates user data.

Working Principle

During the monitoring process, the device continuously updates the binding database and prefix database based on the DHCPv6 packet type.

Generating a Binding or Prefix Record

When the device detects a DHCPv6-Reply packet from a trusted port, it extracts the client IPv6 address or prefix, client MAC address, and lease time from the packet. After that, the device generates a binding or prefix record based on the client's port ID (wired interface index or wireless WLAN ID) and the VLAN that the client resides recorded by the device.

Deleting the Binding or Prefix Record

When the recorded lease time expires, a client sends a valid DHCPv6-Release or DHCPv6-Decline packet, or the user proactively deletes a binding or prefix record by running the **clear** command, the corresponding binding or prefix record is deleted.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic DHCPv6 Snooping Features	⚠ (Mandatory) It is used to enable the DHCPv6 snooping service.	
	ipv6 dhcp snooping	Enables the DHCPv6 snooping feature.
	⚠ (Optional)	
	ipv6 dhcp snooping vlan	Configures the DHCPv6 snooping feature in the specified VLANs.
	ipv6 dhcp snooping database write-delay	Enables periodic saving of DHCPv6 snooping binding and prefix records.
	ipv6 dhcp snooping database write-to-flash	Manually saves DHCPv6 snooping binding and prefix records.
	renew ipv6 dhcp snooping database	Manually imports user records stored in the flash file into the DHCPv6 snooping user database.
	ipv6 dhcp snooping trust	Configures a DHCPv6 snooping trusted port.
	ipv6 dhcp snooping link-detection	Deletes dynamic binding entries from the port in Link Down state.
Configuring DHCPv6 Option 18 or 37	⚠ (Optional) It is used to optimize DHCPv6 server address allocation.	
	ipv6 dhcp snooping Information option [**standard-format**]	Adds Option 18 or 37 to DHCPv6 request packets.

	ipv6 dhcp snooping information option format remote-id	Configures the remote ID in extended format.
	ipv6 dhcp snooping vlan information option format-type interface-id string	Configures a custom string for the interface ID in extended format.
	ipv6 dhcp snooping vlan information option change-vlan-to vlan	Configures VLAN mapping for the interface ID in extended format.

1.4.1 Configuring Basic DHCPv6 Snooping Features

Configuration Effect

- Enable the DHCPv6 snooping service.
- Generate DHCPv6 snooping binding and prefix databases.
- Control the transmission range of DHCPv6 packets.
- Filter invalid DHCPv6 packets.

Notes

- The port connecting the device to a trusted DHCPv6 server must be set as a trusted port.
- The port on which DHCPv6 snooping takes effect can be a switch port, Layer 2 aggregate port, Layer 2 encapsulation sub-interface, or wireless WLAN port. You can configure the port in interface mode or wireless security mode.
- Entry deletion upon port Link Down takes effect only on wired interfaces.

Configuration Steps

↘ Enabling the DHCPv6 Snooping Service Globally

- Mandatory.
- This feature is enabled on the access device, unless otherwise specified.

↘ Configures the DHCPv6 snooping feature in the specified VLANs.

- The DHCPv6 snooping feature is disabled in some VLANs.
- This feature is enabled on the access device, unless otherwise specified.

↘ Configuring a DHCPv6 Trusted Port

- Mandatory.
- The port connecting the device to a trusted DHCPv6 server is set as a trusted port.

↘ Deleting Dynamic Binding Entries from the Port in Link Down State

- This feature can be enabled to reduce hardware entry usage over stable network connections and delete entries from the port in Link Down state in time.
- This feature is enabled on the access device, unless otherwise specified.

Related Commands

Configuring Basic DHCPv6 Snooping Features

Command	**ipv6 dhcp snooping**
Parameter Description	N/A
Defaults	This feature is disabled.
Command Mode	Global configuration mode
Usage Guide	After DHCPv6 snooping is enabled globally, run the **show ipv6 dhcp snooping** command to check whether the DHCPv6 snooping feature is enabled.

Configuring the DHCPv6 Snooping Feature in the Specified VLANs

Command	**ipv6 dhcp snooping vlan** { *vlan-first* [*vlan-last*] | *vlan-rang* }
Parameter Description	*vlan-first*: Indicates the start VLAN ID in which the DHCPv6 snooping feature takes effect. The value range is from 1 to 4094. *vlan-last*: Indicates the last VLAN ID in which the DHCPv6 snooping feature takes effect. The value range is from 1 to 4094. *vlan-rang*: Indicates the VLAN range in which the DHCPv6 snooping feature takes effect, such as 1, 3–5, 7, and 9–11.
Defaults	After DHCPv6 snooping is enabled globally, the DHCPv6 snooping feature takes effect in all VLANs.
Command Mode	Global configuration mode
Usage Guide	● You can run this command to enable the DHCPv6 snooping feature in the specified VLANs. You can also run the **no ipv6 dhcp snooping vlan** { *vlan-first* [*vlan-last*] | *vlan-rang* } command to disable the DHCPv6 Snooping feature in the specified VLANs or VLANs in the specified range. ● This command can be used only when the DHCPv6 snooping feature is enabled.

Periodically Writing Data from the DHCPv6 Snooping Database to the Flash File

Command	**ipv6 dhcp snooping database write-delay** delay-*seconds*
Parameter Description	*delay-seconds*: Indicates the period for writing data from the DHCPv6 snooping database to the flash file, in seconds. The value range is from 600 to 86400.
Defaults	This feature is disabled.
Command Mode	Global configuration mode
Usage Guide	● You can run this command to write data from the DHCPv6 snooping database to the flash file. If the user information is lost after device restart, users must re-obtain IP addresses to communicate with the device. ● High storage frequency reduces the lifespan of the flash memory.

Writing Data from the DHCPv6 Snooping Database to the Flash File

Command	ipv6 dhcp snooping database write-to-flash
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	You can run this command to immediately write dynamic user information from the DHCPv6 snooping database to the flash file.

Importing Data from the Current Flash File to the DHCPv6 Snooping Binding Database

Command	renew ipv6 dhcp snooping database
Parameter Description	N/A
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	● You can run this command to immediately write data from the flash file to the DHCPv6 snooping database. ● Lease expiration records in the flash file are ignored. ● Only the records unavailable in the database are imported.

Configuring a Port as the Trusted Port

Command	ipv6 dhcp snooping trust
Parameter Description	N/A
Defaults	All ports are untrusted ports.
Command Mode	Interface configuration mode
Usage Guide	● Generally, uplink ports connected to the trusted DHCPv6 servers are configured as trusted ports. ● You can run this command to configure a port connected to a valid DHCPv6 server as the trusted port. The trusted port normally forwards received DHCPv6 response packets, but an untrusted port discards received DHCPv6 response packets. ● This command immediately takes effect on a Layer 2 switch port, aggregate port, or Layer 2 encapsulation sub-interface. This command fails on other ports.

Deleting Dynamic Binding Entries from the Port in Link Down State

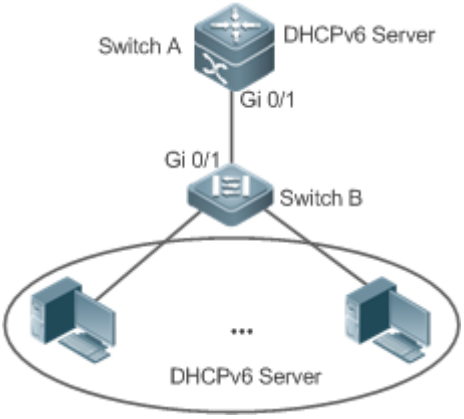
Command	ipv6 dhcp snooping link-detection
Parameter Description	N/A
Defaults	This feature is disabled.

Command Mode	Global configuration mode
Usage Guide	This feature can be enabled to reduce hardware entry usage and delete entries from the port in Link Down state in time.

Configuration Example

The following configuration examples describe only the configurations related to the DHCPv6 snooping feature.

Configuring the DHCPv6 Snooping Feature

Scenario **Figure 1-10**	
Configuration Steps	● Enable the DHCPv6 snooping feature on the access device (Switch B in this example). ● Configure the uplink port (Gi 0/1 in this example) as the trusted port.

B	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#ipv6 dhcp snooping`
	`Hostname(config)#interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)#ipv6 dhcp snooping trust`
	`Hostname(config-if-GigabitEthernet 0/1)#end`

Verification	Check whether the DHCPv6 snooping feature is enabled on Switch B and whether the uplink port is configured as the trusted port. Check whether the client can normally obtain an IPv6 address from the valid DHCPv6 server.
B	`Hostname#show ipv6 dhcp snooping`

```
DHCPv6 snooping status : ENABLE
Interface                    Trusted   Filter DHCPv6
-------------------------    -------    -------------
GigabitEthernet 0/1          YES          DISABLE
Hostname#show ipv6 dhcp snooping binding
Total number of bindings: 1
NO.   MacAddress          IPv6 Address                                  Lease(sec)
VLAN  Interface
----- -----------------  ---------------------------------------- ----------
-- ----- --------------------
1     00d0.f801.0101     2001::10                                      42368
2     GigabitEthernet 0/1
```

Common Errors

- The uplink port is not configured as the DHCPv6 trusted port.
- Another access security option is configured on the uplink port, so the port fails to be configured as the DHCPv6 trusted port.

1.4.2 Configuring DHCPv6 Option 18 or 37

Configuration Effect

- The DHCPv6 server can obtain more information to better allocate IP addresses.
- DHCPv6 options are transparent to DHCPv6 clients, which are not aware of the enabling status of this feature.

Configuration Steps

- Option 18 or 37 can be configured for optimization.
- This feature is enabled on the DHCPv6 snooping-capable access device, unless otherwise specified.

Related Commands

↘ **Adding Option 18 or 37 to DHCPv6 Request Packets**

Command	**ipv6 dhcp snooping information option** [**standard-format**]
Parameter Description	**standard-format**: Configures the standard format for filling DHCPv6 Option 18 or 37. If this keyword is not specified, the extended format is used.
Defaults	This feature is disabled.
Command Mode	Global configuration mode
Usage Guide	You can run this command to add DHCPv6 Option 18 or 37 to DHCPv6 request packets. After that, the DHCPv6 server allocates IP addresses based on the Option 18 or 37 information.

↘ **Configuring a Custom String for Option 37 (Remote ID)**

Command	**ipv6 dhcp snooping information option format remote-id** { **string** *string* | **hostname** }
Parameter Description	*string*: Indicates a custom string for Option 37 (Remote ID) in extended format. The string can be up to 63 characters. **hostname**: Configures a host name for Option 37 (Remote ID) in extended format.
Defaults	This feature is disabled.
Configuration Mode	Global configuration mode
Usage Guide	You can run this command to configure a custom string for Option 37 (Remote ID) in extended format. After that, the DHCPv6 server allocates IP addresses based on the Option 37 information.

Configuring a Custom String for Option 18 (Interface ID)

Command	**ipv6 dhcp snooping vlan** *vlan-id* **information option format-type interface-id string** *string*
Parameter Description	*vlan-id*: Indicates the VLAN to which DHCPv6 request packets belong. *string*: Indicates the custom string for filling Option 18 (Interface ID). The string can contain 3 to 36 characters.
Defaults	This feature is disabled.
Configuration Mode	Interface configuration mode
Usage Guide	You can run this command to configure a custom string for Option 18 (Interface ID) in extended format. After that, the DHCPv6 server allocates IP addresses based on the Option 18 information.

Changing the VLAN Filled in Option 18 (Interface ID) to the Specified VLAN

Command	**ipv6 dhcp snooping vlan** *vlan-id* **information option change-vlan-to vlan** *vlan-id*
Parameter Description	*vlan-id* (first): Indicates the VLAN to which DHCPv6 request packets belong. *vlan-id* (second): Indicates the VLAN to be filled in Option 18 (Interface ID).
Defaults	This feature is disabled.
Configuration Mode	Interface configuration mode
Usage Guide	You can run this command to configure a VLAN mapping for Option 18 (Interface ID) in extended format. After that, the DHCPv6 server allocates IP addresses based on the Option 18 information.

Configuration Example

Configuring DHCPv6 Option 18 or 37

Configuration Steps	Enable Option 18 or 37 on the DHCPv6 snooping-capable device and set the extended filling format.

	`Hostname# configure terminal`
	`Hostname(config)# ipv6 dhcp snooping information option`
	`Hostname(config)# end`

Verification	Check the DHCPv6 snooping configuration.
	`Hostname#show ipv6 dhcp snooping`

```
DHCPv6 snooping status : ENABLE
DHCPv6 snooping database write-delay time : 0 seconds
DHCPv6 snooping binding-delay time : 0 seconds
DHCPv6 DHCPv6 snooping option 18/37 status : ENABLE
DHCPv6 snooping link detection           : DISABLE
Interface               Trusted    Filter DHCPv6
---------------------   -------    -------------
FastEthernet0/10        YES        DISABLE
```

Common Errors

N/A

1.5 Monitoring

Clearing

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

Command	Description
clear ipv6 dhcp snooping binding [*mac* | *ipv6-address* | **interface** *interface-id* | **vlan** *vlan-id* | **wlan** *wlan-id*]	Clears dynamic user information from the DHCPv6 snooping database.
clear ipv6 dhcp snooping prefix [*mac* | *ipv6-address* | **interface** *interface-id* | **vlan** *vlan-id* | **wlan** *wlan-id*]	Clears all entries in the DHCPv6 snooping prefix database.
clear ipv6 dhcp snooping statistics	Clears the statistics on DHCPv6 packets processed by DHCPv6 snooping.

Displaying

Command	Description
show ipv6 dhcp snooping	Displays the DHCPv6 snooping configuration.
show ipv6 dhcp snooping vlan	Displays the VLANs in which DHCPv6 snooping is effective.
show ipv6 dhcp snooping binding	Displays all dynamic binding entries in the DHCPv6 snooping binding database.
show ipv6 dhcp snooping prefix	Displays all entries in the DHCPv6 snooping prefix database.
show ipv6 dhcp snooping statistics	Displays the statistics on packets processed by DHCPv6 snooping.
show ipv6 source binding	Displays all static binding entries that are added manually and all dynamic binding entries in the DHCPv6 snooping binding database.

1 Configuring ND Snooping

1.1 Overview

The Neighbor Discovery Protocol (NDP) is vulnerable to address spoofing attacks and router advertisement (RA) attacks because it lacks built-in security features. However, it is complex to enhance security by deploying an external encryption and authentication mechanism. Neighbor Discovery (ND) Snooping is used to monitor ND packets on a network to filter out invalid address spoofing packets and RA packets. It monitors IPv6 users on the network and binds detected IPv6 users to interfaces to prevent IP address spoofing, ensuring a secure and reliable IPv6 network.

The following section describes only ND snooping.

Protocols and Standards

- RFC 2464: Transmission of IPv6 Packets over Ethernet Networks
- RFC 4861: Neighbor Discovery for IP version 6 (IPv6)
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 6620: FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses

1.2 Applications

Application	Description
Stateless Address Autoconfiguration	Users use stateless address autoconfiguration (SLAAC) to assign IPv6 addresses and configure IPv6 ND snooping to improve IPv6 network security.
Stateful Address Autoconfiguration	Users use DHCPv6 to assign IPv6 addresses, enable DHCPv6 snooping, and deploy ND snooping to improve IPv6 network security.
Manual Configuration	Users manually assign IPv6 addresses and configure ND snooping to improve IPv6 network security.

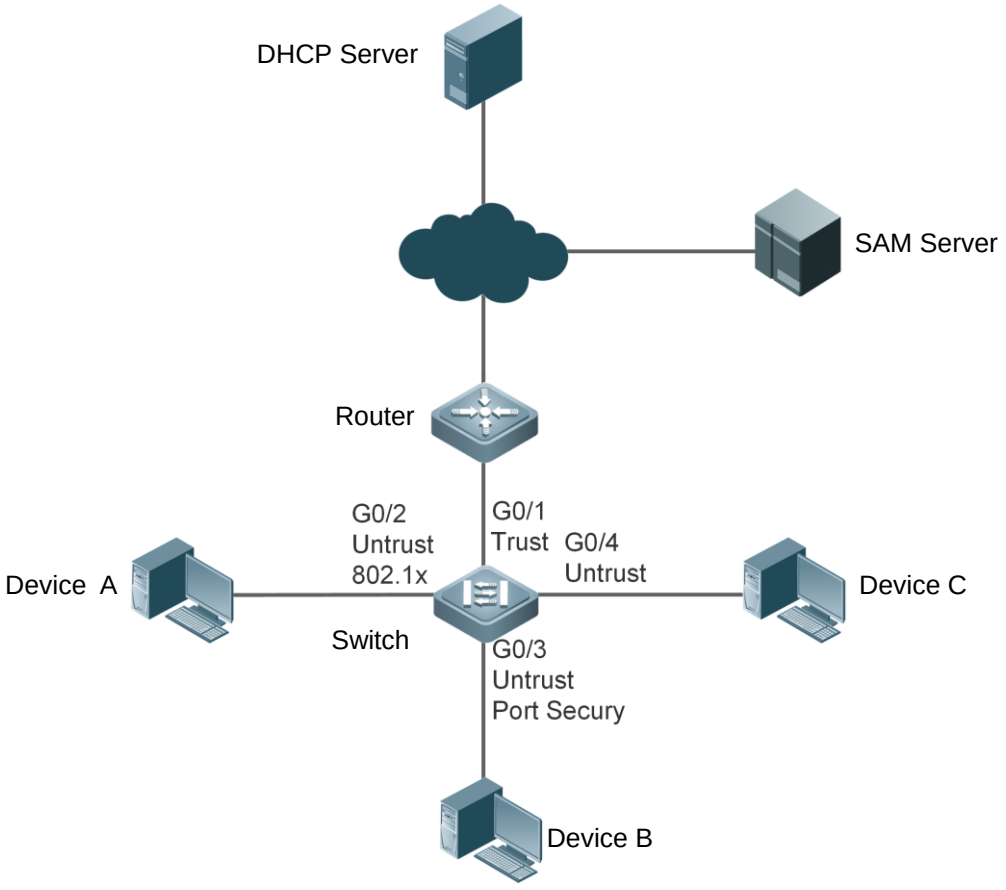
1.2.1 Stateless Address Autoconfiguration

Scenario

Users use SLAAC to assign IPv6 addresses and configure ND snooping to improve IPv6 network security.

- Filter invalid address spoofing packets and RA packets.
- Monitor users who access the IPv6 network and bind these IPv6 addresses to user hosts to prevent IPv6 address spoofing.
- Automatically adapt to IPv6 network configuration changes.

Figure 1-1 Network Topology of SLAAC



Notes	The switch is the access device. Device A is a PC. Device B is a PC. Device C is a PC.

Deployment

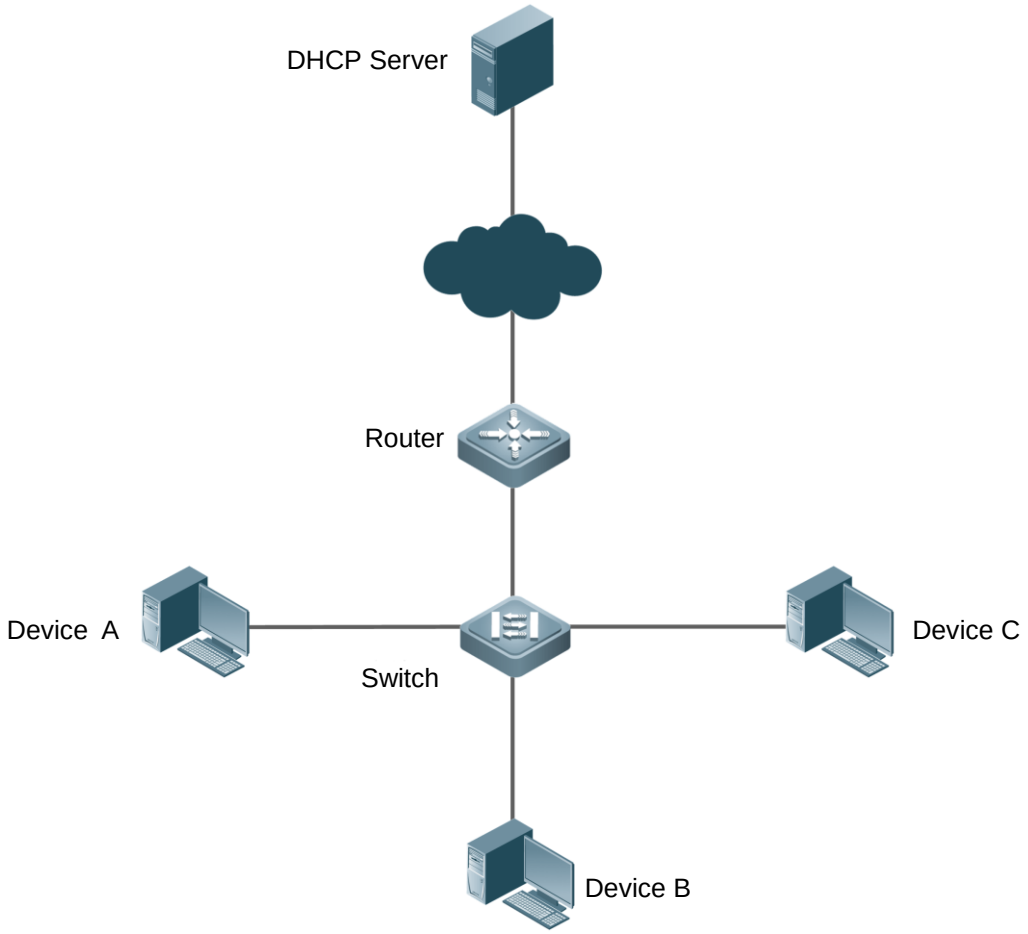
- Enable IPv6 ND snooping on the switch to monitor ND packets.
- Configure trusted interfaces.
- Enable only ND guard against address spoofing attacks.
- Enable SLAAC user monitoring.

1.2.2 Stateful Address Autoconfiguration

Scenario

Users use DHCPv6 to assign IPv6 addresses, enable DHCPv6 snooping, and deploy IPv6 ND snooping to achieve ND guard against RA attacks and ND guard against address spoofing attacks.

Figure 1-2 Network Topology of Stateful Address Autoconfiguration



Notes	The switch is the access device. Device A is a PC. Device B is a PC. Device C is a PC.

Deployment

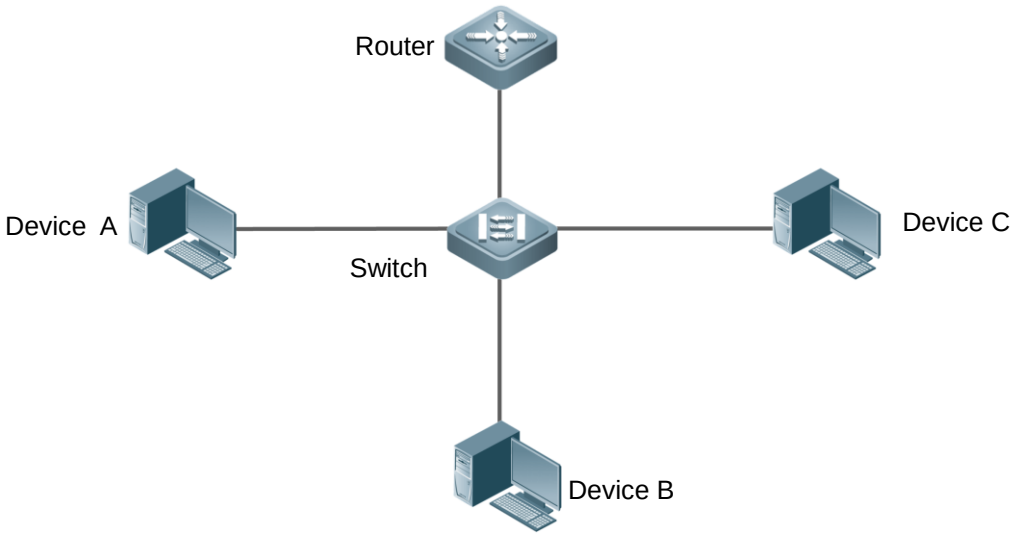
- Enable IPv6 ND snooping on the switch to monitor ND packets.
- Configure trusted interfaces.
- Enable only ND guard against address spoofing attacks.

1.2.3 Manual Configuration

Scenario

Users manually assign IPv6 addresses and deploy the IPv6 ND snooping feature to achieve ND guard against RA attacks and ND guard against address spoofing attacks. This is achieved without the need to deploy other security policies.

Figure 1-3 Network Topology of Manual Configuration



Notes	The switch is the access device. Device A is a PC. Device B is a PC. Device C is a PC.

Deployment

- Enable IPv6 ND snooping on the switch to monitor ND packets.
- Configure trusted interfaces.
- Enable only ND guard against address spoofing attacks on key nodes.
- Manually add a gateway as a key node.

1.3 Features

Basic Concepts

NDP

NDP is a core protocol of the IPv6 protocol suite. It combines and optimizes protocols such as the Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP) Router Discovery, and ICMP Redirect in IPv4. As a basic IPv6 protocol, NDP also provides the prefix discovery, neighbor unreachability detection (NUD), duplicate address detection (DAD), and address autoconfiguration functions.

- Address resolution: a method to determine the link-layer address (LLA) of a target node. The address resolution function of NDP replaces ARP in IPv4 and uses the NUD method to check the reachability status between neighbors.
- Stateless Address Autoconfiguration: It is a unique automatic address configuration mechanism in NDP, including a series of related functions, such as router discovery, automatic interface ID generation, and DAD. Through SLAAC, nodes on a link can automatically obtain global unicast IPv6 addresses.
- Redirection: When a better router for reaching the destination network is found on the local link, the original router needs to send advertisements to nodes, for the nodes to change related configurations.

Features

Feature	Description
ND Snooping	ND snooping is used to monitor ND packets on a network to filter out invalid ARP packets and RA packets, monitor IPv6 users on the network, and bind detected IPv6 users to interfaces to prevent IP address spoofing.

1.3.1 ND Snooping

Working Principle

ND snooping is used to monitor ND packets on a network to filter out invalid ARP packets and RA packets, monitor IPv6 users on the network, and bind detected IPv6 users to interfaces to prevent IP address spoofing.

ND snooping supports the following functions:

ND Guard

When SLAAC is used, IPv6 nodes use RA information to configure interface IPv6 addresses and obtain the prefixes of direct-connected network segments, gateway IP addresses, and maximum transmission units (MTUs) of links. In addition, routers can use ND redirect packets to modify the next-hop information of related routes in the routing tables of hosts. In this case, attackers can send invalid RA and redirect packets and modify routing table information (such as the gateway IP address) of the victim host to initiate denial-of-service (DoS) or man-in-the-middle (MITM) attacks. This type of attacks for spoofing hosts' routing information is called RA attacks.

During unicast communication between IPv6 nodes, the NDP is used for address resolution to obtain LLAs of neighboring nodes. Then, the parsed LLAs are encapsulated into frames to be sent. Five types of ND packets can carry the LLA, and the receiving nodes regard the packets as trusted. Therefore, attackers can send forged ND packets and modify the mappings between IP addresses and LLAs in the neighbor table of the victim node to initiate DoS or MITM attacks. This type of attacks for spoofing the mappings between IP addresses and LLAs on nodes is called address spoofing attacks.

To prevent the preceding two types of attacks, ND snooping classifies interfaces on network devices into trusted interfaces and untrusted interfaces. Trusted interfaces are used to connect trusted nodes, such as routers and servers, and untrusted interfaces are used to connect untrusted nodes, such as PCs. The device forwards ND packets received on trusted interfaces while discarding redirect and RA packets received on untrusted interfaces to prevent RA attacks. For router solicitation (RS), neighbor solicitation (NS), and neighbor advertisement (NA) packets received on untrusted interfaces, the device checks the packet validity and discards invalid ones to prevent address spoofing attacks.

For NS and NA packets, the device checks mappings of the four elements, namely, source/destination IP addresses, VLAN ID (VID), Media Access Control (MAC) address, and inbound interface, to determine the packet validity. The mappings of the four elements of host nodes are provided by monitoring SLAAC users. If an NA packet received on an untrusted interface carries information that can be set only by a router (R bit is set), the packet is regarded as invalid.

Security check on ND packets from all host nodes prevent gateway address spoofing attacks. To guard against only gateway address spoofing attacks, see "ND Auto-guard Against Gateway Attacks." ND guard against RA attacks is regardless of the preceding factors. You can enable ND guard against address spoofing attacks by running the corresponding command. ND guard against RA attacks is enabled as long as ND snooping is enabled.

ND Auto-guard Against Gateway Attacks

Gateway address spoofing is a common attack form and causes severe adverse impact. If gateway address spoofing attacks are eliminated, a network is free from most address spoofing attacks. In addition, you can save significant system resources when only ND auto-guard against gateway attacks is enabled. To facilitate use, ND snooping supports not only manual gateway information configuration but also automatic gateway information acquisition.

A gateway is one of key nodes on a network. ND snooping supports ND guard against address spoofing attacks on key nodes. That is, ND packets received from untrusted interfaces are checked only to determine whether they are forged ND packets of key nodes, so as to discard forged packets. This significantly reduces the CPU load of network devices, resource consumption, and dependency on other security features, such as the features mentioned in the description about ND guard. Gateway information can be obtained automatically or manually. Key node information is automatically generated from the obtained gateway information to implement ND guard against gateway address spoofing attacks.

During automatic gateway information acquisition, ND snooping allows automatic learning of gateway information by snooping RA packets on the network. If the gateway changes, ND snooping automatically updates the gateway information. The whole process is transparent to network administrators and does not require special configuration. If you choose to manually configure an IPv6 network, you can add gateway information and server information as key node information to guard against server address spoofing attacks.

SLAAC User Monitoring

Users configured by SLAAC are called SLAAC users. During SLAAC, the network administrator does not know how many IPv6 users exist on the network and therefore cannot deploy related management policies.

If a network attack occurs, the network administrator can obtain the attacker's IP address. However, the network administrator can only locate the specific network segment based on the IP address but cannot locate the specific network device port or physical client. To resolve this issue, you can monitor SLAAC users on the network to obtain related user information. SLAAC user monitoring can be configured only on untrusted interfaces.

ND Snooping and CPP

Network devices consume certain CPU resources to check ND packet security. To prevent attackers from initiating DoS attacks by sending a large number of ND packets, network devices can use the CPU Protection Policy (CPP) function to control the rate and priority of ND packets on the entire device. After the ND snooping function is enabled, the CPP function is enabled automatically for ND packets.

ND Snooping and NFPP

The CPP function is used for overall control of ND packets on the entire device. Moreover, the Network Foundation Protection Policy (NFPP) function can be used to limit the rate of ND packets based on interfaces. The NFPP function takes effect only on ND packets destined for the CPU.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic ND Snooping Features	(Mandatory) It is used to establish the ND snooping service.	
	ipv6 nd snooping enable	Enables the ND snooping feature.
	(Optional) It is used to configure some attributes of ND snooping.	
	ipv6 nd snooping enable vlan	Enables ND snooping in a VLAN.
	ipv6 nd snooping bind lifetime	Configures the lease for ND snooping binding entries.
	ipv6 nd snooping bind limit	Configures the capacity for ND snooping binding table.
	ipv6 nd snooping bind warning-threshold	Configures the capacity alarm threshold for ND snooping binding entries.
	ipv6 nd snooping tentative wait	Configures the wait time for the device enabled with ND snooping for a DAD response.
Configuring ND Guard	(Optional) It is used to configure ND guard.	
	ipv6 nd snooping trust	Configures an interface as an ND snooping trusted interface.
	ipv6 nd snooping check address-resolution	Enables ND guard against address spoofing attacks.
	ipv6 nd snooping detect packet	Configures the number of detection packets to be sent and the interval for sending detection packets when conflicted packets are received.
	ipv6 nd snooping detect wait	Configures the wait time for the device enabled with ND snooping for a detection packet response.
	ipv6 nd snooping nd-check only	Configures ND snooping to work only in ND packet validity check mode.
	ipv6 nd snooping prefix	Configures IPv6 address prefix manually.
	ipv6 nd snooping log enable	Enables the function of logging ND snooping key information.

	ipv6 nd snooping log limit	Configures the capacity of ND snooping key information logs.
	ipv6 nd snooping syslog enable	Enables system prompts for ND snooping key information.
	ipv6 nd snooping syslog frequency	Configures the frequency of ND snooping key information prompts.

1.4.1 Configuring Basic ND Snooping Features

Configuration Effect

Enable ND snooping to ensure IPv6 network security.

Notes

N/A

Configuration Steps

Enabling ND Snooping

- Mandatory.
- To make ND snooping take effect, you must enable ND snooping on the device.

Command	**ipv6 nd snooping enable**
Parameter Description	N/A
Defaults	ND snooping is disabled.
Command Mode	Global configuration mode
Usage Guide	The monitored SLAAC user information can be used in ND guard against spoofing attacks and other security policies.

Enabling ND Snooping for VLANs

- Optional.

Command	**ipv6 nd snooping enable vlan** { *vlan-rng* | *vid* [*vid*] }
Parameter Description	*vlan-rng:* Indicates the VLAN ID or VLAN ID range. The value of ***vlan-rng*** can be a single VLAN or a VLAN range. When you specify a VLAN range, separate the VLAN IDs by commas (,). Continuous VLAN IDs can be shortened by connecting the first and last VLAN IDs by a hyphen (-). VLAN IDs in the range may not be in order. *vid*: Indicates the VLAN ID. The value range is from 1 to 4094.
Defaults	ND snooping is enabled in all VLANs.
Command Mode	Global configuration mode

Usage Guide	If SLAAC snooping is not required in some VLANs, you can run this command to disable ND snooping in these VLANs.

Configuring the Lease for ND Snooping Binding Entries

- Optional.
- When the aging time of an entry expires, the device enabled with ND snooping sends a probe packet to check whether the user is still online. An excessively short lease indicates frequent probes, while an excessively long lease will overload the device memory. It is recommended that the lease time be increased by 100s for every 1,000 users on the basis of the default value.

The lease time of an ND snooping binding entry is not the lease time of an ND entry. When the lease time of the former expires, the device enabled with ND snooping sends a probe packet to the user to detect whether the user is still online. This prevents the binding entry from occupying the memory space for a long time. The lease time of the latter is the available time of the IP address obtained by the user from the router, which is a part of the RA packets.

Command	**ipv6 nd snooping bind lifetime** *num*
Parameter Description	*num*: Indicates the lease time of an entry, in seconds. The value range is from 5 to 604800.
Defaults	The lease time of ND snooping binding entries is 3600 seconds.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the lease time for an entry to prevent binding entries from occupying the memory space for a long time.

Configuring the Capacity for ND Snooping Binding Table

- Optional.

You can configure the capacity for the binding table to limit the number of users on the network.

Command	**ipv6 nd snooping bind limit** *num*
Parameter Description	*num*: Indicates the capacity of the ND snooping binding table. This parameter varies based on the product version. The actual capacity of the product prevails.
Defaults	The capacity of the ND snooping binding table varies based on the product version. The actual capacity of the product prevails.
Command Mode	Global configuration mode, interface configuration mode, or WLAN security configuration mode
Usage Guide	This command is used to configure the capacity for binding entries. The configured value cannot be smaller than the number of existing binding entries.

Configuring the Capacity Alarm Threshold for ND Snooping Binding Entries

Optional.

Command	**ipv6 nd snooping bind warning-threshold** *num*

Parameter Description	*num*: Indicates the ratio of the capacity alarm threshold for the binding entries to the capacity of binding entries, in percentage (%). The value range is from 15 to 100.
Defaults	The capacity alarm threshold is not configured for ND snooping binding entries.
Command Mode	Global configuration mode, interface configuration mode, or WLAN security configuration mode
Usage Guide	● This command is used to configure a capacity alarm threshold for the binding entries. For example, if ***num*** is set to 60, an alarm is triggered when the current number of entries exceeds 60% of the configured capacity and a prompt is displayed when the current number of entries is less than 60% of the configured capacity. ● When the configuration is removed, ***num*** is set to 0. In this case, no capacity alarm is triggered. ● When this command is configured on an interface and the capacity for binding entries is not limited on the interface (that is, the **num** parameter in the **ipv6 nd snooping bind limit** command is set to 0), no capacity alarm is triggered.

Configuring the Wait Time for a DAD Response

- Optional.
- When receiving a DAD_NS packet from a client, the device enabled with ND snooping considers that the client intends to use this address. However, it does not mean that the client has the right to use this address. Only if the device does not receive a conflicting packet within a period of time, it considers that the terminal can use this address. The period is the wait time for a DAD response.

⚠ The wait time is only a reference value in ND snooping and may be inaccurate.

Command	**ipv6 nd snooping tentative wait** *time*
Parameter Description	*time*: Indicates the wait time, in milliseconds. The value range is from 50 to 5000.
Defaults	The wait time of the device enabled with ND snooping for a DAD response is 500 ms.
Command Mode	Global configuration mode
Usage Guide	When the device enabled with ND snooping receives a DAD_NS packet (for duplicate address check) from a client, the device creates an entry in **TENTATIVE** state. The entry is changed to a formal binding entry after a period of time.

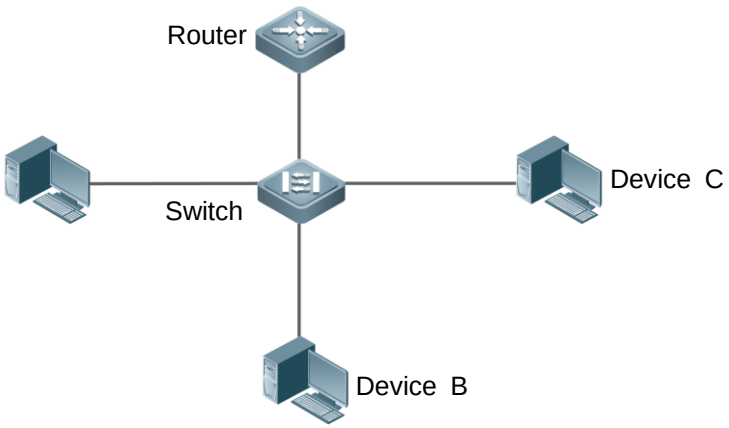
Verification

Run the **show running-config** command to check the ND snooping configuration status.

Configuration Example

Enabling ND Snooping

Scenario	
Figure 1-4	

	 Users manually assign IPv6 addresses and deploy the IPv6 ND snooping feature to achieve ND guard against RA attacks and ND guard against address spoofing attacks. This is achieved without the need to deploy other security policies.
Configuration Steps	● Enable ND snooping globally. ● Disable ND snooping on the VLANs that do not need ND snooping.

Switch	`Hostname#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# ipv6 nd snooping enable`
	`Hostname(config)# no ipv6 nd snooping enable vlan 100`
	`Hostname(config)# no ipv6 nd snooping enable vlan 4,5-7,15`
	`Hostname(config)#`

Verification	● Check whether ND snooping is enabled.
	`Hostname#show running-config | begin ipv6 nd`
	`Current configuration : 491 bytes`
	
	`ipv6 nd snooping enable`
	`no ipv6 nd snooping enable vlan 100`
	`no ipv6 nd snooping enable vlan 4,5-7,15`
	`!`

Common Errors

N/A

1.4.2 Configuring ND Guard

Configuration Effect

The IPv6 ND snooping feature is configured to achieve ND guard against RA attacks and ND guard against address spoofing attacks.

Notes

ND snooping must be enabled for all VLANs before user binding is enabled.

Configuration Steps

Configuring an Interface as a Trusted Interface

- Optional.
- When a network interface is connected to an internal network device, there is no attack. You can set the interface as a trusted interface.
- By default, the trust status of all interfaces is untrust. You can run commands to set the trust status of an interface to trust.

Command	**ipv6 nd snooping trust**
Parameter Description	N/A
Defaults	All interfaces are untrusted interfaces.
Command Mode	Interface configuration mode
Usage Guide	• This command is used to configure an interface as an ND snooping trusted interface. RA and RR packets received on trusted interfaces are forwarded, and such packets received on untrusted interfaces are discarded. • This command can be configured only on Layer 2 switch ports, aggregate ports, or encapsulation sub-interfaces. When this command is configured on other types of interfaces, the configuration will fail. ⚠ Typically, uplink interfaces, that is, interfaces connected to trusted gateways are configured as trusted interfaces.

Enabling ND Guard Against Address Spoofing Attacks

- Optional.
- You are advised to configure ND guard against address spoofing attacks in a complex network environment.

Command	**ipv6 nd snooping check address-resolution**
Parameter Description	N/A
Defaults	ND guard against address spoofing attacks is disabled.
Command Mode	Interface configuration mode, WLAN security configuration mode
Usage Guide	When ND guard against address spoofing attacks is enabled, the IPv6 address and Media Access Control (MAC) address fields in neighbor solicitation (NS), neighbor advertisement (NA), and router solicitation (RS)

	packets received on an interface are checked to determine whether they match the binding entries. ND packets that do not match the binding entries are discarded. ⚠ The entries for ND guard against address spoofing attacks come from the Source Address Validation Improvement (SAVI) binding table instead of the ND snooping binding table.

Configuring the Number and Interval for Sending Detection Packet When Conflicted Packets Are Received

- Optional.
- When the lease of a binding entry for ND snooping expires or the device receives an NS or NA packet with an address that conflicts with that in a binding entry, the device sends a detection packet to the interface recorded in the binding entry. This command is used to set the number of detection packets to be sent and the interval for sending detection packets.

⚠ The interval is only a reference value in ND snooping for sending packets and may be inaccurate.

Command	**ipv6 nd snooping detect packet** *num* **interval** *time*
Parameter Description	*num*: Indicates the number of detection packets to be sent. The value range is from 1 to 10. *time*: Indicates the wait time, in milliseconds. The value range is from 50 to 5000.
Defaults	Two detection packets are sent at an interval of 250 ms.
Command Mode	Global configuration mode
Usage Guide	When the device with ND snooping enabled receives an NS or NA packet with an address that conflicts with that in a binding entry or the lease of a binding entry expires, the device sends a detection packet to the interface recorded in the binding entry. This command is used to set the number of detection packets to be sent and the interval for sending detection packets.

Configuring the Wait Time for a Detection Packet Response

- Optional.

Command	**ipv6 nd snooping detect wait** *time*
Parameter Description	*time*: Indicates the wait time, in milliseconds. The value range is from 50 to 5000. ⚠ The wait time is only a reference value in ND snooping and may be inaccurate.
Defaults	The wait time varies based on the product version. The actual wait time of the product prevails.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the wait time for a detection packet response after the device with ND snooping enabled sends a detection packet. If no response is received within the wait time, the device deletes the corresponding entry.

Configuring ND Snooping to Work Only in ND Packet Validity Check Mode

- Optional.

This command is usually configured in the DHCPv6-only scenario of SAVI to check the validity of ND packets between DHCPv6 users.

Command	**ipv6 nd snooping nd-check only**
Parameter Description	N/A
Defaults	ND snooping does not work only in ND packet validity check mode.
Command Mode	Global configuration mode
Usage Guide	This command can be configured when ND snooping entries do not need to be generated but the ND packet validity needs to be checked. This command takes effect only after ND snooping is enabled.

Configuring IPv6 Address Prefix Manually

- Optional.

Command	**ipv6 nd snooping prefix vlan** *vid ipv6-prefix*
Parameter Description	*vid*: Indicates the access VLAN. The value range is from 1 to 4094. *ipv6-prefix*: Indicates the IPv6 address prefix.
Defaults	No static IPv6 address prefix is configured.
Command Mode	Global configuration mode
Usage Guide	This command can be used to configure an IPv6 address prefix when a valid IPv6 address prefix entry needs to be configured.

Enabling the Function of Logging ND Snooping Key Information

- Optional.
- When the device enabled with ND snooping detects that an attacker has initiated an address spoofing attack or RA attack, the information about the attacker is recorded to the memory via attack logs.
- When this function is disabled, information logs related to ND attacks recorded in the memory will be cleared.

Command	**ipv6 nd snooping log enable**
Parameter Description	N/A
Defaults	The function of logging ND snooping key information is disabled.
Command Mode	Global configuration mode
Usage Guide	When the ND guard or ND auto-guard against gateway attacks function is enabled, the function of logging ND snooping key information can be enabled. When the device receives packets for address spoofing attacks or RA attacks, it will record the attacker information to the memory via attack logs.

Configuring the Capacity of ND Snooping Key Information Logs

- Optional.
- After the function of logging key information is enabled to record information logs related to ND attacks, information about ND attackers is recorded to the memory. If the capacity for storing attack logs reaches the upper limit, new attack logs replace the earliest ones.

Command	**ipv6 nd snooping log limit** *num*
Parameter Description	*num*: Indicates the capacity. The value range is from 50 to 5000.
Defaults	The capacity of ND snooping key information logs varies based on the product version. The actual capacity of the product prevails.
Command Mode	Global configuration mode
Usage Guide	When the capacity value for recording ND snooping key information logs is configured and the capacity for address spoofing or RA attack logs reaches the upper limit, new attack logs will replace the earliest logs.

Enabling System Prompts for ND Snooping Key Information

- Optional.
- When the device enabled with ND snooping detects that an attacker has initiated an address spoofing attack or RA attack, the attacker information will be displayed as system prompt.

Command	**ipv6 nd snooping syslog enable**
Parameter Description	N/A
Defaults	System prompts for ND snooping key information are disabled.
Command Mode	Global configuration mode
Usage Guide	When the ND guard against address spoofing attacks or ND guard against RA attacks function is enabled, the ND snooping key information log recording function is enabled. When the device receives packets for address spoofing attacks or RA attacks, it will display the attacker information as system prompt.

Configuring the Frequency of ND Snooping Key Information Prompts

- Optional.
- This command is used to configure the frequency of ND snooping key information prompts, that is, the maximum number of system prompts generated every second.
- When key information is generated, such as information about address spoofing attacks, RA attacks, capacity threshold alarms, and entry capacity alarms, the system generates corresponding prompt logs.

Command	**ipv6 nd snooping syslog frequency** *num*
Parameter Description	*num*: Indicates the frequency of system prompts, in times/s. The value range is from 1 to 65535.
Defaults	The frequency of ND snooping key information prompts is 5/s.
Command	Global configuration mode

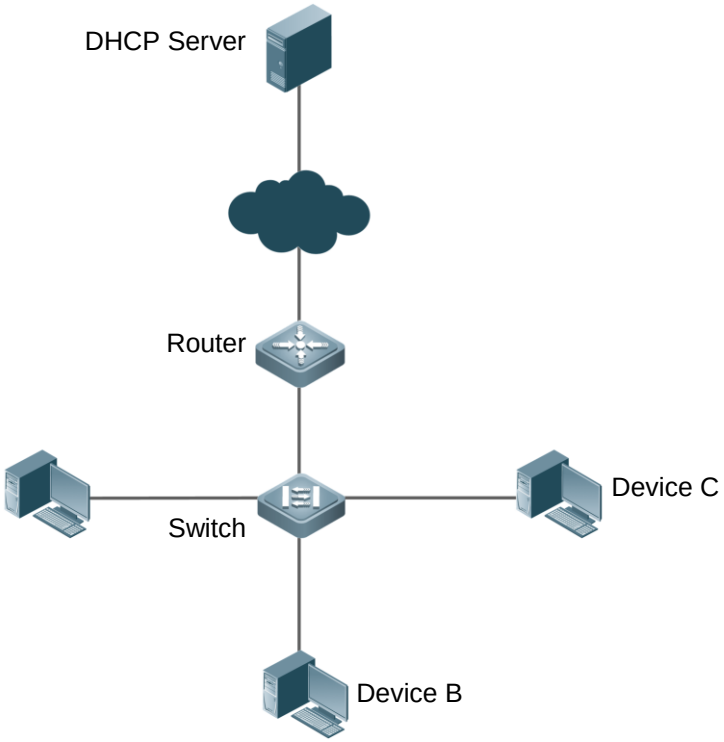
Mode	
Usage Guide	This command is used to configure the frequency of ND snooping key information prompts, that is, the maximum number of system prompts generated per minute. When key information is generated, such as information about address spoofing attacks, RA attacks, capacity threshold alarms, and entry capacity alarms, the system generates corresponding prompt logs. However, when the number of logs generated within one minute is greater than the configured frequency, the system displays logs within the frequency range only and discards remaining logs to prevent the screen from frequent refreshing. ⚠ The log limiting function is implemented based on the system time, while the log display is implemented based on the user time. Therefore, the number of logs with the same time on the console is [0,2 x *num*].

Verification

Run the **show running-config** command to check the ND snooping configuration status.

Configuration Example

↘ Stateful Address Autoconfiguration

Scenario Figure 1-5	 Users use DHCPv6 to assign IPv6 addresses, enable DHCPv6 snooping, and deploy IPv6 ND snooping to achieve ND guard against RA attacks and ND guard against address spoofing attacks.
Configuration Steps	● Enable ND snooping. ● Configure GigabitEthernet 0/1 as an ND snooping trusted interface.

	● Enable only ND guard against address spoofing attacks.
Switch	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#ipv6 nd snooping enable Hostname(config)#interface gigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)#ipv6 nd snooping trust Hostname(config-if-GigabitEthernet 0/1)# interface fastethernet 0/2 Hostname(config-if-GigabitEthernet 0/1)#ipv6 nd snooping check address-resolution
Verification	Run the **show running-config** command to check the ND snooping configuration status.

Common Errors

N/A

1.5 Monitoring

Clearing

Command	Description
clear ipv6 nd snooping prefix [**vlan** *vid*]	Clears prefixes snooped in a VLAN.
clear ipv6 nd snooping binding [**vlan** *vid*]	Clears snooped SLAAC users.
clear ipv6 nd snooping packet [**interface** *interface-type interface-id*]	Clears ND snooping packet statistics on an interface.

Displaying

Command	Description
show ipv6 nd snooping prefix	Displays snooped prefix information.
show ipv6 nd snooping binding [*ip-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-type interface-id*]	Displays monitored ND snooping binding entries.
show ipv6 nd snooping log	Displays ND snooping key information logs recorded in the memory.
show ipv6 nd snooping packet	Displays ND snooping packet statistics on an interface.

Debugging

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

Command	Description

debug ipv6 nd snooping	Debugs ND snooping events.

1 ND Proxy

1.1 Overview

ND proxy, provided by the Access Controller (AC), can act as a proxy for a device on a Wireless Local Area Network (WLAN) to respond to multicast Neighbor Solicitation (NS) packets from another device. Since Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is used for wireless network users, ND proxy can prevent multicast NS packets from being propagated beyond the coverage area of an Access Point (AP) to another AP. This increases the bandwidth utilization of the WLAN and improves the experience of wireless users.

Protocols and Standards

N/A

1.2 Applications

Applications	Description
Providing the ND Proxy Service on a WLAN	The AC acts as the proxy to respond to multicast NS packets from any device within a WLAN.

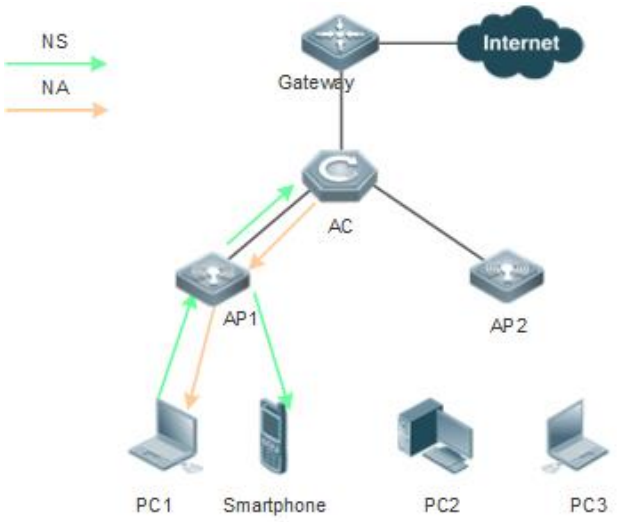
1.2.1 Providing the ND Proxy Service on a WLAN

Scenario

In centralized forwarding mode of the fit AP architecture, the AC acts as a proxy to respond to the multicast NS packets from any device within a WLAN.

- The AC needs to learn the MAC address of a device within a WLAN before acting as a proxy to respond.

Figure 1-1



Note:	The preceding diagram illustrates the flow of ND packets when a wireless user sends requests to a gateway or other devices in centralized forwarding mode of the fit AP architecture.

Deployment

Build a network consisting of a gateway, an AC, APs, and stations (STAs). On this network, the AC acts as a proxy to respond to the multicast NS packets from a STA through ND proxy (which is enabled by default). This prevents multicast NS packets from being sent to other APs.

- ND proxy operates on the AC, with no additional configuration.

1.3 Features

Basic Concepts

↘ ND Proxy

The Layer 2 ND proxy is a special function of ACs. It acts as a proxy for a device to respond to to the multicast NS requests from another device within the same Local Area Network (LAN). Due to the communication mechanism of CSMA/CA between wireless network users, the ND proxy function can reduce the spread of multicast NS packets from the coverage area of an AP to that of another AP. This increases the bandwidth utilization of the wireless network and improves the experience of wireless users.

Feature

Feature	Description
Layer 2 ND Proxy	The AC acts as a proxy to respond to multicast NS packets of a STA through this function. This prevents the spread of multicast NS requests to other APs.
Static ND Binding Entry	A static ND binding entry is configured manually by an administrator. It is not updated by the device and will exist permanently.

1.3.1 Layer 2 ND Proxy

Working Principle

On a typical wireless network, STAs usually access the Internet through APs and ACs. Typically, multiple wireless users are connected to one AP, and multiple APs are connected to one AC. When wireless users on an AP access those on another AP, or when wireless and wired users access each other, NS packets must pass through the AC. This makes it easy for the AC to implement ND proxy.

The working process of ND proxy includes the following steps:

1. The AC learns source IP and MAC addresses of NS packets passing through it or learns the destination address and MAC address in the source link-layer address carried by Neighbor Advertisement (NA) packets to generate ND proxy entries.
2. The AC acts as a proxy to respond to NS packets from other users based on learned entries.
3. If no information about the target host is learned, multicast NS packets are forwarded in compliance with 802.1Q.
4. NA packets are forwarded in the same manner as Ethernet frames in compliance with 802.1Q.

In Figure 1-1, PC3 and PC1 obtain the gateway MAC address one after another. Assume that there is an AC, two APs, and four STAs on this local network.

1 PC3 initiates an NS packet destined for the IPv6 address of the gateway.

2 AP2 forwards this NS packet to PC2 and the AC.

3 The AC learns the IPv6 address and MAC address of PC3 through the NS packet and forwards it to the gateway, AP1, PC1, and the smartphone on AP1.

4 The gateway responds with an NA packet to PC3. When the response packet passes through the AC, the AC learns the IPv6 address and MAC address of the gateway.

5 PC1 initiates an NS packet destined for the IPv6 address of the gateway.

6 AP1 forwards this NS packet to the smartphone and AC.

7 The AC learns the IPv6 address and MAC address of PC1, and takes place of the gateway to send an NA packet to PC1. In step 4, the AC has already learned the MAC address of the gateway and can respond to NS packets, so multicast NS packets will not be broadcast to PC2 and PC3.

Aging mechanism of ND proxy entries:

The mechanism adopts the Least Recently Used (LRU) algorithm. The entries that are not used recently are aged out first, and the aging speed is configured based on the number of entries:

1 When the number of entries exceeds 20,000, configure the device to age 10 entries per second.

2 When the number of entries exceeds 10,000 and is less than 20,000, configure the device to age one entry per second.

3 When the number of entries exceeds 1,000 and is less than 10,000, configure the device to age one entry every 10 seconds.

4 When the number of entries is less than 1,000, configure the device to age one entry every 100 seconds.

Related Configuration

↘ Configuring the Layer 2 ND Proxy Function

- The Layer 2 ND proxy function is enabled by default.
- You can use the **no proxy-nd enable** command to disable the Layer 2 ND proxy function.

1.3.2 Static ND Binding Entry

Working Principle

A static ND binding entry is manually configured by an administrator. It is not updated by the device and will exist permanently. The static ND binding entry can prevent the device from learning incorrect binding entries, which results in proxy errors and thus affects the network.

Related Configuration

↘ Configuring a Static Layer 2 ND Binding Entry

- No static ND binding entry is configured by default.

- You can use the **proxy-nd** *ipv6-address vid mac interface-id* command in global configuration mode to configure the Layer 2 ND binding entry.

1.4 Configuration

Configuration	Description and Command	
Configuring the Layer 2 ND Proxy Function	⚠ (Mandatory) It is used to enable the Layer 2 ND proxy function on the device.	
	proxy-nd enable	Enables the Layer 2 ND proxy function.
Configuring a Static Layer 2 ND Proxy Entry	⚠ (Optional)	
	proxy-nd *ipv6-address vid mac interface-id*	Configures a static ND binding entry.

1.4.1 Configuring the Layer 2 ND Proxy Function

Configuration Effect

Enabling the Layer 2 ND proxy function according to the actual topology can increase the bandwidth utilization of a wireless network and enhance the experience of wireless users.

Notes

N/A

Configuration Step

↘ Configuring the Layer 2 ND Proxy Function

- Mandatory.
- In a wireless IPv6 environment, enabling the Layer 2 ND proxy function on the AC can increase the bandwidth utilization of the wireless network and improve the experience of wireless users.

Verification

- Run the **show proxy-nd statistics** command to check the configuration.

Related Commands

↘ Enabling the Layer 2 ND Proxy Function

Command	**proxy-nd enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling the Layer 2 ND Proxy Function

Configuration Steps	● Use this command to enable the Layer 2 ND proxy function.
	`Hostname(config)# proxy-nd enable`
Verification	● Run the **show proxy-nd statistics** command to check the configuration.

	`Hostname# show proxy-nd statistics`
	`Nd Proxy: Enable`
	`Total Entry: 100`
	`Dynamic Entry: 99`
	`Static Entery: 1`
	`Next Aging Time: 5 Seconds`
	`Droped Packets: 0`

Common Errors

N/A

1.4.2 Configuring a Static Layer 2 ND Proxy Entry

Configuration Effect

Configuring the static mapping between the IP address and the MAC address of a device or a host in a VLAN prevents static ND binding entries from being updated incorrectly and prevents the AC from incorrectly acting as a proxy for other devices, which affect the network.

Notes

N/A

Configuration Step

Configuring a Static Layer 2 ND Proxy Binding Entry

- Optional.
- On the device enabled with the Layer 2 ND proxy function, you can configure the static mapping between the IP address and the MAC address of the uplink device. This prevents the device from changing the MAC address of the ND binding entry on the uplink device due to NS attacks.

Verification

- Run the **show proxy-nd static** or **show running-config** command to display the static Layer 2 ND proxy binding entry.

Related Commands

Enabling the Layer 2 ND Proxy Function

Command	**proxy-nd** *ipv6-address vid mac interface-id*
Parameter Description	N/A

Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling the Layer 2 ND Proxy Function

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. ● Excluded 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 **show running-config** to check the configuration.

	`Hostname# show running-config`
	`!`
	`GigabitEthernet 0/1`

Common Errors

N/A

1.5 Monitoring

Clearing

Command	Description
clear proxy-nd <*ipv6-address vlan-id*>	Deletes specified ND proxy entries.
clear proxy-nd < *interface-id*>	Deletes all ND proxy entries in a specified VLAN.
clear proxy-nd	Deletes all ND proxy entries.

Displaying

Command	Description
show proxy-nd	Displays all ND proxy entries.
show proxy-nd dynamic	Displays all dynamic ND proxy entries.
show proxy-nd static	Displays all static ND proxy entries.
show proxy-nd <*ipv6-address vlan-id*>	Displays specified ND proxy entries.
show-: bgp statistics	Displays statistics about the ND proxy.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug proxy-nd [**vid** *vid*] [**interface** *interface-id*] [**dst-ipv6** *ipv6-address*] [**src-ipv6** *ipv6-address*] [**src-mac** *src-mac*] [**dst-mac** *dst-mac*]	Displays the sending and receiving of ND packets.
debug- event	Displays information about added, deleted, or updated ND binding entries.
debug proxy-nd error	Displays errors in processing ND packets and ND binding entries.
debug proxy-nd all	Enables all the debugging.

1 Configuring Tunnel

1.1 Overview

Tunnel interfaces are virtual interfaces used to implement tunneling. A tunnel interface provides a standard transmission link and you do not need to specify a transport protocol or payload protocol. Each tunnel interface represents a transmission link.

Tunneling involves the following parts:

- Payload protocol: Is used to encapsulate data transmitted over tunnels. For example, IPv4 and IPv6 protocols work as payload protocols. Generic routing encapsulation (GRE) tunnels can carry IPv4 or IPv6 data.
- Bearer protocol: Is used for secondary encapsulation and identification of data to be transmitted. Among the tunnels described in this document, only the GRE tunnel uses a bearer protocol. The other tunnels use the IPv4 and IPv6 protocols. Packets are encapsulated with outer IPv4 and IPv6 headers.
- Transport protocol: Is used to transmit data encapsulated for the second time through a bearer protocol.

In practice, the tunnel mode can be used to establish communication between two private networks running the same protocol through a heterogeneous public network.

Tunneling is applicable to the following scenarios:

- Because tunneling supports different payload protocols, it allows communication between local networks running non-IP protocols through a single network (IP network). It enables protocols with hop count limitations to operate over a broader range because tunneling uses the routing capabilities of the IP protocol.
- Tunneling allows discrete subnets to be connected through a single IP network.
- Tunneling enables the provision of the virtual private network (VPN) over a wide area network (WAN).

Because tunneling encapsulates the payload for transmission, this introduces processing complexity, and the following changes need to be considered:

- Because a tunnel is a logical link, it appears to be a single hop during routing. However, its path cost may involve multiple hops. When you use a tunnel for transmission, note that the route of the tunnel link is different from the actual route.
- In tunnel transmission, the payload is encapsulated into the transport protocol. Consider the tunnel configuration during access control list (ACL) configuration. Note that the transmission bandwidth and maximum transmission unit (MTU) allowed by payload protocols are smaller than the theoretical values.

Protocols and Standards

- RFC 2784: Generic Routing Encapsulation (GRE)
- RFC 2890: Key and Sequence Number Extensions to GRE
- RFC 3056: Connection of IPv6 Domains via IPv4 Clouds
- RFC 3068: An Anycast Prefix for 6to4 Relay Routers

- RFC 3964: Security Considerations for 6to4
- RFC 4023: Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)
- RFC 4087: IP Tunnel MIB
- RFC 4213: Basic Transition Mechanisms for IPv6 Hosts and Routers
- RFC 4797: Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks
- RFC 5158: 6to4 Reverse DNS Delegation Specification
- RFC 5214: Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
- RFC 5332: MPLS Multicast Encapsulations
- RFC 5579: Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Interfaces
- RFC 5845: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- RFC 5969: IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification
- RFC 6245: Generic Routing Encapsulation (GRE) Key Extension for Mobile IPv4
- RFC 6343: Advisory Guidelines for 6to4 Deployment
- RFC 6372: 6to4 Provider Managed Tunnels
- RFC 6654: Gateway-Initiated IPv6 Rapid Deployment on IPv4 Infrastructures (GI 6rd)
- draft-zhou-dhc-gre-option-00 DHCPv4 and DHCPv6 options for GRE
- draft-cai-softwire-6rd-mib-03 Definitions of Managed Objects for 6rd
- draft-howard-isp-ip6rdns-05 Reverse DNS in IPv6 for Internet Service Providers
- draft-tsou-softwire-6rd-multicast-02 IPv6 Multicast Using Native IPv4 Capabilities in a 6rd Deployment
- draft-templin-v6ops-isops-18 Operational Guidance for IPv6 Deployment in IPv4 Sites using ISATAP

1.2 Applications

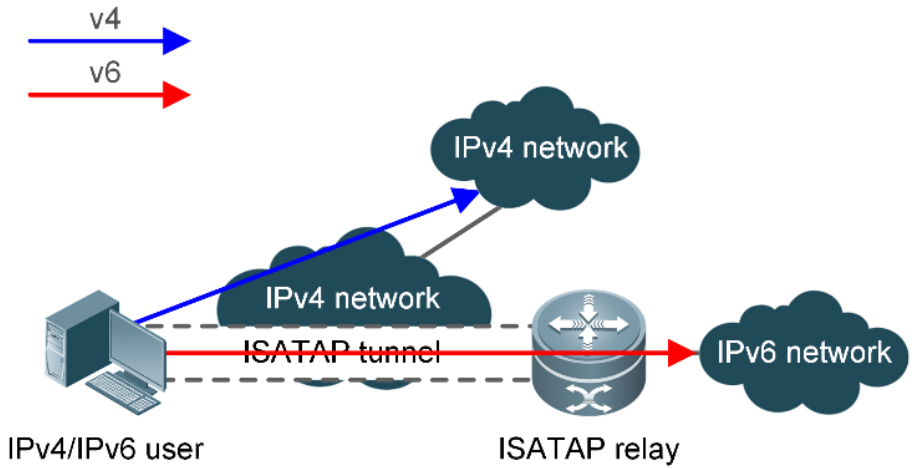
Application	Description
Accessing IPv6 Sites on a Campus Network	Tunneling is used for access to IPv6 sites on a campus network.
Accessing the IPv6 Backbone Network on a Campus Network	Tunneling is used for access to the IPv6 backbone network on a campus network.

1.2.1 Accessing IPv6 Sites on a Campus Network

Scenario

IPv6 servers are deployed on some campus networks, and PCs need to access the servers. The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) can be used to realize the access.

Figure 1-1



Remarks	The ISATAP relay supports tunneling. Users on the campus network can access IPv4 servers directly through the IPv4 network, but need to access IPv6 servers through the ISATAP tunnel.

Deployment

- IPv4 and IPv6 users access the IPv4 network by using IPv4 addresses.
- IPv4 and IPv6 users access the IPv6 network through the ISATAP tunnel.
- The ISATAP tunnel is established between PCs and the ISATAP relay (router).

1.2.2 Accessing the IPv6 Backbone Network on a Campus Network

Scenario

Upgrade the existing campus network to one that supports IPv6 or create a new campus network that supports IPv6 by using the 6to4 automatic tunnel.

1.3 Features

Basic Concepts

MTU of a Tunnel Interface

- The MTU of a tunnel interface is smaller than that of a regular interface, such as a regular IPv4 over IPv4 tunnel. The maximum amount of data carried by a packet transmitted over the Ethernet is 1460 bytes, excluding the Layer 2 IP header. Therefore, the MTU of a tunnel interface is 1480 bytes, not 1500 bytes of a standard Ethernet interface.

PMTU of a Tunnel Interface

- A tunnel interface represents a virtual link. For an IPv4 over IPv4 tunnel, the MTU of a tunnel interface is the MTU of a tunnel link, that is, the MTU of the path between the local and peer ends of the tunnel. When the routing path between the local and peer ends is changed, the path MTU (PMTU) may also be changed, which will affect the MTU of the tunnel interface.

Tunnel Encapsulation Limit

- Tunnel encapsulation is supported. For example, an IPv4 packet can be encapsulated with two or more IPv4 headers and then transmitted over an IPv4 over IPv4 tunnel. Tunnel encapsulation is intended for security guarantee and is seldom used. The amount of data to be transmitted is reduced after tunnel encapsulation. After data is routed through the forwarding information base (FIB), if the outbound interface is another tunnel interface, tunnel encapsulation occurs. If the outbound interface is the local tunnel interface, infinite encapsulation occurs. Such a situation can be detected and information will be displayed.

Overview

Feature	Description
Automatic MTU Adjustment	Dynamically adjusts the MTU of a tunnel interface based on changes of the path MTU of the tunnel link.
Tunnel Encapsulation Limit	Increases the maximum number of nested encapsulations of packets as needed, which is seldom used.
Tunnel Data Validity Check	Adds the checksum to the data transmitted in GRE tunnels to check whether an error occurs during transmission.

1.3.1 Automatic MTU Adjustment

The MTU of a tunnel interface is subject to the MTU of a tunnel link, that is, PMTU. The MTU of the tunnel interface will be changed if a path is changed or the PMTU is changed. The automatic MTU adjustment feature is used to detect these changes and automatically adjust the MTU of the tunnel interface based on the changes.

Working Principle

When a device receives an Internet Control Message Protocol (ICMP) error packet (PACKET TOO BIG) that is an encapsulated IP packet), the faulty tunnel can be located based on encapsulation information. The MTU of the tunnel interface will be changed based on information in the packet.

Related Configuration

↘ Enabling Automatic MTU Adjustment on a Tunnel Interface

By default, automatic MTU adjustment is disabled on a tunnel interface.

To enable or disable automatic MTU adjustment on a tunnel interface, run the **tunnel path-mtu-discovery** command.

For tunnel encapsulation, automatic MTU adjustment needs to be enabled only for the outermost tunnel. The MTU of each inner tunnel is equal to the MTU of the outermost tunnel minus the length of the outer encapsulated header.

1.3.2 Tunnel Encapsulation Limit

In many cases, tunnel encapsulation is a deployment error and is actively deployed only in few cases. By default, products allow four nested encapsulations of a packet at most. Administrators can use a command to change the limit.

Working Principle

If the peer end of tunnel interface A is a regular outbound interface, tunnel Interface A is considered as a regular tunnel interface.

If the peer end of tunnel interface A is another tunnel interface, tunnel Interface A is considered as a nested tunnel interface. If the outbound tunnel is a regular tunnel interface, tunnel Interface A is called a single-nested tunnel. If the outbound tunnel is a single-nested tunnel, tunnel Interface A is called a double-nested tunnel.

If the peer end of tunnel interface A is itself, infinite recursive encapsulation occurs. When the device detects infinite recursive encapsulation, it will output logs and disable tunnel Interface A.

If the peer end of the tunnel is another tunnel interface, routing is performed based on the peer address of the tunnel interface. The actual outbound interface will be determined after multiple times of routing.

If the number of nested encapsulations on a tunnel interface exceeds the upper limit, the device will output logs and disable the tunnel interface.

Note that the tunnel encapsulation limit is specific to the device and differs from the maximum number of encapsulated headers in a packet over a network.

Related Configuration

Configuring the Tunnel Encapsulation Limit on a Tunnel Interface

By default, the maximum number of nested encapsulations of a packet on a tunnel interface is four. To change this limit, run the **tunnel nested-limit** command.

1.3.3 Tunnel Data Validity Check

In a GRE tunnel enabled with data validity check, the receiver checks validity of the packets sent by the peer end to determine whether the packets are tampered during transmission. For long-distance transmission, if application of data carried by a GRE tunnel do not support validity check, you can enable tunnel data validity check.

Working Principle

A GRE tunnel calculates the checksum of the data to be encapsulated at the sender and encapsulates the checksum in the packet before sending the packet out.

Upon receiving the packet, the receiver recalculates the checksum and compares the calculated value to the checksum field in the packet. If the two do not match, the receiver considers that an error occurs in the packet and discards it.

Related Configuration

Enabling Tunnel Data Validity Check on a Tunnel Interface

By default, data validity check is disabled on a tunnel interface.

To enable or disable data validity check on a tunnel interface, run the **tunnel checksum** command.

Tunnel data validity check takes effect only when it is enabled on both ends of a GRE tunnel.

1.4 Configuration

Configuration	Description and Command	
Configuring a Tunnel Interface	⚠ (Mandatory) It is used to create tunnels.	
	Interface tunnel	Creates a tunnel interface.

Configuration	Description and Command	
	tunnel source	Configures the local address of a tunnel.
Configuring an Encapsulation Mode	(Optional) It is used to configure a tunnel mode.	
	tunnel mode	Configures a tunnel encapsulation mode.
Configuring a Peer Address	(Optional) It is used to configure the peer address of a tunnel.	
	tunnel destination	Configures the peer address of a tunnel.
Configuring the ToS of a Tunnel	(Optional) It is used to configure the type of service (ToS) of a tunnel.	
	tunnel tos	Configures the ToS of a tunnel.
Configuring the TTL of a Tunnel	(Optional) It is used to configure the time to live (TTL) of a tunnel.	
	tunnel ttl	Configures the TTL of a tunnel.
Configuring Tunnel Reachability Detection	(Optional) It is used to configure reachability detection for a transmission network.	
	keepalive	Configures reachability detection for a tunnel.
Configuring PMTU Discovery	(Optional) It is used to configure PMTU discovery for a transmission network.	
	tunnel path-mtu-discovery	Configures PMTU discovery for a tunnel.
Configuring the Tunnel Encapsulation Limit	(Optional) It is used to configure the maximum number of nested encapsulations of a packet.	
	tunnel nested-limit	Configures the maximum number of nested encapsulations of a packet.
Configuring Tunnel Data Validity Check	(Optional) It is used to enable data validity check for GRE tunnels.	
	tunnel checksum	Enables data validity check for GRE tunnels.
Configuring a Tunnel Key	(Optional) It is used to configure the check key of a tunnel.	
	tunnel key	Configures the check key of a GRE tunnel.

1.4.1 Configuring a Tunnel Interface

Configuration Effect

- Create a tunnel interface.

Configuration Steps

Creating a Tunnel Interface

- Run the **interface tunnel** *number* command in global configuration mode to create a tunnel interface.
- The tunneling service is available only after a tunnel interface is created.

Verification

- Run the **show interfaces tunnel** *number* command to check whether the tunnel interface is created successfully.

Related Commands

Configuring a Tunnel Interface

Command	**interface tunnel** *number*
Parameter Description	*number*: Indicates the number of a tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Checking the Tunnel Configuration

Command	**show interfaces tunnel** *number*
Parameter Description	*number*: Indicates the number of a tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Creating a Tunnel Interface

Configuration Steps	● Create a tunnel interface.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config-if-Tunnel 1)# end`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`……`
	`Tunnel attributes:`
	`……`
	`Tunnel protocol/transport is gre ip`

Common Errors

- A tunnel interface cannot be created due to insufficient memory.
- A tunnel interface cannot be created due to insufficient hardware resources.

1.4.2 Configuring an Encapsulation Mode

Configuration Effect

- Configure an encapsulation mode in tunnel interface configuration mode when you need to use a tunnel in non-default encapsulation mode.

Configuration Step

Configuring an Encapsulation Mode

- Optional.
- The default encapsulation mode is **tunnel mode gre ip**.
- To change the default encapsulation mode, run the **tunnel mode** command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** *number* command to check whether the tunnel encapsulation mode is configured.

Related Commands

Configuring a Tunnel Mode

Command	**tunnel mode** { **gre ip** | | **ipv6ip** [**6to4** | **isatap**] }
Parameter Description	**gre ip**: Indicates that a packet is encapsulated with a GRE header and an IPv4 header in sequence and then is transmitted over a new IPv4 network. **ipv6ip 6to4**: The transmission network is IPv4 network, and GRE for the route is not at the IP layer. The user network is IPv6 network. The IPv4 address of the peer end does not need to be configured. It is used for connection between IPv6 networks. **ipv6ip isatap**: The transmission network is IPv4 network, and GRE for the route is not at the IP layer. The user network is IPv6 network. The IPv4 address of the peer end does not need to be configured. It is used for quick deployment of IPv6 networks.
Command Mode	Interface configuration mode
Usage Guide	Both ends of a tunnel must be configured with the same encapsulation mode. Otherwise, the tunnel cannot work.

Configuration Example

Configuring the IPv4 over IPv4 Encapsulation Mode

Configuration Steps	● Configure the IPv4 over IPv4 encapsulation mode on a tunnel interface.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config-if-Tunnel 1)# tunnel mode ipip`
	`Hostname(config)# end`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`……`
	`Tunnel attributes:`
	`……`
	`  Tunnel protocol/transport is ipv6ip`

Common Errors

N/A

1.4.3 Configuring a Local Address

Configuration Effect

- Configure the local address of a tunnel.

Notes

- The local address of a tunnel must match the transport protocol used by the tunnel. Otherwise, the tunnel interface will not go Up (be disabled).
- When the local address is specified indirectly by configuring another interface, the local address is the primary IPv4 address or the first global public IPv6 address of IPv6.

Configuration Step

↘ Configuring a Local Address

- Mandatory.
- Run the **tunnel source** command in tunnel interface configuration mode to specify the local address of a tunnel.

Verification

- Run the **show interfaces tunnel** *number* command to display the local address of the tunnel.

Related Commands

↘ Configuring a Local Address

Command	**tunnel source** { *ip-address* | *interface-name interface-number* }
Parameter Description	**ip-address**: Indicates an IPv4 or IPv6 address. *Interface-name interface-number*: Indicates a Layer 3 interface.
Command Mode	Interface configuration mode
Usage Guide	If you specify an IPv4 or IPv6 address directly, you need to configure the address of the device.

Configuration Example

↘ Configuring a Local Address

Configuration Steps	● Configure the local address of a tunnel as 1.1.1.1.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config-if-Tunnel 1)# tunnel mode ipv6ip`
	`Hostname(config-if-Tunnel 1)# tunnel source 1.1.1.1`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`……`
	`Tunnel attributes:`
	`  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable`

	Tunnel TOS/Traffic Class not set, Tunnel TTL 254 Tunnel config nested limit is 0, current nested number is 0 Tunnel protocol/transport ipv6ip Tunnel transport VPN is no set ……

1.4.4 Configuring a Peer Address

Configuration Effect

- A manual tunnel can be used (the tunnel interface is Up) only after its peer address is configured.

Notes

- Peer addresses cannot be configured for automatic tunnels.

Configuration Steps

Configuring a Peer Address

- The peer addresses must be configured for all tunnels except 6RD, 6to4, and ISATAP tunnels.
- Run the **tunnel destination** command in interface configuration mode to configure the peer address of a tunnel.

Verification

- Run the **show interfaces tunnel** command to check whether the destination address is configured.

Related Commands

Configuring a Peer Address

Command	**tunnel destination** *ip-address*
Parameter Description	***ip-address***: Indicates an IPv4 or IPv6 address.
Command Mode	Interface configuration mode
Usage Guide	The peer address of a manual tunnel must be configured. The protocol suite type of the configured peer address must be consistent with the transport protocol used by the tunnel. If they are inconsistent, the tunnel interface will be disabled (Down).

Configuration Example

Configuring a Peer Address

Configuration Steps	● Configure the peer address of a tunnel as 2.2.2.2.
	Hostname# configure terminal Hostname(config)# interface tunnel 1 Hostname(config-if-Tunnel 1)# tunnel mode ipv6ip Hostname(config-if-Tunnel 1)# tunnel destination 2.2.2.2
Verification	● Check the configuration of the tunnel interface.

Configuration Steps	● Configure the peer address of a tunnel as 2.2.2.2.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config-if-Tunnel 1)# tunnel mode ipv6ip`
	`Hostname(config-if-Tunnel 1)# tunnel destination 2.2.2.2`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`……`
	`Tunnel attributes:`
	`  Tunnel source: UNKNOWN, destination 2.2.2.2, unrouteable`
	`  Tunnel TOS/Traffic Class not set, Tunnel TTL 254`
	`  Tunnel config nested limit is 0, current nested number is 0`
	`  Tunnel protocol/transport ipv6ip`
	`  ……`

Common Errors

- A peer address is configured for an automatic tunnel.
- The peer address configured for a tunnel is the same as that of another tunnel.

1.4.5 Configuring the ToS of a Tunnel

Configuration Effect

- Specify the ToS or Traffic Class field in the transport protocol header.

Notes

- If the ToS or Traffic Class field in the transport protocol header is not specified, the ToS or Traffic Class field of the protocol is copied to the header.

Configuration Step

↘ Configuring the ToS of a Tunnel

- Optional.
- To change the priority of tunnel data on a network, run the **tunnel tos** command in interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the ToS is configured.

Related Commands

↘ Configuring the ToS of a Tunnel

Command	**tunnel tos** *number*
Parameter Description	***number***: Indicates the ToS of a tunnel.

Command Mode	Interface configuration mode
Usage Guide	By default, if the IPv4 protocol is used for the inner bearer and outer encapsulation in a tunnel, the ToS bytes in the inner IPv4 header are copied to the outer IPv4 header. If the IPv6 protocol is used for the inner bearer and outer encapsulation in a tunnel, the 8-bit Traffic Class in the inner IPv6 header is copied to the outer IPv6 header. In other cases, the ToS field in the outer IPv4 header and the Traffic Class field in the IPv6 header are 0.

Configuration Example

Configuring the ToS of a Tunnel

Configuration Steps	● Configure the ToS of a tunnel.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config-if-Tunnel 1)# tunnel mode ipv6ip`
	`Hostname(config-if-Tunnel 1)# tunnel tos 2`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`……`
	`Tunnel attributes:`
	`  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable`
	`  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 254`
	`  Tunnel config nested limit is 0, current nested number is 0`
	`  Tunnel protocol/transport ipv6ip`
	`  Tunnel transport VPN is VPN1`
	`……`

1.4.6 Configuring the TTL of a Tunnel

Configuration Effect

- Specify the TTL or hop limit of tunnel encapsulation protocol headers.

Configuration Step

Configuring the TTL of a Tunnel

- Optional.
- By default, the TTL is 254.
- To change the hop limit of a tunnel, run the **tunnel ttl** command.

Verification

- Run the **show interfaces tunnel** command to check whether the TTL is configured.

Related Commands

Configuring the TTL of a Tunnel

Command	**tunnel ttl** *hop-limit*
Parameter Description	*hop-limit*: Indicates the hop limit of a tunnel.
Command Mode	Global configuration mode
Usage Guide	The hop limit specifies the maximum number of routers that a packet can pass through. The default value is 254. This command is used to change the hop limit.

Configuration Example

Configuring the TTL of a Tunnel

Configuration Steps	● Configure the TTL of a tunnel.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config-if-Tunnel 1)# tunnel mode ipv6ip`
	`Hostname(config-if-Tunnel 1)# tunnel ttl 3`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`……`
	`Tunnel attributes:`
	`  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable`
	`  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3`
	`  Tunnel config nested limit is 0, current nested number is 0`
	`  Tunnel protocol/transport ipv6ip`
	`  Tunnel transport VPN is VPN1`

1.4.7 Configuring Tunnel Reachability Detection

Configuration Effect

- Determine availability of tunnels more accurately through tunnel reachability detection.

Configuration Step

Configuring Tunnel Reachability Detection

- Tunnel reachability detection is optional for manual tunnels. Automatic tunnels do not support reachability detection.
- To dynamically monitor availability of tunnel links, configure tunnel reachability detection in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether tunnel reachability detection is configured.

Related Commands

Configuring Tunnel Reachability Detection

Command	**keepalive** [*seconds* [*retries*]]
Parameter Description	***seconds***: Indicates the interval at which keepalive packets are retransmitted, in seconds. *retries*: Indicates the number of times keepalive packets are retransmitted.
Command Mode	Interface configuration mode
Usage Guide	Manual tunnels support reachability detection, whereas automatic tunnels do not support it. By default, tunnel reachability detection is disabled. A tunnel interface is Up if the route to the destination IP address can be found in the routing table of the device. After tunnel reachability detection is enabled, the tunnel interface is Up if keepalive packets are sent and received correctly.

Configuration Example

Configuring Tunnel Reachability Detection

Configuration Steps	● Configure tunnel reachability detection.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config)# tunnel mode ipv6ip`
	`Hostname(config)# keepalive 3 5`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`Index(dec):11 (hex):b`
	`…`
	`  Keepalive interval is 3 sec ,retries 5.`

1.4.8 Configuring PMTU Discovery of a Tunnel

Configuration Effect

- Configure PMTU discovery to allow the MTU of a tunnel interface to be adjusted automatically based on the changes of the route MTU. Before this feature is configured, the MTU of the tunnel interface is equal to the MTU of the transport protocol minus the length of the header encapsulated through a transport protocol.

Configuration Step

Configuring PMTU Discovery

- PMTU discovery is optional for manual tunnels. Automatic tunnels do not support PMTU discovery.
- To dynamically monitor and adjust MTUs of tunnel links, configure PMTU discovery in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether PMTU discovery is configured.

Related Commands

Configuring PMTU Discovery

Command	**tunnel path-mtu-discovery** [**age-timer** {*aging-mins* | **infinite**} | **min-mtu** *mtu-bytes*]
Parameter Description	*aging-mins*: Indicates the interval at which the MTU of a tunnel interface ages, in minutes. **infinite** indicates that the MTU never ages. *mtu-bytes*: Indicates the minimum value of the MTU. The value range is from 92 to 65535. The default value is 92.
Command Mode	Global configuration mode
Usage Guide	Use this command to dynamically monitor and automatically change MTUs of tunnel links. You can configure the monitoring frequency and the lower limit of MTU change. PMTU discovery has three states: ● **init**: Detection is not initiated. ● **learning**: Dynamic learning is in progress. ● **keep**: Dynamic MTU adjustment is completed and the next round of adjustment is ready. PMTU discovery depends on the "ICMP Packet Too Big" error packet returned by a device. If the packet is filtered by an intermediate device, discovery results will be inaccurate.

Configuration Example

Configuring PMTU Discovery

Configuration Steps	● Configure PMTU discovery.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config)# tunnel mode ipv6ip`
	`Hostname(config)# tunnel path-mtu-discovery`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`…`
	`Tunnel transport VPN is no set`
	`  Path MTU Discovery state:init, ager 10 mins, min MTU 92`

Common Errors

- PMTU discovery is enabled for automatic tunnels.

1.4.9 Configuring the Tunnel Encapsulation Limit

Configuration Effect

- Change the maximum number of nested encapsulations allowed by the outer protocol of a tunnel.

Notes

- In many cases, the tunnel encapsulation limit does not need to be changed.

Configuration Step

Configuring the Tunnel Encapsulation Limit

- By default, the device allows a maximum of four nested encapsulations of a packet, which can meet most service requirements.
- To change the limit, run the **tunnel nested-limit** *number* command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the tunnel encapsulation limit is configured.

Related Commands

Configuring the Tunnel Encapsulation Limit

Command	**tunnel nested-limit** *number*
Parameter Description	*number*: Indicates the maximum number of nested encapsulations of a packet. The value range is from 0 to 10. The default value is 4.
Command Mode	Interface configuration mode
Usage Guide	The device automatically discovers nested encapsulations and prevents excessive nested encapsulations. Only manual tunnels support the tunnel encapsulation limit, whereas automatic tunnels do not support it. The tunnel encapsulation limit is specific to a device and indicates the maximum number of times a packet is encapsulated from its entry to the device until its exit.

Configuration Example

Configuring the Tunnel Encapsulation Limit

Configuration Steps	● Configure the tunnel encapsulation limit.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config-if-Tunnel 1)# tunnel mode ipv6ip`
	`Hostname(config-if-Tunnel 1)# tunnel nested-limit 8`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`……`
	`Tunnel attributes:`
	`  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable`
	`  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3`
	`  Tunnel config nested limit is 8, current nested number is 0`
	`  Tunnel protocol/transport ipv6ip`
	`  Tunnel transport VPN is VPN1`
	`……`

Common Errors

- The tunnel encapsulation limit is configured for automatic tunnels.

1.4.10 Configuring Tunnel Data Validity Check

Configuration Effect

- Configure tunnel data validity check to determine whether data carried by tunnels is changed during transmission. If data is changed, the device considers the data as corrupted and discards it. If application of data carried by a tunnel do not support validity check, you can enable data validity check of the tunnel.

Notes

- Only GRE tunnels support data validity check.

Configuration Step

Configuring Tunnel Data Validity Check

- Optional.
- If application protocols do not support data validity check, you can enable data validity check of GRE tunnels.
- To enable tunnel data validity check, run the **tunnel checksum** command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether tunnel data validity check is enabled.

Related Commands

Configuring Tunnel Data Validity Check

Command	**tunnel checksum**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Use this command to enable data validity check of a GRE tunnel if service data carried in the GRE tunnel does not support validity check. Data validity check must be configured on both ends of a tunnel. The sender adds the checksum to an encapsulated packet. The receiver calculates the checksum of the packet and compares it to the checksum provided by the sender. If they are consistent, the packet is valid. Otherwise, the packet is invalid.

Configuration Example

Configuring Tunnel Data Validity Check

Configuration Steps	• Configure data validity check in a tunnel.
	`Hostname# configure terminal`

	Hostname(config)# interface tunnel 1 Hostname(config-if-Tunnel 1)# tunnel mode gre ip Hostname(config-if-Tunnel 1)# tunnel checksum
Verification	● Check the configuration of the tunnel interface.

	Hostname# show interfaces tunnel 1
	……
	Tunnel attributes:
	  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable
	  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3
	  Tunnel config nested limit is 8, current nested number is 0
	  Tunnel protocol/transport gre ip
	  Key disabled, Sequencing disabled
	  Checksumming of packets enabled
	  Tunnel transport VPN is VPN1
	……

Common Errors

- Data validity check is configured for regular tunnels (non-GRE tunnels).

1.4.11 Configuring a Tunnel Key

Configuration Effect

- By configuring the key of a tunnel interface, the device can ensure security of both ends of the tunnel and prevents malicious probes and attacks.

Notes

- Each packet encapsulated in the GRE format contains the configured key, but the attempt to ensure security through the key is inconsiderate.
- Both ends of a tunnel must use the same key settings.

Configuration Step

↘ Configuring a Tunnel Key

- Optional.
- You can configure different keys to segregate the data carried in a GRE tunnel.
- To configure a tunnel key, run the **tunnel key** *key-value* command in tunnel interface configuration mode.

Verification

- Run the **show interfaces tunnel** command to check whether the tunnel key is configured.

Related Commands

↘ Configuring a Tunnel Key

Command	**tunnel key** *key-value*

Parameter Description	*key-value*: Indicates the value of a tunnel key. The value range is from 0 to 2147483647.
Command Mode	Interface configuration mode
Usage Guide	The sender encapsulates the key in a packet. The receiver compares the local key to the key in the packet. If they are inconsistent, the packet is discarded.

Configuration Example

Configuring a Tunnel Key

Configuration Steps	● Configure a tunnel key.

	`Hostname# configure terminal`
	`Hostname(config)# interface tunnel 1`
	`Hostname(config-if-Tunnel 1)# tunnel mode gre ip`
	`Hostname(config-if-Tunnel 1)# tunnel key 10`

Verification	● Check the configuration of the tunnel interface.

	`Hostname# show interfaces tunnel 1`
	`……`
	`Tunnel attributes:`
	`  Tunnel source 1.1.1.1, destination UNKNOWN, unrouteable`
	`  Tunnel TOS/Traffic Class 0x2, Tunnel TTL 3`
	`  Tunnel config nested limit is 8, current nested number is 0`
	`  Tunnel protocol/transport gre ip`
	`    Key 0xa, Sequencing disabled`
	`    Checksumming of packets enabled`
	`   Tunnel transport VPN is VPN1`
	`……`

Common Errors

- Tunnel keys are configured for regular tunnels (non-GRE tunnels).

1.5 Monitoring

Displaying

Command	Description
show interfaces tunnel *number*	Displays the information about a tunnel interface.
show tunnel statistics	Displays the configurable tunnel capacity and the number of used tunnels.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug tunnel	Enables tunnel interface debugging.

1 Configuring TCP

1.1 Overview

The Transmission Control Protocol (TCP) is a transport-layer protocol providing reliable connection-oriented and IP-based services 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 through TCP. The Maximum Segment Size (MSS) is typically limited by the Maximum Transmission Unit (MTU) of the data link layer. Then packets are sent to the IP layer and then to the TCP layer of a receiver through the network.

TCP assigns a sequence number to each byte to prevent packet loss. 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 the specified 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. Unidentified packets 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 Exception	TCP checks whether the peer works normally.

1.2.1 Optimizing TCP Performance

Scenario

For example, a TCP connection is established between A and D, as shown in Figure 1-1. 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, avoid packet fragmentation between B and C.

Figure 1-1



Deployment

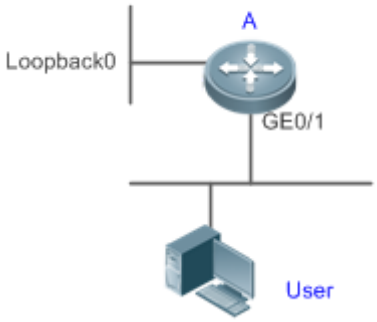
- Enable PMTUD on A and D.

1.2.2 Detecting TCP Connection Exceptions

Scenario

In Figure 1-2, a user logs in to A through Telnet but the user's computer is shut down abnormally. In case of TCP retransmission timeout, the user's TCP connection remains for a long period. Therefore, TCP keepalive can be used to rapidly detect TCP connection exceptions.

Figure 1-2



Deployment

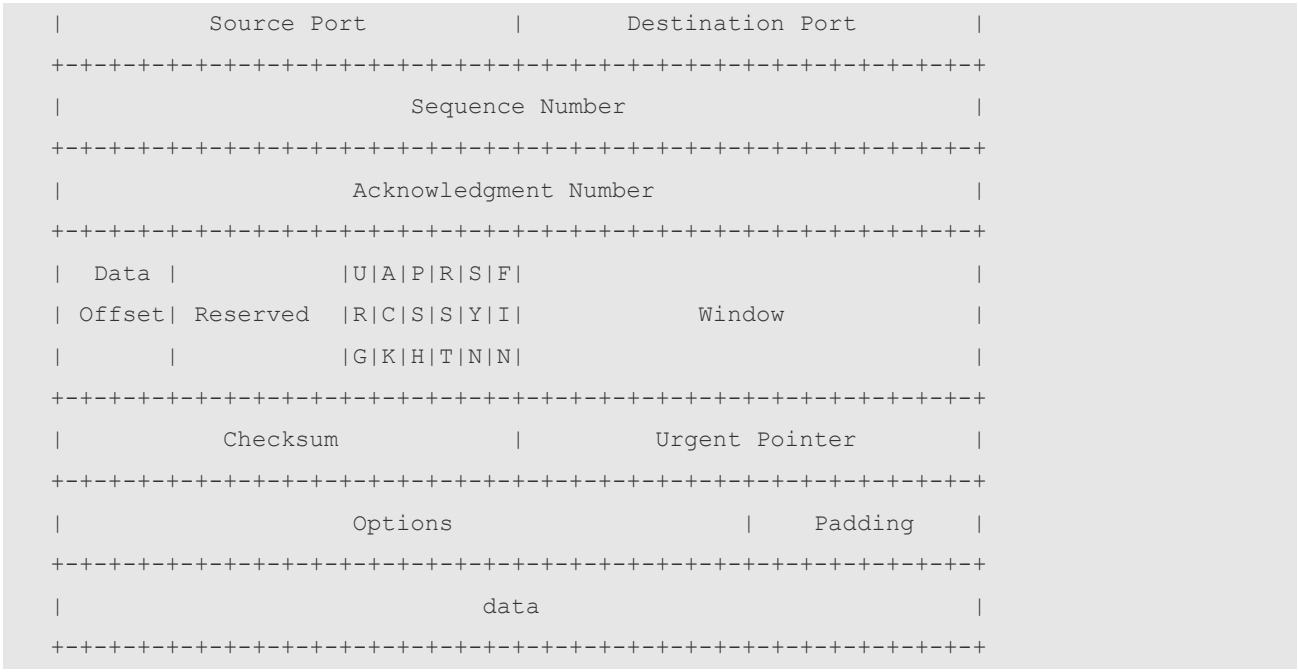
- Enable TCP keepalive on A.

1.3 Features

Basic Concepts

TCP Header Format

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



- **Source Port**: Is a 16-bit source port number.
- **Destination Port**: Is a 16-bit destination port number.
- **Sequence Number**: Is a 32-bit sequence number.
- **Acknowledgment Number**: Is a 32-bit number that identifies the next sequence number that the receiver is expecting to receive.
- **Data Offset**: Is a 4-bit number that indicates the total number of bytes in the TCP header (option included) divided by 4.
- A flag bit is 6-bit. URG indicates that the urgent pointer field is significant; ACK indicates that the acknowledgment field is significant; PSH indicates the push function; RST indicates that the TCP connection is reset; SYN indicates that the sequence number is synchronized (used during TCP connection establishment); FIN indicates that the sender does not have data to be sent (used during TCP connection termination).
- **Window**: Is of 16 bits. 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 indicates the offset of urgent data relative to the sequence number. It is available only when URG is set.

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	Configures a timeout waiting for a response packet after an SYN or SYN ACK packet is sent.
Configuring the Window Size	Configures a window size.
Configuring Reset Packet Sending	Configures the device to send TCP reset packets after receiving port unreachable packets.
Configuring the MSS	Configures an MSS for a TCP connection.
Configuring the MSS for SYN Packet	Changes the MSS in an SYN packet.
PMTU	Discovers the smallest MTU on the TCP transmission path, and adjusts the size of TCP packets based on the MTU to avoid fragmentation.
TCP Keepalive	Checks 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 a specified number of times or until the 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 a specified number of times or until the timeout period expires. (This occurs in the case of SYN flooding.)

Related Configuration

Configuring the 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. The value range is from 5 to 300, in seconds.
- In case of SYN flooding, shortening the SYN timeout reduces consumed resources. However, this mechanism is invalid for continuous SYN flooding. When a device proactively requests to establish a connection with an external device, for example, through Telnet, shortening the SYN timeout reduces user's waiting time. You may prolong the SYN timeout properly on un unstable network.

The **ip tcp syntime-out** command in version 10.x is not used but is 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 the 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 the connection involves high bandwidth and much data, increasing the window size dramatically enhances TCP transmission performance.

Related Configuration

Configuring the Window Size

- Run the **ip tcp window-size** *size* command in global configuration mode to configure a window size. The value range is from 128 to 10737418240 (65535<< 14), in bytes. The default value is 65535 bytes. If the window size is greater than 65535 bytes, window increasing 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 that 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 packets to attack the device.

Related Configuration

Configuring the Device to Send TCP Reset Packets After Receiving Port Unreachable Packets

By default, the device is enabled to send TCP reset packets upon receiving port unreachable packets.

Run the **no ip tcp send-reset** command in global configuration mode to disable the device from sending TCP reset packets upon receiving port unreachable packets.

After this function is enabled, attackers may use port unreachable packets to attack the device.

The **ip tcp not-send-rst** command in version 10.x is not used 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 the MSS

Working Principle

The MSS refers to the total amount of data contained in a TCP segment excluding TCP options.

Three-way handshake is implemented through MSS negotiation. Both parties add the MSS option to SYN packets, indicating the largest amount of data that the local end can handle, namely, the amount of data allowed from the peer. Both parties use the smaller MSS between them as the advertised MSS.

The MSS is calculated as follows:

- IPv4 TCP: MSS = Outbound interface's MTU – IP header size (20-byte) – TCP header size (20-byte)
- IPv6 TCP: MSS = IPv6 PMTU – 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** considered) should be deducted from an MSS. For example, 20 bytes for MD5 digest (with **data offset** considered) should be subtracted from the MSS.

Related Configuration

Configuring the MSS

- Run the **ip tcp mss** *max-segment-size* command in global configuration mode to set an MSS. The value range is from 68 to 1000, in bytes. By default, the MSS is calculated based on the MTU. If an MSS is configured, the effective MSS is the smaller one between the calculated MSS and the configured MSS.
- A small MSS reduces transmission performance. You can promote TCP transmission by increasing the MSS. Choose an MSS by referring to the interface's MTU. If the former is larger, TCP packets will be fragmented and transmission performance will be lowered.

1.3.5 Configuring the MSS for SYN Packets

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 Figure 1-3, 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. Change the MSS in SYN packets on interfaces (1) and (2) of R2 to enable TCP packets to pass R1 and R2.

Figure 1-3



Related Configuration

Configuring the MSS for TCPv4 SYN Packets

- By default, the MSS in TCPv4 SYN packets is not changed.
- Run the **ip tcp adjust-mss** *max-segment-size* command in interface configuration mode to set the MSS. The value range is from 500 to 1460, in bytes.
- To avoid packet fragmentation in the case of a small PMTU, you may configure the 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 considering the interface MTU.

This configuration applies to a new connection but is invalid for an existing TCP connection.

Configuring the MSS for TCPv6 SYN Packets

- By default, the MSS in TCPv6 SYN packets is not changed.
- Run the **ipv6 tcp adjust-mss** *max-segment-size* command in interface configuration mode to configure the MSS for TCPv6 SYN packets. The value range is from 1220 to 1440, in bytes.
- To avoid packet fragmentation in the case of a small PMTU, you may configure the 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 considering the interface MTU.

This configuration applies to a new TCPv6 connection but is invalid for an existing TCPv6 connection.

1.3.6 PMTUD

Working Principle

The Path MTU Discovery (PMTUD) stipulated in RFC 1191 is used to discover the smallest MTU in a TCP path to avoid fragmentation, enhancing network bandwidth utilization. The process of TCPv4 PMTUD 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 outbound interface's MTU 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.

4 The size of subsequent data segments sent by the source will not surpass the MSS, which is calculated as follows:

TCP MSS = PMTU – IP header size – TCP header size

Related Configuration

Enabling PMTUD

By default, PMTUD 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

Working Principle

You may enable TCP keepalive to check whether the peer works normally. If a peer end does not send packets to the local end for a period of time (namely idle period), the local end starts sending keepalive packets successively to the peer end for several times. If no response packet is received, the TCP connection is considered inactive and then ended.

Related Configuration

Enabling Keepalive

- By default, TCP keepalive is disabled.

- Run the **ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*] command to in global configuration mode to enable TCP keepalive.

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.

1.4 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 device to send TCP reset packets after receiving port unreachable packets.
	ip tcp mss	Configures the MSS for TCP connections.
	ip tcp adjust-mss	Configures the MSS for TCPv4 SYN packets.
	ipv6 tcp adjust-mss	Configures the MSS for TCPv6 SYN packets.
	ip tcp path-mtu-discovery	Enables PMTUD.
Detecting TCP Connection Exception	(Optional) It is used to detect whether the peer 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 Step

Configuring the SYN Timeout

- Optional.
- Perform this configuration on both ends of a TCP connection.

Configuring TCP Window Size

- Optional.
- Perform this configuration on both ends of a TCP connection.

Configuring the Device to Send TCP Reset Packets After Receiving Port Unreachable Packets

- Optional.
- Perform this configuration on both ends of a TCP connection.

Configuring MSS

- Optional.
- Perform this configuration on both ends of a TCP connection.

Configuring the MSS for TCPv4 SYN Packets

- Optional.
- If the MTU between two routers in TCP transmission is small, you may configure the MSS on the routers.

Configuring the MSS for TCPv6 SYN Packets

- Optional.
- If the MTU between two routers in TCPv6 transmission is small, you may configure the MSS on the routers.

Enabling PMTUD

- Optional.
- Perform this configuration on both ends of a TCP connection.

Verification

N/A

Related Commands

Configuring SYN Timeout

Command	**ip tcp synwait-time** *seconds*
Parameter Description	*seconds*: Indicates the SYN packet timeout, in seconds. The value range is from 5 to 300. The default value is 20 seconds.
Command Mode	Global configuration mode
Usage Guide	In case of SYN flooding, shortening the SYN timeout reduces consumed resources. However, this mechanism is invalid for continuous SYN flooding. When a device proactively requests to establish a connection with an external device, for example, through Telnet, shortening the SYN timeout reduces user's waiting time. You may prolong the SYN timeout properly on un unstable network.

Configuring TCP Window Size

Command	**ip tcp window-size** *size*
Parameter Description	*size*: Indicates a TCP window size, in bytes. The value range is from 128 to 10737418240 (65535<< 14). The default value is 65535 bytes.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Device to Send TCP Reset Packets After Receiving Port Unreachable Packets

Command	**ip tcp send-reset**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the device is enabled to send TCP reset packets upon receiving port unreachable packets.

Configuring the MSS

Command	**ip tcp mss** *max-segment-size*
Parameter Description	*max-segment-size*: Indicates the maximum segment size, in bytes. The value range is from 68 to 10000. By default, the MSS is calculated based on the MTU.
Command Mode	Global configuration mode
Usage Guide	This command defines the MSS for a TCP connection 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 MSS for TCPv4 SYN Packets

Command	**ip tcp adjust-mss** *max-segment-size*
Parameter Description	*max-segment-size*: Indicates the maximum segment size, in bytes. The value range is from 500 to 1460.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the MSS for TCPv6 SYN Packet

Command	**ipv6 tcp adjust-mss** *max-segment-size*
Parameter Description	*max-segment-size*: indicates the maximum segment size, in bytes. The value range is from 1220 to 1440.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring PMTUD

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 PMTU is discovered, in minutes. The value range is from 10 to 30. The default value is 10 minutes. **age-timer infinite**: No probe is implemented after a PMTU is discovered.
Command Mode	Global configuration mode
Usage Guide	PMTUD is defined in RFC 1191 to improve bandwidth utilization. When TCP is applied to bulk data transmission, this function can enhance transmission performance. According to RFC 1191, after discovering the PMTU, TCP can use a larger MSS after a certain period to probe for a new PMTU. This interval is specified by the **age-timer** parameter. When the device detects that the PMTU is smaller than the MSS negotiated by both ends of the TCP connection, the

	device will attempt to discover a larger PMTU according to the configured interval. This probe process will continue until the PMTU reaches the MSS, or until the timer is stopped manually. To stop the timer, use the **age-timer infinite** parameter.

Configuration Example

↘ Enabling PMTUD

Configuration Steps	● Enable PMTUD for a TCP connection. Adopt the default age timer settings.

	`Hostname# configure terminal`
	`Hostname(config)# ip tcp path-mtu-discovery`
	`Hostname(config)# end`

Verification	● Run the **show tcp pmtu** command to display the IPv4 TCP PMTU.

	`Hostname# show tcp pmtu`
	`Number Local Address Foreign Address PMTU`
	`1 192.168.195.212.23 192.168.195.112.13560 1440`

	● Run the **show ipv6 tcp pmtu** command to display the IPv6 TCP PMTU.

	`Hostname# show ipv6 tcp pmtu`
	`Number Local Address Foreign Address PMTU`
	`1 1000::1:23 1000::2.13560 1440`

Common Errors

N/A

1.4.2 Detecting TCP Connection Exceptions

Configuration Effect

- Check whether the peer works normally.

Notes

N/A

Configuration Step

↘ Enabling TCP Keepalive

- Optional.

Verification

N/A

Related Commands

↘ Enabling TCP Keepalive

Command	**ip tcp keepalive** [**interval** *num1*] [**times** *num2*] [**idle-period** *num3*]

Parameter Description	**interval** *num1*: Indicates the interval for sending keepalive packets, in seconds. The value range is from 1 to120. The default value is 75 seconds. **times** *num2*: Indicates the maximum number of times for sending keepalive packets. The value range is from 1 to 10. The default value is 6. **idle-period** *num3*: Indicates the time when the peer sends no packets to the local end, in seconds. The value range is from 60 to 1800. 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. Assume that the TCP keepalive function is enabled, with the default interval, number of times, and idle period. The user device does not receive packets from the other end within 15 minutes and then starts sending Keepalive packets every 75 seconds for 6 times. If the user device receives no TCP packets, the TCP connection is considered inactive and then terminated.

Configuration Example

↘ Enabling TCP Keepalive

Configuration Steps	● Enable TCP keepalive on a device with **interval** and **idle-period** set to 3 minutes and 60 seconds respectively. If the user device receives no TCP packets from the other end after sending keepalive packets four times, the TCP connection is considered inactive.

	`Hostname# configure terminal`
	`Hostname(config)# ip tcp keepalive interval 60 times 4 idle-period 180`
	`Hostname(config)# end`

Verification	● A user logs in to a device through Telnet, and then shuts down the local device. Run the **show tcp connect** command on the remote device to observe the time when IPv4 TCP connection is deleted.

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show tcp connect [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]	Displays basic information on IPv4 TCP connections.
show tcp connect statistics	Displays IPv4 TCP connection statistics.
show tcp pmtu [**local-ip** *a.b.c.d*] [**local-port** *num*] [**peer-ip** *a.b.c.d*] [**peer-port** *num*]	Displays IPv4 TCP PMTU.
show tcp port [*num*]	Displays IPv4 TCP port information.
show tcp parameter	Displays TCP parameters.
show tcp statistics	Displays TCP statistics.

Command	Description
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 basic information on IPv6 TCP connections.
show ipv6 tcp connect statistics	Displays IPv6 TCP connection statistics.
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 PMTU.
show ipv6 tcp port [*num*]	Displays IPv6 TCP port information.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
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 debugging information on IPv4 TCP packets.
debug ip tcp transactions [**local-ip** *a.b.c.d*] [**peer-ip** *a.b.c.d*] [**local-port** *num*] [**peer-port** *num*]	Displays debugging information on IPv4 TCP connections.
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 packets.
debug ipv6 tcp transactions [**local-ipv6** *X:X:X:X::X*] [**peer-ipv6** *X:X:X:X::X*] [**local-port** *num*] [**peer-port** *num*]	Displays debugging information on IPv6 TCP connections.

1 Configuring IPv4/IPv6 REF

1.1 Overview

On the device that do not support hardware-based forwarding, IPv4 and IPv6 packets are forwarded by software. The device uses the IPv4/IPv6 Ruijie Express Forwarding (REF) technology to optimize the forwarding performance of software.

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 contains link layer information for the next hop.

REF is used to proactively resolve next hops and implement load balancing.

Protocols and Standards

N/A

1.2 Applications

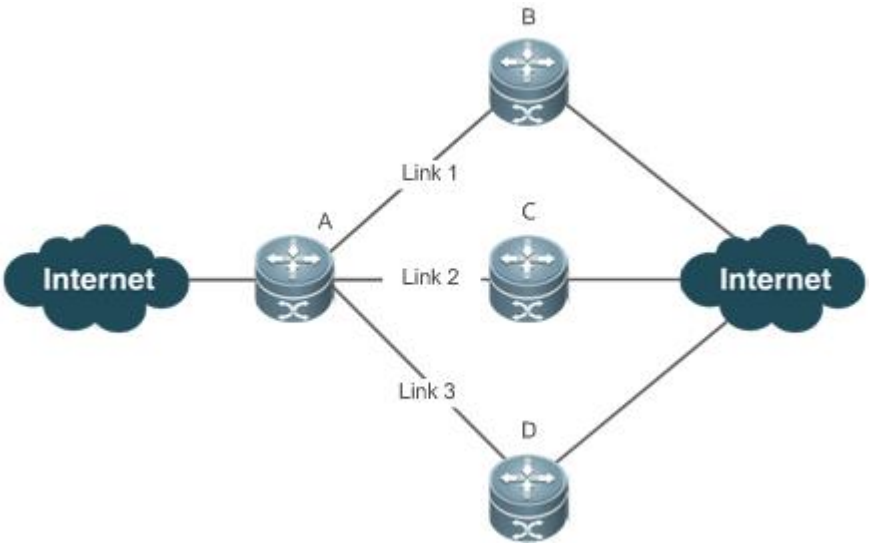
Application	Description
Load Balancing	During network routing, when a route prefix is associated with multiple next hops, REF can implement load balancing among multiple next hops.

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 source and destination IP addresses.

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 topology information. During packet forwarding, IPv4/IPv6 REF selects packet transmission paths based on the routing table.

Adjacent Node

An adjacent node contains outbound interface information about routed packets, for example, next hop, next component to be processed, and link layer encapsulation. When a packet is matched with an adjacent node, the packet is directly encapsulated and then forwarded. An adjacent node table is often organized into a hash table to facilitate query and update; next hop information is organized into a load balancing entry to support load balancing. 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.

Proactive Resolution

REF supports next hop resolution. If the MAC address of the next hop is unknown, REF will proactively resolve the next hop. IPv4 REF requests the ARP module for next hop resolution, while IPv6 REF applies the ND module for 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.

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, that is, a multi-path route is used. The route will be associated with a load balancing table and implement weight-based load balancing. When an IPv4/IPv6 packet is matched with a load balancing 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 types of load balancing policies: load balancing based on destination IP address and 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 IPv4 destination addresses.
- Run the **ip ref load-sharing** { **original** | **original**-**only** } command to configure load balancing.
- Then load balancing is implemented based on IPv4 source and destination addresses.

Configuring Load Balancing Based on IPv6 Source and Destination Addresses

- By default, load balancing is implemented based on IPv6 destination addresses.
- Run the **ipv6 ref load-sharing original** command to configure the load balancing.
- Then load balancing is implemented based on 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	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 types of load balancing policies:

- Destination address-based load balancing indicates performing hash calculation based on the destination address of a packet. The path with a greater weight is more likely to be selected. This policy is used by default.
- Load balancing based on source and destination addresses indicates hash calculation based on source and destination addresses of a packet. The path with a greater weight is more likely to be selected.

Notes

N/A

Configuration Step

- Optional.
- Perform this configuration if you want to implement load balancing based on 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

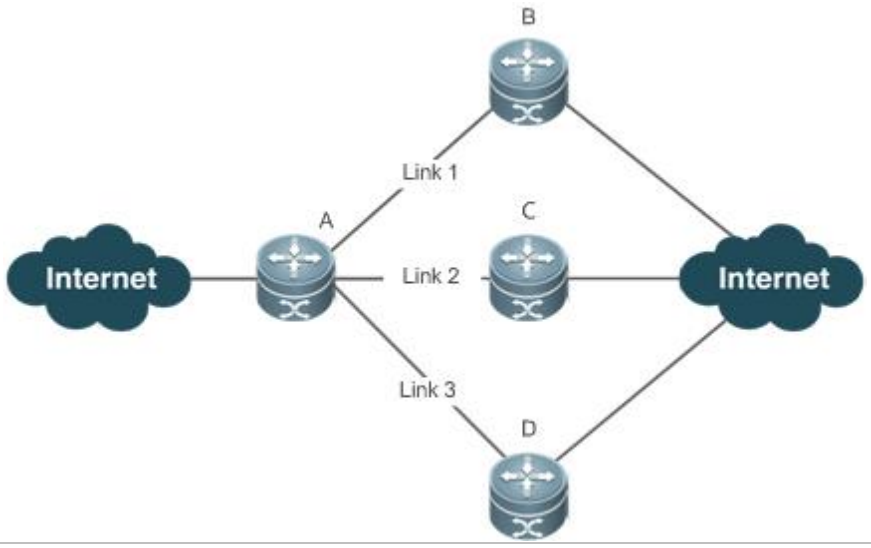
Command	**ip ref load-sharing** { **original** | **original-only** }
Parameter Description	**Original**: Configures load balancing based on IPv4 source and destination addresses. **original-only**: Configures load balancing based on IPv4 source addresses.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Load Balancing Based on IPv6 Source and Destination Addresses

Command	**ipv6 ref load-sharing original**
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`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`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.

Command	Description
show ip ref packet statistics	Displays IPv4 REF packet statistics.
clear ip ref packet statistics	Clears IPv4 REF packet statistics.
show ipv6 ref packet statistics	Displays IPv6 REF packet statistics.
clear ipv6 ref packet statistics	Clears IPv6 REF packet statistics.

Displaying Adjacency Information

You can run the following commands to display adjacency information.

Command	Description
show ip ref adjacency [**glean** | **local** | *ip-address* | **interface** *interface_type interface_number* | **discard** | **statistics**]	Displays gleaned adjacencies, local adjacencies, adjacencies of a specified IP address, adjacencies associated with a specified interface, and all adjacent nodes in IPv4 REF.
show ipv6 ref adjacency [**glean** | **local** | *ipv6-address* | **interface** *interface_type interface_number* | **discard** | **statistics**]	Displays gleaned adjacencies, local adjacencies, adjacencies of a specified IPv6 address, adjacencies associated with a specified interface, and all adjacent nodes in IPv6 REF.

Displaying Active Resolution Information

You can run the following commands to display next hops to be resolved.

Command	Description
show ip ref resolve-list	Displays the next hop to be resolved .
show ipv6 ref resolve-list	Displays the next hop to be resolved.

Displaying Packet Forwarding Path Information

Packets are forwarded based on their IPv4/IPv6 addresses. If 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, sent to a CPU, or forwarded. Furthermore, the interface that forwards the packet is displayed.

Command	Description
show ip ref exact-route *source-ipaddress destination_ipaddress*	Displays the forwarding path of a packet. oob indicates the out-of-band management network.
show ipv6 ref exact-route *source-ipv6-address destination-ipv6-address*	Displays the forwarding path of an IPv6 packet. oob indicates the out-of-band, management network.

Displaying Route Information in an REF Table

Run the following commands to display route information in an REF table.

Command	Description
show ip ref route [**default** | {*ip-address mask*}| **statistics**]	Displays route information in the IPv4 REF table. The parameter **default** indicates a default route. oob indicates the out-of-band management network.
show ipv6 ref route [**default** | **statistics** | *prefix/len*]	Displays route information in the IPv6 REF table. The parameter **default** indicates a default route. oob indicates the out-of-band management network.

1 Configuring FPM

1.1 Overview

The flow platform (FPM) is designed to accelerate packet processing. By identifying flow attributes of IP packets before service processing, the FPM enhances the efficiency of service handling. As a core component of the system, the FPM is initialized at startup. This document provides configuration commands for configuring and managing the FPM. Typically, the default configuration of the FPM is sufficient to meet practical needs.

The following sections describe the FPM only.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Configuring the Packet Receiving Threshold	When the device receives a large number of repeated TCP connection requests on a local area network (LAN), perform FPM configuration to effectively defend against such attacks.
Configuring Loose TCP Status Check	Perform an active/standby switchover in the AS environment.

1.2.1 Configuring the Packet Receiving Threshold

Scenario

When the device receives a large number of repeated TCP connection requests on a LAN, no valid connection can be established if the device cannot receive any handshake response packet from the peer. In this case, attacks may occur. You can perform FPM configuration to restrict the number of TCP connection requests, so as to effectively defend against such attacks.

Protocols

- Enable the strict packet status tracing function on the forwarding device.
- Configure a low TCP-SYN-SENT packet threshold.

1.2.2 Configuring Loose TCP Status Check

Scenario

Loose TCP status check needs to be configured on the device to prevent flow interruption during an active/standby switchover of the device. Then a connection can be established and packets can be forwarded as long as one end sends an ACK packet, so that the connection is not interrupted during the active/standby switchover.

Protocols

- Configure loose TCP status check on the backup device.

1.3 Features

Basic Concepts

Flow Entry

A flow entry is a physical resource for the device to identify and manage all connections of an IP session, and records basic information about the current IP session. The corresponding protocols include Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Raw Internet Protocol (RAWIP).

Overview

Feature	Description
Transparent Transmission of Packets When the Flow Table Is Full	Ensures that existing flows are not interrupted when the flow table is full.
Flow Entry Aging	Reclaims invalid flow entries.
Number of Packets Permitted in a Flow	Prevents IP packet flooding attacks.
TCP Status Tracing	Filters out packets on invalid TCP connections.
Loose TCP Status Check	Allows establishment of a connection with only ACK packets.

1.3.1 Transparent Transmission of Packets When the Flow Table Is Full

Working Principle

Acceleration of IP service processing relies on a flow table. Flow table resources are configured based on the device hardware configuration and typically meet application requirements. However, in extreme environments, flow table resources may be exhausted, preventing new flows from being established. With this feature, when the flow table is full, packets are transparently transmitted without establishing any flow on the device, and service processing is not accelerated. This approach ensures that service flows are not interrupted.

1.3.2 Flow Entry Aging

Working Principle

Aging of a flow entry occurs when the device proactively withdraws the flow entry after a specified period of inactivity. This mechanism helps address the issue of flow table saturation, which can prevent new sessions from being established during a session attack. To manage this, the flow table aging feature is used. The aging time should be adjusted based on the type of data and the state of the flows. For instance, the aging time for a TCP flow in the SYN state differs from that of a TCP flow in ESTABLISHED state. In cases such as port scanning attacks, where system resources are consumed by numerous connections, configuring appropriate aging time values for different flow states can help efficiently reclaim flow entries and prevent interruptions. Setting the right aging time helps reduce unnecessary flow entries while still supporting the exchange of service data flows.

1.3.3 Number of Packets Permitted in a Flow

Working Principle

A count of the number of packets processed for each flow in its current state is maintained. By configuring the number of packets allowed through for each flow state, you can effectively address the issue of other packets not being processed in a timely manner during high-volume attacks of a particular type of packet, thus ensuring the exchange of service data flows.

1.3.4 TCP Status Tracing

Working Principle

A complete handshake process is required for establishment of a TCP connection; otherwise, the connection is invalid or packets are attack packets. The FPM needs to trace the state of TCP connections, so as to distinguish flows that are established over TCP session connections in various states and determine whether the connections are valid. In some special scenarios such as asymmetrical routing, the state of TCP connections cannot be traced and this function should be disabled.

1.3.5 Loose TCP Status Check

Working Principle

A complete handshake process is required for establishment of a valid TCP connection. In some cases such as active/standby switchover, however, a handshake process may have been performed for the current TCP connection but no corresponding information exists. In such cases, the system requires only ACK packets. In this case, 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 disable the device from transparently transmitting packets when the flow table is full.	
	ip session direct-trans-disable	Disables the device from transparently transmitting packets when the flow table is full.
Configuring the Flow Entry Aging Time	(Optional) It is used to configure the aging time.	
	ip session timeout	Configures the flow entry aging time.
Configuring the Number of Packets Permitted in a Flow	(Optional) It is used to configure the number of packets that can be received for each flow in certain state.	
	ip session threshold	Configures the number of packets that can be received for each flow in certain state.
Enabling the TCP Status Tracing Function	(Optional) It is used to enable the TCP status tracing function.	
	ip session tcp-state-inspection-enable	Enables the TCP status tracing function.
Configuring Loose TCP Status Check	(Optional) It is used to enable the loose TCP status transition check function.	

Configuration	Description and Command	
	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 devices, the FPM should not allow transparent transmission of packets when no flow is established.

Notes

- By default, packets can be transparently transmitted without flow establishment when the flow table is full.

Configuration Step

- Optional.
- 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 running-config** command to check whether the configuration includes **ip session direct-trans-disable**. If not, the transparent transmission function is enabled.

Configuration Example

Scenario	If the NAT service is required on the wireless device, you need to disable the transparent transmission function because the NAT service does not allow 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 running-config** 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

- Make use of system flow table resources so as to reduce invalid 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 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 later than the configured aging time.

Configuration Step

Configuring the Aging Time

- Optional.
- 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. A longer aging time indicates a longer 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 state, which is 10 seconds by default and ranges from 5 to 60. **icmp-connected**: Sets the aging time of ICMP flows in connected state, which is 10 seconds by default and ranges from 5 to 120. **icmp-started**: Sets the aging time of ICMP flows in started state, which is 10 seconds by default and ranges from 5 to 120. **rawip-closed**: Sets the aging time of RAWIP flows in closed state, which is 10 seconds by default and ranges from 5 to 60. **rawip-connected**: Sets the aging time of RAWIP flows in connected state, which is 300 seconds by default and ranges from 10 to 300. **rawip-established**: Sets the aging time of RAWIP flows in established state, which is 300 seconds by default and ranges from 10 to 600. **rawip-started**: Sets the aging time of RAWIP flows in started state, 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 state, which is 60 seconds by default and ranges from 10 to 120. **tcp-closed**: Sets the aging time of TCP flows in tcp-closed state, which is 10 seconds by default and ranges from 5 to 20.

	tcp-established: Sets the aging time of TCP flows in tcp-established state, 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-wait1 state, 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-wait2 state, 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 state, 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 state, 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 state, 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 state, which is 10 seconds by default and ranges from 5 to 60. **udp-closed**: Sets the aging time of UDP flows in closed state, which is 10 seconds by default and ranges from 5 to 60. **udp-connected**: Sets the aging time of UDP flows in connected state, which is 30 seconds by default and ranges from 10 to 300. **udp-established**: Sets the aging time of UDP flows in established state, which is 600 seconds by default and ranges from 120 to 600. **udp-started**: Sets the aging time of UDP flows in started state, which is 10 seconds by default and ranges from 10 to 300. **num**: Sets the aging time
Defaults	Default values are used by default.
Command Mode	Global configuration mode
Usage Guide	Use the **no** form of the command to restore the default aging time.

Verification

- Use the **show running-config** command to check whether the configuration includes **ip session timeout**. If not, 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 forwarding device, you can shorten the aging time of the UDP-established flows to improve aging efficiency.
Configuration Steps	If the firewall card is used for forwarding, set the aging time of flows in udp-established state to 120 seconds.
	`Hostname# configure terminal` `Hostname(config)# ip session timeout udp-established 120`
Verification	The aging time should be 120 seconds. Use the **show running-config** command to verify that the configuration contains the following item: `ip session timeout udp-established 120` This indicates that the aging time is 120s.

Common Errors

N/A

1.4.3 Configuring the Number of Packets Permitted in a Flow

Networking Requirements

- By configuring the number of packets allowed through for each flow state, you can effectively address the issue of other packets not being processed in a timely manner during high-volume attacks of a particular type of packet, thus ensuring the exchange of service data flows.

Notes

- There is a default packet count upon system initialization, which can meet requirements in most scenarios. Therefore, the configuration is optional.
- The check function is disabled by default. To enable the check function, you need to configure packet threshold check for flows in various states first.

Configuration Step

- Optional.
- By default, a flow is determined 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** [*dev*] [*slot*] **threshold** command to change the number of packets allowed to pass in the corresponding flow. A greater value indicates 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 state, which is 10 by default and ranges from 1 to 2000000000. **icmp-started**: Sets the number of packets permitted to pass in each ICMP flow in started state, which is 300 by default and ranges from 5 to 2000000,000. **rawip-closed**: Sets the number of packets permitted to pass in each RAWIP flow in closed state, which is 10 by default and ranges from 1 to 2000000000. **tcp-syn-sent**: Sets the number of packets permitted to pass in each TCP flow in syn-send state, which is 10 by default and ranges from 10 to 2000000,000. **tcp-syn-receive**: Sets the number of packets permitted to pass in each TCP flow in syn-receive state, which is 20 by default and ranges from 5 to 2000000000. **tcp-closed**: Sets the number of packets permitted to pass in each TCP flow in closed state, which is 20 by default and ranges from 5 to 2000000000. **udp-closed**: Sets the number of packets permitted to pass in each UDP flow in closed state, which is 10 by default and ranges from 1 to 2000000000. *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 running-config** command to check whether the configuration includes **ip session threshold**. If not, the default values about the number of packets permitted to pass is used.

Configuration Example

Scenario	When a large number of ping packets exist on a network, a flooding attack may occur. You can configure the number of packets permitted to pass in each ICMP flow in icmp-started state, so as to deny such ping packets.
Configuration Steps	If a firewall card is used for forwarding, set the number of packets permitted to pass in each ICMP flow in icmp-started state to 10.
	`Hostname# configure terminal` `Hostname(config)# ip session threshold icmp-started 10`
Verification	The number should be 10. Use the **show running-config** command to verify that the configuration contains the following item: `ip session threshold icmp-started 10` This indicates that the number of packets permitted to pass in each ICMP flow in icmp-started state is 10.

Common Errors

N/A

1.4.4 Enabling the TCP Status Tracing Function

Networking Requirements

- The TCP status tracing function needs to be enabled on corresponding devices.

Notes

- By default, the TCP status tracing function is disabled on devices.

Configuration Step

- Optional.
- The TCP status tracing function is disabled by default. You can use the **ip session tcp-state-inspection-enable** command to enable it.

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 default setting of the TCP status tracing function.

Verification

- Use the **show running-config** command to check whether the configuration includes **ip session tcp-state-inspection-enable**. If no, the TCP status tracing function is disabled.

Configuration Example

Scenario	The TCP status tracing function needs to be enabled on the wireless forwarding device.
Configuration Steps	Enable the TCP status tracing function on the device.
	`Hostname# configure terminal` `Hostname(config)# ip session tcp-state-inspection-enable`
Verification	Use the **show running-config** command to verify that the configuration includes **ip session tcp-state-inspection-enable**.

Common Errors

N/A

1.4.5 Configuring Loose TCP Status Check

Networking Requirements

- A flow can be directly established with only ACK packets.

Notes

- By default, a flow cannot be directly established for ACK packets on firewalls, and can be directly established for ACK packets on EG devices.
- This configuration is optional.

Configuration Step

- Optional.
- By default, the loose TCP status check function is disabled on firewalls. 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 devices.
- 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 running-config** command to check whether the configuration includes **ip session tcp-loose**. If not, the loose TCP status check function is disabled.

Configuration Example

Scenario	If the device functions as the firewall card of the backup device, an active/standby switchover is required. Perform this configuration on the backup device.
Configuration Steps	Enable the loose TCP status check function on the device.
	`Hostname# configure terminal` `Hostname(config)# ip session tcp-loose`
Verification	Use the **show running-config** command to verify that the configuration includes **ip session tcp-loose**.

Common Errors

N/A

1.5 Monitoring

Clearing

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

Command	Function
clear ip fpm counters	Clears counters about IPv4 packets.
clear ip v6fpm counters	Clears counters about IPv6 packets.

Displaying

Command	Function
show ip fpm counters	Displays the counters about the IPv4 packets.
show ip v6fpm counters	Displays the counters about the IPv6 packets.
show ip fpm flows	Displays IPv4 packet flow information.
show ip fpm flows filter	Displays IPv4 packet flow information except specific IPv4 packet flows.
show ip v6fpm flows	Displays IPv6 packet flow information.
show ip fpm statistics	Displays IPv4 flow statistics.
show ip v6fpm statistics	Displays IPv6 flow statistics.

1 Configuring SAVI

1.1 Overview

Source Address Validation Improvement (SAVI) establishes binding entries between the source IPv4/IPv6 addresses and anchors (or source MAC addresses and port numbers of access devices) for access devices through Control Packet Snooping (CPS) so as to verify the source addresses of IP packets through a specified interface. The records in the binding table are sourced from ND snooping, DHCPv6 snooping, and the static address configuration. Only packets whose source addresses match binding entries will be forwarded. This ensures the authenticity of source addresses of data packets over the network.

This document mainly describes the application of SAVI over IPv6 networks in stateful address configuration (typically DHCPv6), stateless address autoconfiguration (SLAAC), and static address configuration scenarios.

Protocols and Standards

- RFC 3315: Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 4861: Neighbor Discovery for IP version 6
- RFC 4862: IPv6 Stateless Address Autoconfiguration
- RFC 6959: SAVI Threat Scope
- RFC 6620: FCFS SAVI Improvement for Locally Assigned IPv6 Addresses
- RFC 8074: SAVI for Mixed Address Assignment Methods Scenario
- RFC 7039: SAVI Framework
- RFC 7513: Solution for DHCP

1.2 Applications

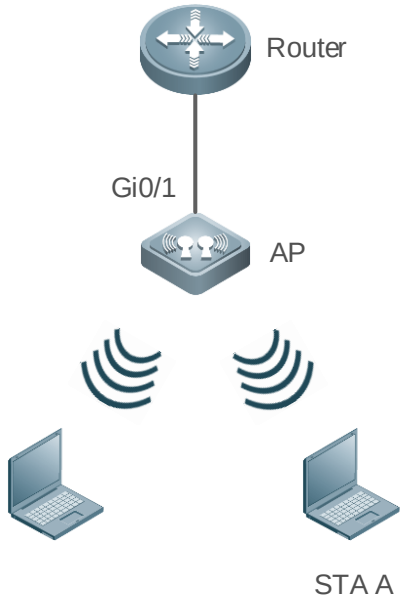
Application	Description
SLAAC-Only Scenario	Users use SLAAC to generate IPv6 addresses for communication.
DHCPv6-Only Scenario	Users use stateful address autoconfiguration to generate IPv6 addresses for communication.
SLAAC and DHCPv6 Hybrid Deployment Scenario	Users use stateful or stateless address autoconfiguration to generate IPv6 addresses for communication.

1.2.1 SLAAC-Only Scenario

Scenario

In this scenario, the hosts connect to the access device with SAVI enabled. The hosts can use only the addresses automatically configured through SLAAC for communication except the static address configured on the SAVI device.

Deployment



- Enable neighbor discovery (ND) snooping on device AP to monitor the SLAAC process.
- Configure uplink interface Gi0/1 on access device AP as an ND snooping trusted interface.
- Enable SAVI on access device AP and enable the device to receive SLAAC binding entries.
- Enable IPv6 packet filtering in the specified WLAN on the AP.

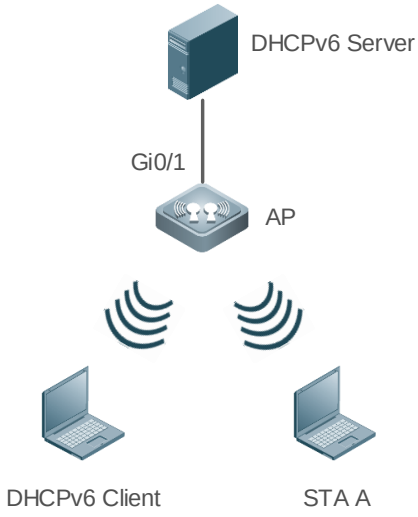
Notes	Device AP is enabled with SAVI. SLAAC User indicates a client whose IPv6 address is configured via SLAAC. STA A indicates a common client.

1.2.2 DHCPv6-Only Scenario

Scenario

In this scenario, the hosts connect to the access device with SAVI enabled. The hosts can use only the addresses dynamically obtained through DHCPv6 for communication except the static address configured on the SAVI device.

Deployment



- Enable DHCPv6 snooping on device AP to monitor the DHCPv6 process.
- Configure uplink interface Gi0/1 on access device AP as a DHCPv6 snooping trusted interface.
- Enable SAVI on access device AP and enable the device to receive DHCPv6 binding entries.
- Enable IPv6 packet filtering in the specified WLAN on the AP.

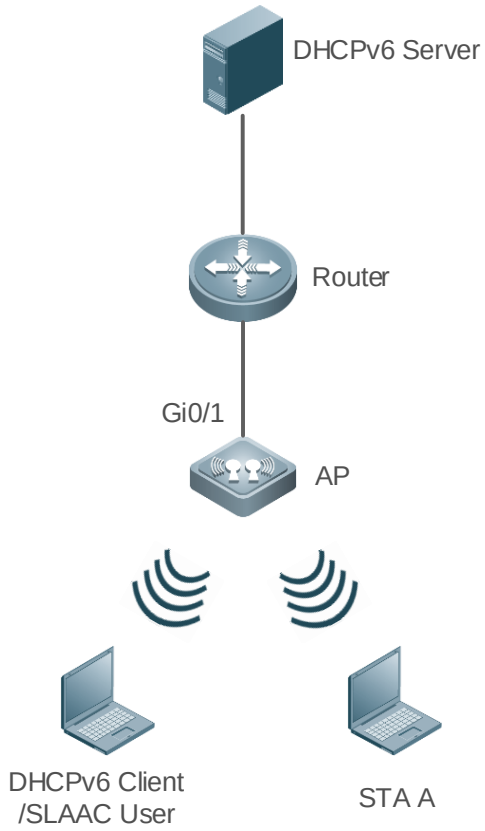
Notes	Device AP is enabled with SAVI. DHCPv6 Client obtains an IPv6 address via DHCPv6. STA A indicates a common client.

1.2.3 SLAAC and DHCPv6 Hybrid Deployment Scenario

Scenario

In this scenario, the hosts connect to the access device with SAVI enabled. The hosts use the addresses dynamically obtained through DHCPv6 or SLAAC for communication except the static address configured on the SAVI device.

Deployment



- Enable DHCPv6 snooping and ND snooping on access device AP to monitor the dynamic address obtaining.
- Configure uplink interface Gi0/1 of access device AP as a DHCPv6 snooping and ND snooping trusted interface.
- Enable SAVI on access device AP and enable the device to receive DHCPv6 and SLAAC binding entries.
- Enable IPv6 packet filtering in the specified WLAN on the AP.

Notes	Device AP is enabled with SAVI.

	DHCPv6 Client/SLAAC User indicates a client that can obtain an IPv6 address through SLAAC or DHCPv6. STA A indicates a common client.

1.3 Features

Basic Concepts

Source IPv6 Address

It indicates the source IPv6 address field in IPv6 packets.

Source MAC Address

It indicates the source MAC address field in Layer 2 packets.

Filtering Based on the Source IPv6 Address

The IPv6 packet filtering policy checks only source IPv6 addresses of all IPv6 packets (ND packets are not checked, and DHCPv6 packets are not checked if DHCPv6 snooping is enabled on a device) passing through an interface. Only packets whose source IPv6 addresses match SAVI binding entries can pass through the interface.

Filtering Based on the Source IPv6 Address and Source MAC Address

The IPv6 packet filtering policy checks the source IPv6 addresses and source MAC addresses of all IPv6 packets and allows only the packets matching the SAVI binding entries to pass through.

ND Snooping

ND snooping enables a device to snoop the SLAAC process of a client, extract the client's IPv6 address and MAC address from a packet, and generate a binding entry based on extracted information together with the client's port number (wired interface index or WLAN ID) and VLAN ID recorded by the device.

DHCPv6 Snooping

DHCPv6 snooping enables a device to snoop the process that a client obtains a dynamic IPv6 address through DHCPv6, extract the client's IPv6 address, MAC address, and lease from a packet, and generate a binding entry based on extracted information together with the client port number (wired interface index or WLAN ID) and client VLAN ID recorded by the device.

Overview

Feature	Description
Checking the Source Address Fields of Packets	Checks IPv6 packets passing through an interface based on the source IPv6 addresses or source IPv6 addresses and MAC addresses.

1.3.1 Checking the Source Address Fields of Packets

IPv6 packets passing through an interface are checked based on source IPv6 addresses or source IPv6 addresses and MAC addresses. This prevents malicious users from forging packets to launch attacks.

Working Principle

A device with SAVI enabled checks the source addresses of packets passing through an interface (wired switch port, Layer 2 aggregate port, or Dot11 radio interface). The source address can also refer to a WLAN ID. Only packets whose source addresses match the SAVI binding entries or those statically configured by the administrator can pass through the interface. There are two matching methods:

Filtering Based on the Source IPv6 Address

Packets whose source IPv6 addresses match the IPv6 address set in the binding entries can pass through an interface.

Filtering Based on the IPv6 Address and MAC Address

The device with SAVI enabled forwards only packets whose Layer 2 source MAC addresses and Layer 3 source IPv6 addresses match a binding entry.

1.4 Configuration

Configuration	Description and Command	
Configuring the SAVI Service	(Mandatory) It is used to enable the SAVI service.	
	savi ipv6 check source ip-address	Enables source IPv6 address check or source IPv6-MAC check in interface configuration mode.
	(Optional)	
	savi ipv6 source binding	Configures static binding users in global configuration mode.
	savi ipv6 check source exclude-vlan	Disables the check on IPv6 packets from a specified VLAN in interface configuration mode.
	savi ipv6 bind-source add	Adds the source of binding entries in global configuration mode.
	savi ipv6 check permit link-local	Configures SAVI to permit packets from link-local addresses and unspecified addresses in global configuration mode.

1.4.1 Configuring the SAVI Service

Configuration Effect

- The source IPv6 address field in incoming IPv6 packets is checked.

Notes

- After SAVI is enabled, an interface will deny all data packets whose source IPv6 addresses are not in the binding list. Only ICMPv6 packets with types 133, 134, 135, 136, 137, and 143 are permitted to pass through the interface; DHCPv6 packets are also permitted to pass through the interface after DHCPv6 snooping is enabled.
- SAVI-related commands can be configured only after SAVI is enabled globally.

Configuration Steps

Adding the Source of SAVI Binding Entries

- This function is enabled by default. Binding entries generated during the SLAAC and DHCPv6 processes are snooped and used as the sources of dynamic binding entries by default. Binding entries can also be statically configured.

Command	**savi ipv6 bind-source add** { **dhcp** | **slaac** }
Parameter Description	**dhcp**: Uses binding entries snooped and generated during the DHCPv6 process as a source of SAVI binding entries. **slaac**: Uses binding entries snooped and generated during the SLAAC process as a source of SAVI binding entries.
Command Mode	Global configuration mode
Usage Guide	Use ND snooping to snoop the SLAAC process. When entries snooped by ND snooping are configured as a source of SAVI binding entries, ND snooping needs to be enabled. DHCPv6 snooping is used to snoop the DHCPv6 process. When entries snooped by DHCPv6 snooping are configured as a source of SAVI binding entries, DHCPv6 snooping needs to be enabled.

Enabling SAVI on an Interface

- By default, SAVI is disabled on an interface.
- You can run the **savi ipv6 check source ip-address** [**mac-address**] command to enable or disable SAVI on an interface.

Typically, SAVI needs to work with DHCPv6 snooping or ND snooping. Therefore, DHCPv6 snooping or ND snooping should also be enabled. DHCPv6 snooping or ND snooping can be enabled either before or after SAVI is enabled on a Ruijie device.

Typically, SAVI is not enabled on DHCPv6 snooping or ND snooping trusted interfaces.

After SAVI is enabled on an interface, the permit rules of IPv6 packets are related to the IPv6 address binding mode of global IP address and MAC address binding. The default address binding mode is the strict mode. In this mode, if IPv4 SAVI is enabled but IPv6 SAVI is disabled on an interface, all IPv6 packets will be denied on the interface. When IPv4 SAVI is enabled but IPv6 SAVI is disabled on all interfaces, it is recommended that the IPv6 address binding mode of global IP address and MAC address binding be set to the loose mode. For details, see the "Global IP Address and MAC Address Binding Configuration" section.

Command	**savi ipv6 check source ip-address** [**mac-address**]
Parameter Description	**mac-address**: Configures SAVI filtering based on IPv6 and MAC addresses.
Command Mode	Interface configuration mode or WLAN security configuration mode
Usage Guide	By enabling SAVI on an interface through this command, users can detect packets based on the IPv6 addresses or IPv6 addresses and MAC addresses.

Disabling SAVI for Packets from a Specified VLAN on an Interface

- By default, SAVI takes effect for packets from all VLANs after being enabled on an interface.
- To disable SAVI for packets from a specified VLAN on an interface, run the **savi ipv6 check source exclude-vlan** *vid* command.

After SAVI is enabled on an interface, you can run this command to permit IPv6 packets from some VLANs.

Command	**savi ipv6 check source exclude-vlan** *vid*
Parameter Description	*vid*: Indicates the ID of a VLAN from which packets are permitted on an interface.
Command Mode	Interface configuration mode or WLAN security configuration mode
Usage Guide	Use this command to permit IPv6 packets from a specified VLAN.

Adding a Static User Record to the IPv6 Source Address Binding Database

- By default, the authorized user set that SAVI verifies is entirely derived from the binding users through DHCPv6 snooping or ND snooping.
- You can run the **savi ipv6 source binding** command to add static binding user records.

Command	**savi ipv6 source binding** *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-name interface-number* | **ip-mac** | **ip-only** | **wlan** *wlan-id* }
Parameter Description	*mac-address*: Indicates the MAC address of a statically added user. **vlan** *vlan-id*: Indicates the VLAN ID of a statically added user. The value range is from 1 to 4094. *ipv6-address*: Indicates the IPv6 address of a statically added user. **interface** *interface-name interface-number*: Indicates the wired access interface to which a statically added user is connected. **ip-mac**: Specifies that the IP address and MAC address binding type is used globally. **ip-only**: Specifies the IPv6 address binding type is used globally. **wlan** *wlan-id*: Indicates the WLAN to which a statically added user belongs. The value range is from 1 to 4094.
Command Mode	Global configuration mode
Usage Guide	Use this command to permit packets from a specified user.

Configuring SAVI to Permit Packets with Link-Local Addresses and Unspecified Addresses

- If SAVI is enabled on an interface, SAVI denies IPv6 packets from all users not in the binding list by default.
- The **savi ipv6 check permit link-local** command permits all IPv6 packets with fe80::/10 and ::/128 as source addresses.

This command is typically configured in a DHCPv6-only scenario. In this scenario, fe80::/10 addresses cannot be obtained through DHCPv6.

Command	**savi ipv6 check permit link-local**
Parameter Description	-
Command Mode	Global configuration mode
Usage Guide	After SAVI is enabled on an interface, SAVI checks the validity of source IPv6 addresses in IPv6 packets transmitted through the interface. After configuring this command, SAVI permits all IPv6 packets with fe80::/10 and ::/128 as source addresses.

Verification

Run the monitoring command provided by the device to display SAVI filtering entries.

Configuration Example

SAVI in an SLAAC-Only Scenario

Configuration Steps	● Enable ND snooping.
	`Hostname# configure terminal`
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)#ipv6 nd snooping trust`
	`Hostname(config-if-GigabitEthernet 0/1)#exit`
	`Hostname(config)#ipv6 nd snooping enable`
	● Enable SAVI.
	`Hostname(config)# wlansec 1`
	`Hostname(config-wlansec)# savi ipv6 check source ip-address mac-address`
	`Hostname(config-wlansec)# end`

Verification	● Check the SAVI filtering entries. `Hostname# show savi ipv6 check source`

SAVI in a DHCPv6-Only Scenario

Configuration Steps	● Enable DHCPv6 snooping.
	`Hostname# configure terminal`
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)#ipv6 dhcp snooping trust`
	`Hostname(config-if-GigabitEthernet 0/1)#exit`
	`Hostname(config)#ipv6 dhcp snooping`
	● Enable SAVI.
	`Hostname(config)# savi ipv6 check permit link-local`
	`Hostname(config)# wlansec 1`
	`Hostname(config-wlansec)# savi ipv6 check source ip-address mac-address`
	`Hostname(config-wlansec)# end`

Verification	● Check the SAVI filtering entries. `Hostname# show savi ipv6 check source`

SAVI in an SLAAC and DHCPv6 Hybrid Deployment Scenario

Configuration Steps	● Enable ND snooping.
	`Hostname# configure terminal`
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)#ipv6 nd snooping trust`
	`Hostname(config-if-GigabitEthernet 0/1)#exit`
	`Hostname(config)#ipv6 nd snooping enable`
	● Enable DHCPv6 snooping.
	`Hostname(config)# interface gigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)#ipv6 dhcp snooping trust`
	`Hostname(config-if-GigabitEthernet 0/1)#exit`
	`Hostname(config)#ipv6 dhcp snooping`
	● Enable SAVI.

	`Hostname(config)# wlansec 1`
	`Hostname(config-wlansec)# savi ipv6 check source ip-address mac-address`
	`Hostname(config-wlansec)# end`

Verification	● Check the SAVI filtering entries. `Hostname# show savi ipv6 check source`

Adding a Static Binding User

Configuration Steps	● Add a statically binding user.
	`Hostname# configure terminal`
	`Hostname(config)#savi ipv6 source binding 1000.1000.1000 vlan 1 2018:7::21 ip-mac`
	`Hostname(config)# end`

Verification	● Check static filtering entries.
	`Hostname(config)#show savi ipv6 check source`
	`Total entries found: 1`
	`No. Ipv6 Address Mac Address VLAN Interface Filter`
	`------ ---------- ---------- ---- --------- -------`
	`0 2018:7::21 1000.1000.1000 1 GLOBAL IP+MAC`

Common Misconfigurations

- SAVI is enabled on a DHCPv6 snooping or ND snooping trusted interface.

1.5 Monitoring

Displaying

Command	Description

show savi ipv6 source binding [*ipv6-address*] [*mac-address*] [**vlan** *vlan-id*] [**interface** *interface-name interface-number* **| wlan** *wlan-id*] [**type** { **dhcp** | **slaac** | **static** }]	Displays information of the IPv6 source address binding database.
show savi ipv6 check source [*ipv6-address* | **interface** *interface-name interface-number* | **wlan** *wlan-id*]	Displays effective IPv6 SAVI filtering entries.

Debugging

N/A

Configuring IP Routing

1. Configuring Route Management
2. Configuring RIP
3. Configuring OSPFv2
4. Configuring Routing Policies
5. Configuring PBR
6. Configuring Keys

1 Configuring Route Management

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 classified into three types by source:

- Direct route: Is the route discovered by a link-layer protocol and is also called interface route.
- Static route: Is manually configured by a network administrator. A static route is easy to configure and has low requirements on the system, which makes it to be fit for 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 topological changes.
- Dynamic route: Is discovered by a dynamic routing protocol.

1.2 Applications

Application	Description
Basic Functions of a Static Route	Manually configure a route.
Floating Static Route	Configure a standby route in the multipath scenario.
Load Balancing Static Route	Configure load balancing static routes in the multipath scenario.
Correlation Between a Static Route and Track	Correlate a static route with track in the multipath scenario.

1.2.1 Basic Functions of a Static Route

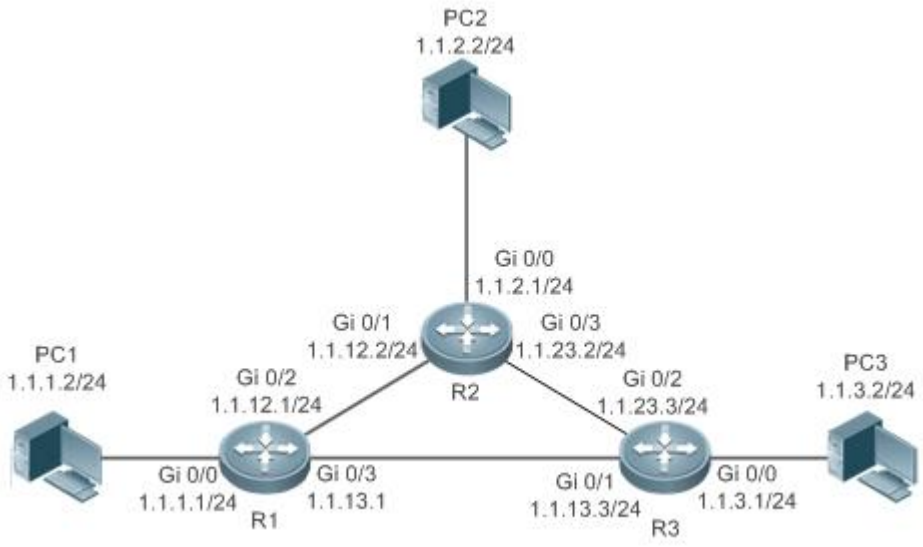
Scenario

On a network with a simple topology, you can configure only static routes to implement interworking. Properly configuring and using static routes can improve the network performance and guarantee the bandwidth for important network applications.

As shown in Figure 1-1, to implement interworking between PC1, PC2, and PC3, you can configure static routes on R1, R2, and R3.

- On R1, configure a route to the network segment of PC2 through R2, and a route to the network segment of PC3 through R3.
- On R2, configure a route to the network segment of PC1 through R1, and a route to the network segment of PC3 through R3.
- On R3, configure a route to the network segment of PC1 through R1, and a route to the network segment of PC2 through R2.

Figure 1-1



Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R1, R2, and R3.

1.2.2 Floating Static Route

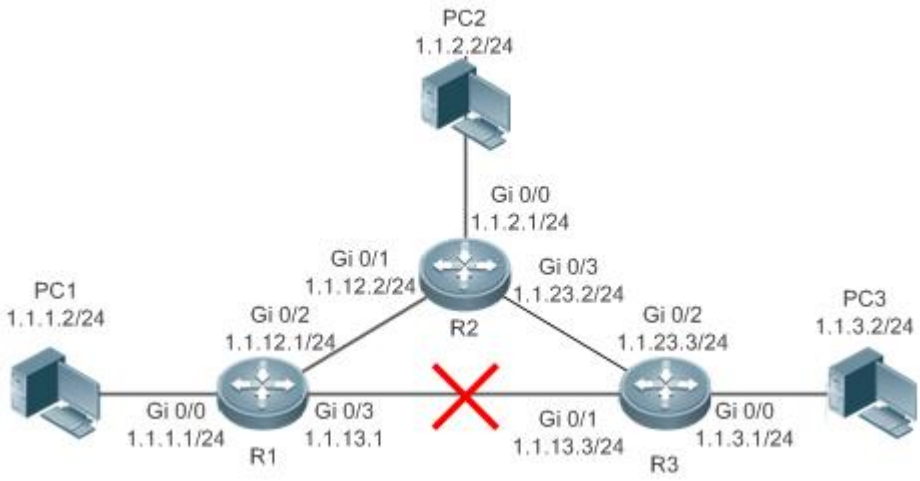
Scenario

If no dynamic routing protocol is configured, you can configure floating static routes to implement dynamic switching of routes to prevent communication interruption caused by network connection failures.

In Figure 1-2, to prevent communication interruption caused by a line failure between R1 and R3, you can configure a floating static route respectively on R1 and R3. Normally, packets are forwarded on a path with a small administrative distance. If a link on this path is Down, the route is automatically switched to the path with a large administrative distance.

- On R1, configure two routes to the network segment of PC3, including a route through R3 (default distance = 1) and a route through R2 (default distance = 2).
- On R3, configure two routes to the network segment of PC1, including a route through R1 (default distance = 1) and a route through R2 (default distance = 2).

Figure 1-2



Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R1, R2, and R3.

1.2.3 Load Balancing Static Route

Scenario

If there are multiple paths to the same destination, you can configure load balancing routes. Unlike floating routes, the administrative distances of load balancing routes are the same. Packets are distributed among these routes based on the balanced forwarding policy.

As shown in Figure 1-3, load balancing routes are configured respectively on R1 and R3, so that packets sent to the network segment of PC3 or PC1 are load balanced between two routes, including a route through R2 and a route through R4.

- On R1, configure two routes to the network segment of PC3, including a route through R2 and a route through R4.
- On R3, configure two routes to the network segment of PC1, including a route through R2 and a route through R4.

Figure 1-3



Remarks
- Load balancing is conducted based on source IP addresses by default.

- Use the **aggregateport load-balance** command on the switch to change the load balancing mode of ECMP routing.
- Use the **ip ref load-sharing original** command on the device to specify the load balancing policy for IPv4 routes.
- Use the **ipv6 ref load-sharing original** command on the device to specify the load balancing policy for IPv6 routes.

Deployment

- Configure the address and subnet mask of each interface.
- Configure static routes on R1, R2, R3, and R4.
- Configure the load balancing policy on R1 and R3.

1.2.4 Correlation Between a Static Route and Track

Whether this function is supported depends on the actual product version.

In scenarios with floating routes or load balancing routes are deployed, sometimes a fault may occur in a line but the interface status is normal; therefore, the static route cannot detect its unreachability. To solve this problem, check the reachability of the next hop of the static route. When the next hop is unreachable, switch to the backup route.

You can check whether the next hop of the static route is reachable by associating the static route with the track module.

As shown in Figure 1-4, to prevent static routes from being configured on R1 and R2, correlate the static routes with track.

- Configure static routes on R1 and R2, and specify the outbound interface or next hop as the interconnection interface.
- Correlate static routes on R1 and R2 with track, and check connectivity of the next hop of the static routes.

Figure 1-4



Deployment

- Configure IP addresses and masks for interfaces.
- Configure a track detection port.
- Configure static routes on R1 and R2, and correlate them with track.

1.3 Overview

Feature	Description
Route Computation	Generates a valid route on a device.

Optimal Route Selection	Selects an optimal route to forward packets.
Default Route	Forwards all packets and helps reduce the size of a routing table.
Route Reliability	Quickly detects routing failures and restores communication.

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 cannot forward packets based on 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 is unreachable.

Static Route

On a network with a simple topology, you can configure only static routes to implement interworking. Properly configuring and using 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 link status of the outbound interface of a static route is Up and assigned an IP address, 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, priorities of these routes are determined based on the administrative distance. A smaller administrative distance indicates a higher priority.

Equal-Cost Route

If multiple routes to the same destination have different next hops but the same administrative distance, these routes are equal-cost routes. Packets are distributed among these routes to implement load balancing based on the balanced forwarding policy.

On a specific device, the total number of equal-cost routes is limited. Routes beyond the limit do not participate in packet forwarding.

Floating Route

If multiple routes to the same destination have different next hops and different administrative distances, these routes are floating routes. The route with the smallest administrative distance will be first selected for packet forwarding. If this route is unreachable, a route with a larger administrative distance is further selected for forwarding, thus preventing communication interruption caused by a network line failure.

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.

Default Gateway

On a Layer 2 device, the **ip default gateway** command can be used to generate a default route.

Static Default Route

On a Layer 3 switch, a static route with the network segment 0.0.0.0 and the subnet mask 0.0.0.0 is configured to generate the default route.

Default Network

The default network is configured to generate a default route. If the **ip default-network** command is configured to specify a network (a classful network, such as a Class A, B, or C network), and information about this network exists in the routing table, the router will use this network as the default network and the next hop of this network is the default gateway. As the network specified by the **ip default-network** command is a classful one, if this command is used to identify a subnet in a classful network, the router automatically generates a static route of the classful network but not any default route.

1.3.4 Route Reliability

When a device on a network fails, some routes may become unreachable, causing traffic interruptions. Real-time detection of reachability of the next hop of the route can result in immediate route recalculation or switching to a backup route when a failure occurs.

Correlation with Track

Whether this function is supported depends on the actual product version.

A track object can be used to track whether an IP address is reachable or whether an interface is Up. Correlating dynamic or static routing protocols with track can enable them to quickly detect unreachability of the next hop and respond promptly.

1.4 Configuration

Configuration Item	Description and Command	
Configuring a Static Route	(Mandatory) It is used to configure a static route.	
	ip route	Configures an IPv4 static route.
	ipv6 route	Configures an IPv6 static route.
Configuring a Default Route	(Optional) It is used to configure the default gateway.	
	ip default gateway	Configures an IPv4 default gateway on a Layer 2 device.

Configuration Item	Description and Command	
	ipv6 default gateway	Configures an IPv6 default gateway on a Layer 2 device.
	ip route 0.0.0.0 0.0.0.0 *gateway*	Configures an IPv4 default gateway on a Layer 3 device.
	ipv6 route ::/0 *ipv6-gateway*	Configures an IPv6 default gateway on a Layer device.
	ip default network	Configures an IPv4 default network on a Layer 3 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.
	no ip routing	Disables IPv4 routing.
	noipv6 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

- This configuration cannot be performed on a Layer 2 device.
- If the **no ip routing** command is configured on a Layer 3 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 restore the deleted IPv4 static routes. After the device is restarted, deleted IPv4 static routes cannot be restored.
- To correlate static routes with track, you must first create a track object using the **track** command.

Configuration Step

Configuring a Static IPv4 Route

Configure the following command on an IPv4-enabled router.

Command	**ip route** *network net-mask* { *ip-address* [**global**] | *interface* [*ip-address*] } [*distance* | **description** *description-text* | [**disabled** | **enabled**] | [**track** *object-number*] [**permanent**] | **tag** *tag* | **weight** *number*] *	
Parameter Description	*network*	Indicates the address of the destination network.
	net-mask	Indicates the mask of the destination network.
	ip-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *ip-address* is not specified, a static direct route is configured.
	global	(Optional) Indicates that the next hop belongs to a global VRF.

	interface	(Optional) Indicates the next-hop outbound 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 outbound 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. The value is a string of 1 to 60 characters. By default, no description is configured.
	disabled/enabled	(Optional) Indicates whether the static route is enabled. The default value is **enabled**.
	track *object-number*	(Optional) Correlates with track. *object-number* specifies the track object ID. Correlation with track is disabled 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 default value is 0.
	weight *number*	(Optional) Indicates the weight of the static route. The default value is 1.
	all	(Optional) Deletes all static routes.
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-maskip-address.* When correlating static routes with the track object that is detected in Down state, the static route becomes invalid and cannot be used for packet forwarding.	

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* | **description** *description-text* | **tag** *tag* | **weight** *number*] *	
Parameter Description	*ipv6-prefix*	Indicates the IPv6 prefix, which must comply with the address expression specified in RFC 4291.
	prefix-length	Indicates the length of an IPv6 prefix. Note that a slash (/) must be added following 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 outbound 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 outbound 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. The value is a string of 1 to 60 characters. By default, no description is configured.

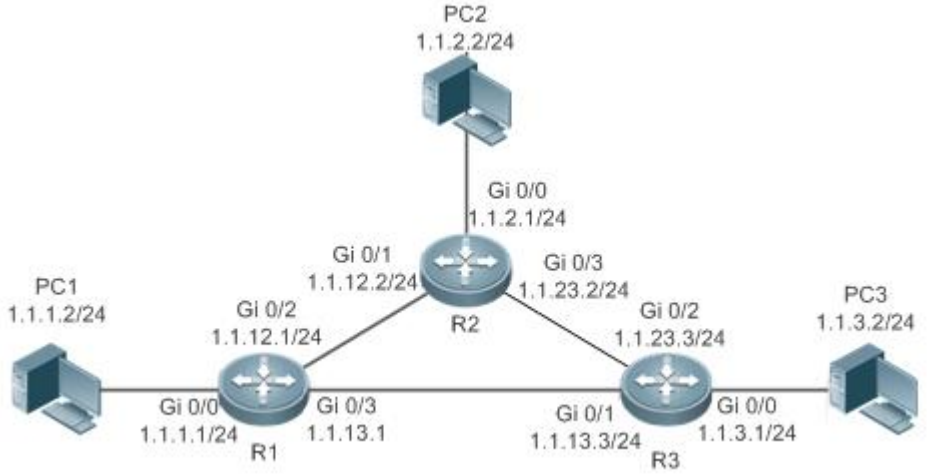
	tag *tag*	(Optional) Indicates the tag value of a static route. The value range is from 1 to 4294967295 and the default value is 0.
	weight *number*	(Optional) Indicates the weight of a static route, which must be specified when you configure equal-cost routes. The value range is from 1 to 8. When the 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.
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-lengthipv6-address.*	

Verification

- Run the **show ip route** command to display the IPv4 routing table and check whether the configured IPv4 static route takes effect.
- Run the **show ipv6 route** command to display the IPv6 routing table and check whether the configured IPv6 static route takes effect.

Configuration Example

Configuring Static Routes to Implement Interworking of the IPv4 Network

Scenario Figure 1-5	
Configuration Steps	● Configure interface addresses on each device.

R1	`R1#configure terminal`
	`R1(config)#interface gigabitEthernet 0/0`
	`R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0`
	`R1(config-if-GigabitEthernet 0/0)# exit`
	`R1(config)#interface gigabitEthernet 0/2`
	`R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0`
	`R1(config-if-GigabitEthernet 0/0)# exit`
	`R1(config)#interface gigabitEthernet 0/3`

	R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/3 R2(config-if-GigabitEthernet 0/3)# ip address 1.1.23.2 255.255.255.0
R3	R3#configure terminal R3(config)#interface gigabitEthernet 0/0 R3(config-if-GigabitEthernet 0/0)# ip address 1.1.3.1 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/1 R3(config-if-GigabitEthernet 0/1)# ip address 1.1.13.3 255.255.255.0 R3(config-if-GigabitEthernet 0/0)# exit R3(config)#interface gigabitEthernet 0/2 R3(config-if-GigabitEthernet 0/2)# ip address 1.1.23.3 255.255.255.0
	● Configure static routes on each device.
R1	R1#configure terminal R1(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.12.2 R1(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.13.3
R2	R2#configure terminal R2(config)#ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.12.1 R2(config)# ip route 1.1.3.0 255.255.255.0 GigabitEthernet 0/3 1.1.23.3
R3	R3#configure terminal R3(config)#ip route 1.1.2.0 255.255.255.0 GigabitEthernet 0/2 1.1.23.2 R3(config)# ip route 1.1.1.0 255.255.255.0 GigabitEthernet 0/1 1.1.13.1
Verification	● Display the routing table.
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. S 1.1.2.0/24 [1/0] via 1.1.12.2, GigabitEthernet 0/2 S 1.1.3.0/24 [1/0] via 1.1.13.3, GigabitEthernet 0/2 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/2

	C 1.1.12.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.13.1/32 is local host.
R2	R2# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set S 1.1.1.0/24 [1/0] via 1.1.12.1, GigabitEthernet 0/0 C 1.1.2.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.2.1/32 is local host. S 1.1.3.0/24 [1/0] via 1.1.23.3, GigabitEthernet 0/3 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.2/32 is local host. C 1.1.23.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.23.2/32 is local host.
R3	R3# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set S 1.1.1.0/24 [1/0] via 1.1.13.1, GigabitEthernet 0/2 S 1.1.2.0/24 [1/0] via 1.1.23.2, GigabitEthernet 0/2 C 1.1.3.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.3.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.13.3/32 is local host. C 1.1.23.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.23.3/32 is local host.

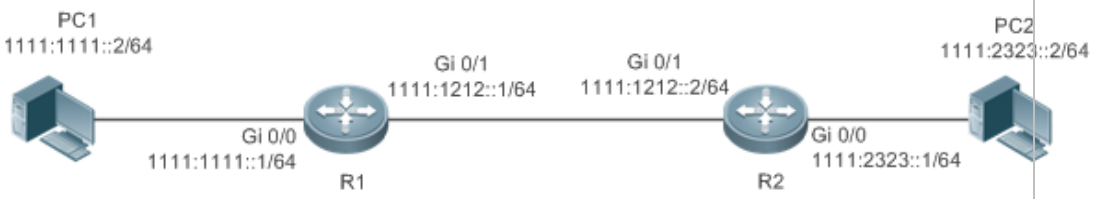
Correlating an IPv4 Static Route with Track

Scenario **Figure 1-6**	

Configuration Steps	● Configure static routes on R1 and R2, and specify the outbound interface or next hop as the interconnection interface. ● Correlate the static routes on R1 and R2 with track, and check connectivity of the next hop of the static routes.
R1	R1# configure terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/1)# exit R1(config)#track 2 interface gigabitEthernet 0/1 line-protocol R1(config)# ip route 1.1.2.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.2 track 2
R2	R2# configure terminal R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R1(config-if-GigabitEthernet 0/1)# exit R1(config)#track 2 interface gigabitEthernet 0/1 line-protocol R1(config)# ip route 1.1.1.0 255.0.0.0 gigabitEthernet 0/1 1.1.12.1 track 2

Verification	● Check the track status.
	● Check the static routes correlated with track.
	R1# show track 2
	Track 2
	Interface gigabitEthernet 0/1
	  The state is Up, delayed Down (5 secs remaining)
	  1 change, current state last: 300 secs
	  Delay up 0 secs, down 0 secs
	
	R1#show ip route track-table
	ip route 1.1.2.0 255.0.0.0 GigabitEthernet 0/1 1.1.12.2 track 2 up

Configuring Static Routes to Implement Interworking of the IPv6 Network

Scenario Figure 1-7	
Configuration Steps	● Configure interface addresses on each device.
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ipv6 address 1111:1111::1/64 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/1

	R1(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::1/64
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)#ipv6 address 1111:2323::1/64 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ipv6 address 1111:1212::2/64
	● Configure static routes on each device.
R1	R1#configure terminal R1(config)# ipv6 route 1111:2323::0/64 gigabitEthernet 0/1
R2	R2#configure terminal R2(config)#ipv6 route 1111:1111::0/64 gigabitEthernet 0/1
Verification	● Display the routing table.
R1	R1# show ipv6 route IPv6 routing table name - Default - 10 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 1111:1111::/64 via GigabitEthernet 0/0, directly connected L 1111:1111::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:2323::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host
R2	R2# show ipv6 route IPv6 routing table name - Default - 10 entries Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area C 1111:2323::/64 via GigabitEthernet 0/0, directly connected

	L 1111:2323::1/128 via GigabitEthernet 0/0, local host C 1111:1212::/64 via GigabitEthernet 0/1, directly connected L 1111:1212::1/128 via GigabitEthernet 0/1, local host S 1111:1111::/64 [1/0] via GigabitEthernet 0/1, directly connected C FE80::/10 via ::1, Null0 C FE80::/64 via GigabitEthernet 0/0, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/0, local host C FE80::/64 via GigabitEthernet 0/1, directly connected L FE80::2D0:F8FF:FEFB:C092/128 via GigabitEthernet 0/1, local host

Common Errors

- The link on the interface is not Up.
- No IP address is configured for the interface.
- The static routes are correlated with track, but a track object is not configured.

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 Layer 2 device, the **ip default-gateway** or **ipv6 default-gateway** command can be used to configure the gateway.
- On a Layer 3 switch, the **ip route** 0.0.0.0 0.0.0.0 *gateway* or **ipv6 route** ::/0 *ipv6-gateway* command can be used to configure the default gateway.
- If **no ip routing** or **no ipv6 unicast-routing** is configured on a Layer 3 device, the **ip default-gateway** or **ipv6 default-gateway** command can be used to configure the gateway.

Configuration Step

↘ Configuring an IPv4 Gateway on a Layer 2 Device

Command	**ip default-gateway** *gateway*
Parameter Description	*Gateway:* Indicates the IPv4 gateway address.
Defaults	No IPv4 gateway is configured.
Command Mode	Global configuration mode
Usage Guide	-

↘ Configuring an IPv6 Gateway on a Layer 2 Device

Command	**ipv6 default-gateway** *gateway*
Parameter	*gateway:* Indicates the IPv6 gateway address.

Description	
Defaults	No IPv6 gateway is configured.
Command Mode	Global configuration mode
Usage Guide	-

Configuring the IPv4 Default Gateway on a Layer 3 Switch

Command	**ip route 0.0.0.0 0.0.0.0** { *ip-address* [**global**] | *interface* [*ip-address*] } [*distance* | **description** *description-text* | [**disabled** | **enabled**] | [**track** *object-number*] [**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.
	ip-address	(Optional) Indicates the next-hop address of the static route. You must specify at least one of *ip-address* and *interface,* or both of them. If *ip-address* is not specified, a static direct route is configured.
	global	(Optional) Indicates that the next hop belongs to a global VRF.
	interface	(Optional) Indicates the next-hop outbound 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 outbound 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. The value is a string of 1 to 60 characters. By default, no description is configured.
	disabled/enabled	(Optional) Indicates whether the static route is enabled. The default value is **enabled**.
	track *object-number*	(Optional) Correlates with track. *object-number* specifies the track object ID. Correlation with track is disabled 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 value of the static route. The value range is from 1 to 4294967295 and the default value is 0.
	weight *number*	(Optional) Indicates the weight of the static route. The default value is 1. The value range is from 1 to 8.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ip route0.0.0.0 0.0.0.0** *ip-address.*	

Configuring the IPv6 Default Gateway on a Layer 3 Switch

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 RFC 4291.

	0	Indicates the length of the IPv6 prefix. Note that a slash (/) must be added following 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 outbound 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 outbound 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. The value is a string of 1 to 60 characters. By default, no description is configured.
	tag *tag*	(Optional) Indicates the tag value of the static route. The value range is from 1 to 4294967295 and the default value is 0.
	weight *number*	(Optional) Indicates the weight of a static route, which must be specified when you configure equal-cost routes. The value range is 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.
Defaults	By default, no static default route is configured.	
Command Mode	Global configuration mode	
Usage Guide	The simplest configuration of this command is **ipv6 route** ::/0 *ipv6-gateway.*	

Configuring the IPv4 Default Network

Command	**ip default-network** *network*	
Parameter Description	*network*	Indicates the address of the network. The network must be a Class A, B, or C network.
Defaults	By default, no default network is configured.	
Command Mode	Global configuration mode	
Usage Guide	If the network specified by the **ip default-network** command exists, a default route is generated and the next hop to this network is the default gateway. If the network specified by the **ip default-network** command does not exist, the default route is not generated.	

Verification

- On devices where routing is disabled, use the **show ip redirects** or **show ipv6 redirects** command to display the default gateway.
- On a device where routing is enabled, run the **show ip route** or **show ipv6 route** command to display the default route.

Configuration Example

Configuring IPv4 Default Routes to Implement Interworking

Scenario **Figure 1-8**	
Configuration Steps	● Configure IP addresses on Layer 3 devices.
R1	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)# ip address 1.1.12.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit
R2	R2#configure terminal R2(config)#interface gigabitEthernet 0/0 R2(config-if-GigabitEthernet 0/0)# ip address 1.1.2.1 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit R2(config)#interface gigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)# ip address 1.1.12.2 255.255.255.0 R2(config-if-GigabitEthernet 0/0)# exit
R1	● Configure an IPv6 default gateway on R1. R1#configure terminal R1(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.2
R2	R2#configure terminal R2(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet 0/1 1.1.12.1
Verification	● Display the routing table.
R1	R1# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is 1.1.12.2 S* 0.0.0.0/0 [1/0] via 1.1.12.2, GigabitEthernet 0/1 C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. C 1.1.12.0/24 is directly connected, GigabitEthernet 0/1 C 1.1.12.1/32 is local host.

1.4.3 Configuring Route Limitations

Configuration Effect

- Limit the number of equal-cost routes and number of static routes, or disable routing.

Configuration Step

Configuring the Maximum Number of Equal-Cost Routes

Command	**maximum-paths***number*
Parameter Description	*number :* Indicates the maximum number of equal-cost routes. The value range is from 1 to 64. The actual range varies from products.
Defaults	The default value varies from products.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the maximum number of next hops in the equal-cost route. In load balancing mode, the number of routes on which traffic is load balanced does not exceed the configured number of equal-cost routes.

Configuring the Maximum Number of IPv4 Static Routes

Command	**ip static route-limit***number*
Parameter Description	*number:* Indicates the upper limit of routes. The value range is from 1 to 10000.
Defaults	By default, a maximum of 1024 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 range is from 1 to 10000.
Defaults	By default, a maximum of 1000 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, IP routing is enabled.
Command	Global configuration mode

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. In this case, you can disable the IPv4 routing function of the device.

Disabling IPv6 Routing

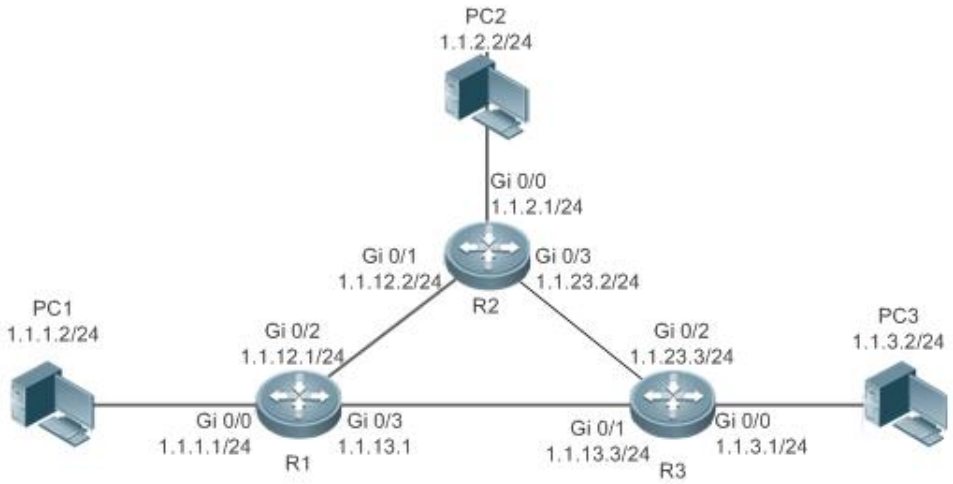
Command	no ipv6 unicast-routing
Parameter Description	N/A
Defaults	By default, IPv6 routing is enabled.
Command Mode	Global configuration mode
Usage Guide	Run this command to disable IPv6 routing. If the device functions only as a bridge or a VoIP gateway, the device does not need to use the IPv6 routing function. In this case, you can disable the IPv6 routing function of the device

Verification

- Run the **show run** command to display the configuration file and verify that the preceding configuration commands exist.

Configuration Example

Configuring a Maximum of Two Static Routes

Scenario Figure 1-9	
Configuration Steps	• On R1, configure the IP addresses, static routes, and maximum number of static routes.
	R1#configure terminal R1(config)#interface gigabitEthernet 0/0 R1(config-if-GigabitEthernet 0/0)# ip address 1.1.1.1 255.255.255.0 R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)# ip address 1.1.12.1 255.255.255.0

	R1(config-if-GigabitEthernet 0/0)# exit R1(config)#interface gigabitEthernet 0/3 R1(config-if-GigabitEthernet 0/3)# ip address 1.1.13.1 255.255.255.0 R1(config-if-GigabitEthernet 0/3)# exit R1(config)#ip route 1.1.3.0 255.255.255.0 1.1.13.3 R1(config)#ip route 1.1.4.0 255.255.255.0 1.1.12.2 R1(config)#ip route 1.1.5.0 255.255.255.0 1.1.12.2 R1(config)#ip static route-limit 2 % Exceeding maximum static routes limit.
Verification	● Check the static routes that really take effect in the routing table.
	R1(config)# show ip route Codes: C - Connected, L - Local, S - Static R - RIP, O - OSPF, B - BGP, I - IS-IS N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 SU - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 IA - Inter area, * - candidate default Gateway of last resort is no set C 1.1.1.0/24 is directly connected, GigabitEthernet 0/0 C 1.1.1.1/32 is local host. S 1.1.3.0/24 [1/0] via 1.1.13.3 S 1.1.4.0/24 [1/0] via 1.1.12.2 C 1.1.12.0/24 is directly connected, GigabitEthernet 0/2 C 1.1.12.1/32 is local host. C 1.1.13.0/24 is directly connected, GigabitEthernet 0/3 C 1.1.13.1/32 is local host.

1.5 Monitoring

Clearing

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

Command	Description
clear ip route	Clears the routing table cache.

Displaying

Command	Description
show ip redirects	Displays the default IPv4 gateway.
show ip route [*network* [*mask* [**longer-prefix**]] | **count** | **ecmp** [*network* [*mask*]] | **normal** [*network* [*mask*]] | *protocol* [*process-id*] | **weight**]	Displays IPv4 routing table information.
show ip route summary [**all**]	Displays IPv4 routing table statistics.

Command	Description
show ip route track-table	Displays information of the track correlated with IPv4 routes.
show ipv6 redirects	Displays the default IPv6 gateway.
show ipv6 route [*ipv6-prefix/prefix-length* [**longer-prefixes**] | *protocol* [*process-id*] | **weight**]]	Displays IPv6 routing table information.
show ipv6 route summary [**all**]	Displays IPv6 routing table statistics.

Debugging



Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug nsm kernel ucast- v4	Debugs IPv4 route management.
debug nsm kernel ucast-v6	Debugs IPv6 route management.
debug nsm kernel frr	Enables the debugging of fast reroute (FRR).
debug nsm kernel default-network	Debugs default network management.
debug nsm events	Debugs internal events of route management.
debug nsm packet send	Debugs sending of route management and routing protocol messages.
debug nsm packet recv	Debugs receiving of route management and routing protocol messages.

1 Configuring RIP

1.1 Overview

The Routing Information Protocol (RIP) is a unicast routing protocol applied on IPv4 networks. RIP-enabled routers exchange routing information to obtain routes to remote networks.

As an Interior Gateway Protocol (IGP), RIP can run only within an autonomous system (AS) and is applicable to small-sized networks whose longest path involves less than 16 hops.

Protocols and Standards

- RFC 1058: Defines RIP version 1 (RIPv1).
- RFC 2453: Defines RIP version 2 (RIPv2).

1.2 Applications

Application	Description
Basic RIP Application	Routing information is automatically maintained through RIP on a small-sized network.

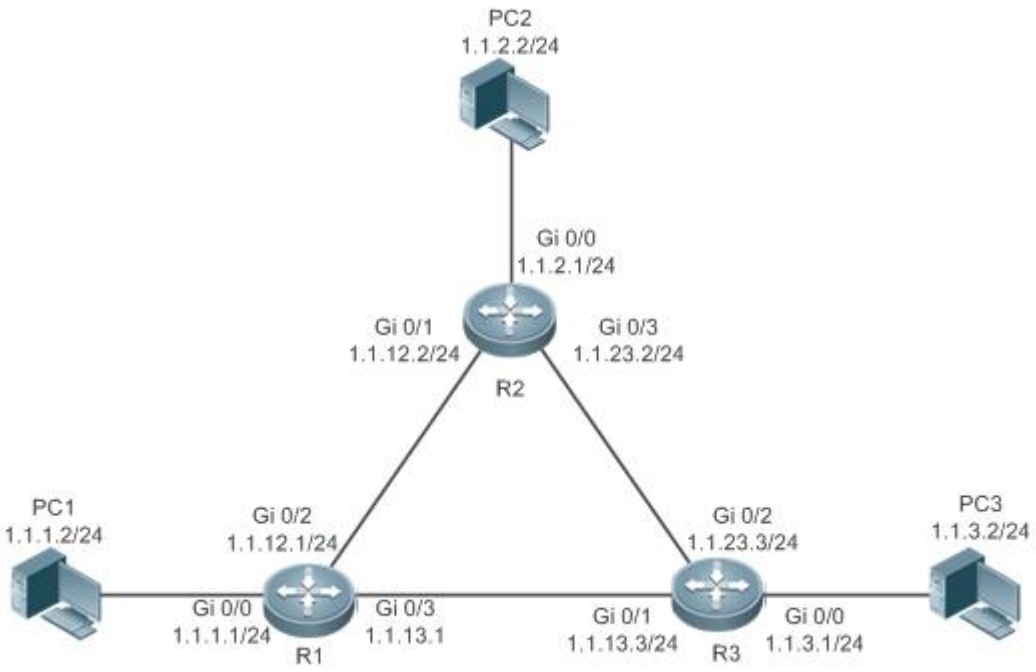
1.2.1 Basic RIP Application

Scenario

On a network with a simple architecture, you can configure RIP to implement interworking. Configuring RIP is simpler than configuring other IGP protocols such as the Open Shortest Path First (OSPF). Compared with static routing, RIP can dynamically adapt to the network architecture changes and is easier to maintain.

As shown in Figure 1-1, to implement interworking between PC1, PC2, and PC3, you can configure RIP routes on R1, R2, and R3.

Figure 1-1



Deployment

- Configure IP addresses and gateways on three PCs.
- Configure IP addresses and subnet masks on three routers.
- Configure RIP on three routers.

1.3 Features

Basic Concepts

IGP and EGP

An IGP runs within an AS. For example, RIP is an IGP.

An Exterior Gateway Protocol (EGP) runs between ASs. For example, BGP is an EGP.

Classful and Classless Routing Protocols

Protocols can be classified based on the type of routes supported:

- Classful routing protocol: Supports classful routes. For example, RIPv1 is a classful routing protocol.
- Classless routing protocol: Supports classless routes. For example, RIPv2 is a classless routing protocol.

Overview

Feature	Description
RIPv1 and RIPv2	RIP is available in two versions: RIPv1 and RIPv2.
Exchanging Routing Information	By exchanging routing information, RIP-enabled devices can automatically obtain routes to a remote network and update routes in real time.

Feature	Description
Routing Algorithm	Based on the distance-vector algorithm, RIP uses the vector addition method to compute routing information.
Avoiding Routing Loops	RIP uses split horizon and poison reverse to avoid routing loops.
Security Measures	RIP uses authentication and source address verification to ensure protocol security.
Reliability Measures	RIP uses Graceful Restart (GR) to enhance protocol reliability.

1.3.1 RIPv1 and RIPv2

Two RIP versions are available: RIPv1 and RIPv2.

Working Principle

RIPv1

RIPv1 packets are broadcast, with broadcast address 255.255.255.255 and UDP port 520. RIPv1 cannot identify the subnet mask, and supports only classful routes.

RIPv2

RIPv2 packets are multicast, with multicast address 224.0.0.9 and UDP port 520. RIPv2 can identify the subnet mask, and supports classless routes, summarized route, and supernetting routes. RIPv2 supports cleartext authentication and Message Digest 5 (MD5) authentication.

Related Configuration

Enabling the RIP Process

The RIP process is disabled by default.

Run the **router rip** command to enable the RIP process.

You must enable the RIP process on a device; otherwise, all functions related to RIP cannot take effect.

Running RIP on an Interface

By default, RIP does not run on an interface.

Run the **network** command to define an address range. RIP runs on interfaces that belong to this address range.

After RIP runs on an interface, RIP packets can be exchanged on the interface and RIP can learn routes to the network segments directly connected to the device.

Defining the RIP Version

By default, an interface receives RIPv1 and RIPv2 packets, and sends RIPv1 packets.

Run the **version** command to define the version of RIP packets sent or received on all interfaces.

Run the **ip rip send version** command to define the version of RIP packets sent on an interface.

Run the **ip rip receive version** command to define the version of RIP packets received on an interface.

⚠ If the versions of RIP running on adjacent routers are different, the RIPv1-enabled router will learn incorrect routes.

Preventing an Interface from Sending or Receiving Packets

By default, a RIP-enabled interface is allowed to send and receive RIP packets.

Run the **no ip rip receive enable** command to prevent an interface from receiving RIP packets.

Run the **no ip rip send enable** command to prevent an interface from sending RIP packets.

Run the **passive-interface** command to prevent an interface from sending broadcast or multicast RIP packets.

Configuring a Mode for Sending RIP Packets

By default, RIPv1 packets are broadcast and RIPv2 are multicast.

Run the **ip rip v2-broadcast** command to broadcast RIPv2 packets on an interface.

Run the **neighbor** command to unicast RIP packets to a specified neighboring router.

1.3.2 Exchanging Routing Information

Compared with static routing, dynamic routing protocols have a significant advantage. By exchanging routing information, devices can automatically obtain routes to a remote network and update them in real time.

Working Principle

Initialization

After RIP is enabled on a router, the router sends a request packet to its neighboring router, requesting for all routing information, that is, the routing table. After receiving the request packet, the neighboring router returns a response packet containing the local routing table. After receiving the response packet, the router updates the local routing table, and sends an update packet to the neighboring router, informing the neighboring router of routing update information. After receiving the update packet, the neighboring router updates the local routing table, and sends the update packet to other adjacent routers. After a series of updates, all routers can obtain and retain the latest routing information.

Periodical Update

By default, periodical update is enabled for RIP. Adjacent routers exchange complete routing information with each other every 30s (update timer), that is, the entire routing table is sent to neighboring routers. One update packet contains at most 25 routes. Therefore, many update packets may be required to send the entire routing table. You can set the sending delay between update packets to avoid loss of routing information.

For every non-local route, if the route is not updated within 180s (invalid timer), the metric of the route is changed to 16 (unreachable). If the route is still not updated in the next 120s (flush timer), the route is deleted from the routing table.

Triggered Update

After the triggered update function is enabled, periodical update is automatically disabled. When routing information changes on a router, the router immediately sends routes related to the change (instead of the complete routing table) to the neighboring router, and use acknowledgment and retransmission mechanisms to ensure that the neighboring router receives the routes successfully. Compared with periodical update, triggered update helps reduce flooding and accelerates route convergence.

Events that can trigger update include router startup, interface status change, changes in routing information (such as the metric), and receiving of a request packet.

Route Summarization

When sending routing information to a neighboring router, the RIP-enabled router summarizes subnet routes that belong to the same classful network into a route, and sends the summarized route to the neighboring router. For example, summarize 80.1.1.0/24 (metric=2) and 80.1.2.0/24 (metric=3) into 80.0.0.0/8 (metric=2), and set the metric of the summarized route to the optimal value.

Only RIPv2 supports route summarization. Route summarization can reduce the size of the routing table and improve the efficiency of routing information exchange.

Supernetting Route

If the subnet mask length of a route is smaller than the natural mask length, this route is called supernetting route. For example, in the route 80.0.0.0/6, 80.0.0.0 is a Class A network address and the natural mask is 8 bits, so route 80.0.0.0/6 is a supernetting route.

Only RIPv2 supports supernetting routes.

Default Route

In the routing table, a route to the destination network 0.0.0.0/0 is called default route.

The default route can be learned from a neighboring router, or sent to a neighboring router.

Route Redistribution

For RIP, other types of routes (such as direct routes, static routes, and routes of other routing protocols) are called external routes.

External routes (excluding the default route) can be redistributed to RIP and advertised to neighbors.

Route Filtering

Filtering conditions can be configured to limit routing information exchanged between adjacent routers. Only the routing information that meets filtering conditions can be sent or received.

Related Configuration

Sending Delay Between Update Packets

By default, update packets are sent continuously without any delay.

Run the **output-delay** command to set the sending delay between update packets.

RIP Timers

By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Run the **timers basic** command to change values of RIP timers.

Increasing the value of the flush timer can reduce route flapping. Decreasing the value of the flush timer helps accelerate route convergence.

The values of RIP timers must be consistent on adjacent routers. Unless otherwise required, you are advised not to change RIP timers.

Triggered Update

By default, periodical update is enabled.

Run the **ip rip triggered** command to enable triggered updates on the interface and disable periodical update.

Run the **ip rip triggered retransmit-timer** command to modify the retransmission interval of update packets. The default value is 5s.

Run the **ip rip triggered retransmit-count** command to modify the maximum retransmission times of update packets. The default value is 36.

Route Summarization

By default, route summarization is automatically enabled if an interface is allowed to send RIPv2 packets.

Run the **no auto-summary** command to disable route summarization.

Run the **ip rip summary-address** command to configure route summarization on an interface.

Supernetting Route

By default, supernetting routes can be sent if an interface is allowed to send RIPv2 packets.

Run the **no ip rip send supernet-routes** command to prevent the device from sending supernetting routes.

Default Route

Run the **ip rip default-information** command to advertise the default route to neighbors on an interface.

Run the **default-information originate** command to advertise the default route to neighbors from all interfaces.

Route Redistribution

Run the **redistribute** command to redistribute external routes (excluding the default route) to RIP and advertise them to neighbors.

Route Filtering

Run the **distribute-list out** command to set filtering rules to limit routing information sent by the device.

Run the **distribute-list in** command to set filtering rules to limit routing information received by the device.

1.3.3 Routing Algorithm

Based on the distance-vector algorithm, RIP uses the vector addition method to compute routing information.

Working Principle

Distance-Vector Algorithm

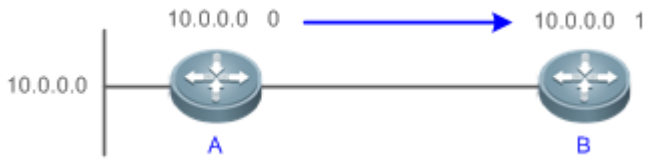
RIP is based on the distance-vector algorithm. The distance-vector algorithm treats a route as a vector that consists of the destination network and distance (metric). The router obtains a route from its neighbor and adds the distance vector (from itself to the neighbor) to the route to form its own route.

RIP uses the hop count to evaluate the distance (metric) to the destination network. By default, the hop count from a router to its directly connected network is 0, the hop count from a router to a network that can be reached through the router is 1, and so on. That is, the metric is equal to the number of routers from the local network to the destination network. To restrict the convergence time, RIP defines that the metric must be an integer between 0 and 15. If the

metric is equal to or greater than 16, the destination network or host is unreachable. For this reason, RIP cannot be applied on a large-scale network.

As shown in Figure 1-2, Router A is connected to the network 10.0.0.0. Router B obtains the route (10.0.0.0,0) from Router A and adds metric 1 to the route to obtain its own route (10.0.0.0,1), and the next hop points to Router A.

Figure 1-2

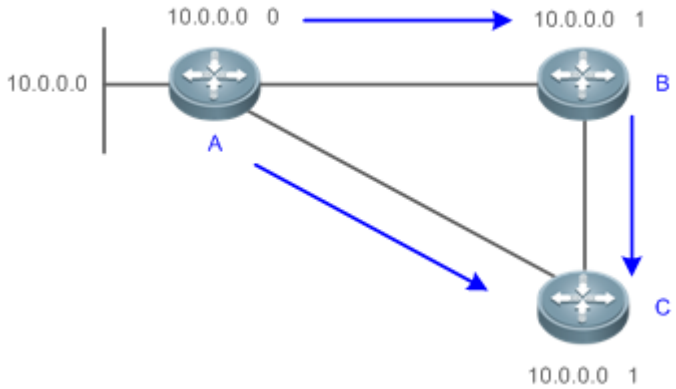


Selecting the Optimal Route

If multiple routes to the same destination network is available, a RIP-enabled router preferentially selects the route with the smallest metric.

As shown in Figure 1-3, Router A is connected to the network 10.0.0.0. Router C obtains the route (10.0.0.0,0) from Router A and the route (10.0.0.0,1) from Router B. Router C will select the route that is obtained from Router A and add metric 1 to this route to form its own route (10.0.0.0,1), and the next hop points to Router A.

Figure 1-3



When routes originated from different sources exist on a router, the route with the smallest distance is preferentially selected.

Route Source	Default Distance
Directly-connected network	0
Static route	1
OSPF route	110
IS-IS route	115
RIP route	120
Unreachable route	255

Related Configuration

Changing the Distance

By default, the distance of a RIP route is 120.

Run the **distance** command to change the distance of a RIP route.

Changing the Metric

For a RIP route that is proactively discovered by a device, the default metric is equal to the number of hops from the local network to the destination network. For a RIP router that is manually configured (default or redistributed route), the default metric is 1.

Run the **offset-list in** command to increase the metric of a received RIP route.

Run the **offset-list out** command to increase the metric of a sent RIP route.

Run the **default-metric** command to change the default metric of a redistributed route.

Run the **redistribute** command to change the metric of a route when the route is redistributed.

Run the **default-information originate** command to change the metric of a default route when the default route is introduced.

Run the **ip rip default-information** command to change the metric of a default route when the default route is created.

1.3.4 Avoiding Routing Loops

RIP uses split horizon and poison reverse to avoid routing loops.

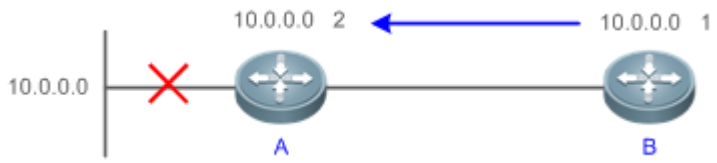
Working Principle

Routing Loop

A RIP routing loop occurs due to defects of the distance-vector algorithm.

As shown in Figure 1-4, Router A is connected to the network 10.0.0.0, and sends an update packet every 30s. Router B receives the route 10.0.0.0 from Router A every 30s. If Router A is disconnected from 10.0.0.0, the route to 10.0.0.0 will be deleted from the routing table on Router A. Then the update packet sent by Router A no longer contains this route. Because Router B does not receive an update packet related to 10.0.0.0, Router B determines that the route to 10.0.0.0 is valid within 180s and uses the update packet to send this route to Router A. Because the route to 10.0.0.0 does not exist on Router A, the route learned from Router B is added to the routing table. Router B determines that data can reach 10.0.0.0 through Router A, and Router A determines that data can reach 10.0.0.0 through Router B. In this case, a routing loop is formed.

Figure 1-4



Split Horizon

Split horizon can prevent routing loops. After split horizon is enabled on an interface, a route received on this interface will not be sent out from this interface.

As shown in Figure 1-5, after split horizon is enabled on the interface between Router A and Router B, Router B will not send the route 10.0.0.0 back to Router A. Router B will learn that 10.0.0.0 is not reachable 180s later.

Figure 1-5



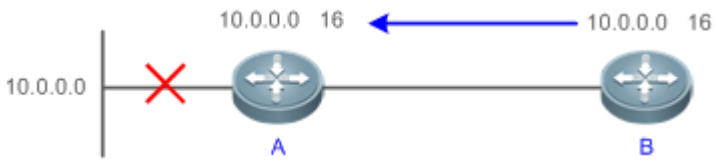
Poison Reverse

Poison reverse can also prevent routing loops. Compared with split horizon, poison reverse is more reliable, but results in more protocol packets, which makes network congestion more severe.

After poison reverse is enabled on an interface, a route received from this interface will be sent out from this interface again, but the metric of this router will be changed to 16 (unreachable).

As shown in Figure 1-6, after learning the route 10.0.0.0 from Router A, Router B sets the metric of this route to 16 and sends the route back to Router A. After this route becomes invalid, Router B advertises the route 10.0.0.0 (metric = 16) to Router A to accelerate the process of deleting the route from the routing table.

Figure 1-6



Related Configuration

Split Horizon

By default, split horizon is enabled.

Run the **no ip rip split-horizon** command to disable split horizon.

Poison Reverse

By default, poison reverse is disabled.

Run the **ip rip split-horizon poisoned-reverse** command to enable poison reverse. After poison reverse is enabled, split horizon is automatically disabled.

1.3.5 Security Measures

RIP uses authentication and source address verification to ensure protocol security.

Working Principle

Authentication

RIPv2 supports authentication, but RIPv1 does not.

After authentication is enabled on an interface, routing information cannot be exchanged between adjacent devices if authentication fails. The authentication function is used to prevent unauthorized devices from accessing the RIP routing domain.

RIPv2 supports cleartext authentication and MD5 authentication.

Source Address Verification

When a RIP-enabled device receives an update packet, it checks whether the source IP address in the packet and the IP address of the inbound interface are on the same network segment. If not, the device drops the packet. Source address verification is used to ensure that RIP routing information is exchanged only between adjacent routing devices.

- Source address verification is invalid for the interface with the unnumbered IP address.
- If the triggered update function is enabled, source address verification is automatically enabled (not configurable).
- If split horizon is disabled, source address verification is automatically enabled (not configurable).

Related Configuration

Authentication

By default, authentication is disabled.

Run the **ip rip authentication mode text** command to enable cleartext authentication on an interface.

Run the **ip rip authentication mode md5** command to enable MD5 authentication on an interface.

Run the **ip rip authentication text-password** command to set the password for cleartext authentication on an interface.

Run the **ip rip authentication key-chain** command to reference the key in the configured key chain as the authentication key on an interface.

Source Address Verification

By default, source address verification is enabled.

Run the **no validate-update-source** command to disable source address verification.

1.3.6 Reliability Measures

RIP uses GR to enhance protocol reliability.

Working Principle

GR

GR ensures uninterrupted data transmission when the protocol is restarted. If RIP is restarted on a GR-enabled device, the forwarding table before restart will be retained and a request packet will be sent to the neighbor so that the route can be learned again. During the GR period, RIP completes route re-convergence. After the GR period expires, RIP updates the forwarding entry and advertises the routing table to the neighbor.

Related Configuration

GR

By default, GR is disabled.

Run the **graceful-restart** command to enable GR.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic RIP Functions	(Mandatory) It is used to build a RIP routing domain.	
	router rip	Enables a RIP routing process and enters routing process configuration mode.
	network	Runs RIP on interfaces in the specified address range.
	version	Defines the RIP version.
	ip rip split-horizon	Enables split horizon or poison reverse on an interface.
	passive-interface	Configures a passive interface.
Controlling Interaction of RIP Packets	(Optional) It is used to change the default mechanism for sending or receiving RIP packets.	
	neighbor	Unicasts RIP packets to a specified neighbor.
	ip rip v2-broadcast	Broadcasts RIPv2 packets on an interface.
	ip rip receive enable	Allows the interface to receive RIP packets.
	ip rip send enable	Allows the interface to send RIP packets.
	ip rip send version	Defines the version of RIP packets sent on an interface.
	ip rip receive version	Defines the version of RIP packets received on an interface.
Enabling Triggered Update	Optional.	
	ip rip triggered	Enables triggered update on an interface.
Enabling Source Address Verification	Optional.	
	validate-update-source	Enables source address verification.
Enabling Authentication	(Optional) Only RIPv2 supports authentication.	
	ip rip authentication mode	Enables authentication and sets the authentication mode on an interface.
	ip rip authentication text-password	Configures the password for cleartext authentication on an interface.
	ip rip authentication key-chain	Configures the authentication key chain on an interface.
Enabling Route Summarization	(Optional) Only RIPv2 supports route summarization.	
	auto-summary	Enables automatic summarization of RIP routes.
	ip rip summary-address	Configures route summarization on an interface.
Enabling Supernetting	(Optional) Only RIPv2 supports supernetting routes.	

Configuration	Description and Command	
Routes	**ip rip send supernet-routes**	Enables advertisement of RIP supernetting routes on an interface
Advertising the Default Route or External Routes	⚠ Optional.	
	ip rip default-information	Advertises the default route to neighbors on an interface.
	default-information originate	Advertises the default route to neighbors.
	redistribute	Redistributes routes and advertises external routes to neighbors.
Setting Route Filtering Rules	⚠ Optional.	
	distribute-list in	Filters the received RIP routing information.
	distribute-list out	Filters the sent RIP routing information.
Changing Route Selection Parameters	⚠ Optional.	
	distance	Changes the administrative distance (AD) of a RIP route.
	offset-list	Increases the metric of a received or sent RIP route.
	default-metric	Configures the default metric of an external route redistributed to RIP.
Changing Values of Timers	⚠ Optional.	
	timers basic	Changes the update timer, invalid timer, and flush timer.
	output-delay	Sets the sending delay between RIP route update packets.
Enabling GR	⚠ Optional.	
	graceful-restart	Configures the GR capability.

1.4.1 Configuring Basic RIP Functions

Configuration Effect

- Build a RIP routing domain on a network.
- Routers in the domain obtain routes to a remote network through RIP.

Notes

- IPv4 addresses must be configured.
- IPv4 unicast routes must be enabled.

Configuration Step

↘ Enabling a RIP Routing Process

- Mandatory.

- Unless otherwise required, this configuration must be performed on each router in the RIP routing domain.

Associating with the Local Network

- Mandatory.
- Unless otherwise required, this configuration must be performed on each router in the RIP routing domain.
- Unless otherwise required, the local network associated with RIP should cover network segments of all Layer 3 interfaces.

Defining the RIP Version

- If RIPv2 functions (such as the variable length subnet mask and authentication) are required, enable RIPv2.
- Unless otherwise required, you must define the same RIP version on each router.

Enabling Split Horizon or Poison Reverse

- By default, split horizon is enabled and poison reverse is disabled.
- Unless otherwise required, enable split horizon on each interface connected to the broadcast network, such as the Ethernet. (Retain the default setting.)
- Unless otherwise required, enable split horizon on each interface connected to the point-to-point (P2P) network, such as the PPP and HDLC. (Retain the default setting.)
- It is recommended that split horizon and poison reverse be disabled on an interface connected to a non-broadcast multi-access (NBMA) network, such as FR and X.25; otherwise, some devices may fail to learn complete routing information.
- If the secondary IP address is configured for an interface connected to a non-broadcast network, it is recommended that split horizon and poison reverse be disabled.

Configuring a Passive Interface

- To suppress update packets on a RIP interface, configure the interface as a passive interface.
- Use the passive interface to set the boundary of the RIP routing domain. The network segment of the passive interface belongs to the RIP routing domain, but RIP packets cannot sent over the passive interface.
- If RIP routes need to be exchanged on an interface (such as the interconnected interface of the router) in the RIP routing domain, this interface cannot be configured as a passive interface.

Verification

- Check the routing table on a router to verify that the route to a remote network can be obtained through RIP.

Related Commands

Enabling a RIP Routing Process

Command Syntax	**router rip**
Parameter Description	N/A
Command	Global configuration mode

Mode	
Configuration Usage	This command is used to create a RIP routing process and enter the routing process configuration mode.

Associating with the Local Network

Command Syntax	**network** *network-number* [*wildcard*]
Parameter Description	*network-number*: Indicates the number of a network. *wildcard*: Defines the IP address comparison bit. The value 0 indicates exact match, and the value 1 indicates that the bit is not compared.
Command Mode	Routing process configuration mode
Configuration Usage	RIP can run and learn direct routes and RIP packets can be exchanged only on an interface whose address is within the range defined by **network**. If **network 0.0.0.0 255.255.255.255** is configured, all interfaces are covered. If *wildcard* is not configured, the classful address range is used by default, that is, the interfaces whose addresses fall into the classful address range participate in RIP operations.

Defining the RIP Version

Command Syntax	**version** { **1** | **2** }
Parameter Description	**1**: Indicates RIPv1. **2**: Indicates RIPv2.
Command Mode	Global configuration mode
Configuration Usage	This command takes effect on the router. You can run this command to define the version of RIP packets sent or received on all interfaces.

Enabling Split Horizon

Command Syntax	**ip rip split-horizon** [**poisoned-reverse**]
Parameter Description	**poisoned-reverse**: Indicates poison reverse.
Command Mode	Interface configuration mode
Configuration Usage	After poison reverse is enabled, split horizon is automatically disabled.

Configuring a Passive Interface

Command Syntax	**passive-interface** { **default** | *interface-type interface-num* }
Parameter Description	**default**: Indicates all interfaces. ***interface-type interface-num***: Specifies an interface.
Command	Routing process configuration mode

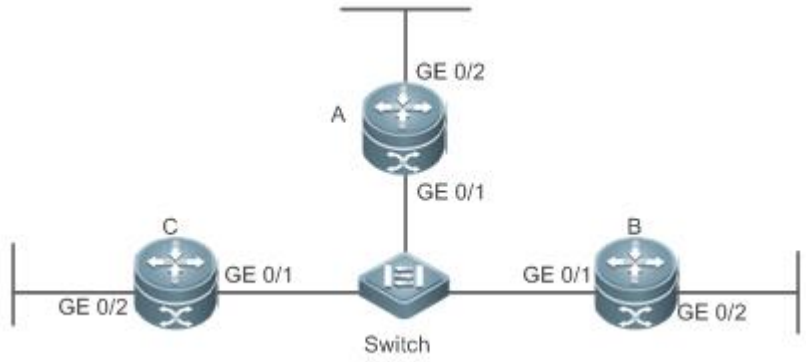
Mode	
Configuration Usage	First, run the **passive-interface default** command to configure all interfaces as passive interfaces. Then, run the **no passive-interface** *interface-type interface-num* command to cancel the interfaces used for interconnection between routers in the domain.

Configuration Example

Building a RIP Routing Domain

Scenario

Figure 1-7



Remarks	The interface IP addresses are as follows: A: GE0/1: 110.11.2.1/24; GE0/2: 155.10.1.1/24 B: GE0/1: 110.11.2.2/24; GE0/2: 196.38.165.1/24 C: GE0/1: 110.11.2.3/24; GE0/21: 17.102.0.1/16

Configuration Steps

- Configure the interface IP addresses on all routers.
- Configure basic RIP functions on all routers.

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip address 110.11.2.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)# exit
A(config)# interface GigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)# ip address 155.10.1.1 255.255.255.0
A(config)# router rip
A(config-router)# version 2
A(config-router)# network 0.0.0.0 255.255.255.255
A(config-router)# passive-interface default
A(config-router)# no passive-interface GigabitEthernet 0/1
```

B

```
B# configure terminal
B(config)# interface GigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)# ip address 110.11.2.2 255.255.255.0
B(config-if-GigabitEthernet 0/1)# exit
B(config)# interface GigabitEthernet 0/2
B(config-if-GigabitEthernet 0/2)# ip address 196.38.165.1 255.255.255.0
B(config-if-GigabitEthernet 0/2)# exit
B(config)# router rip
B(config-router)# version 2
B(config-router)# network 0.0.0.0 255.255.255.255
```

	B(config-router)# passive-interface default B(config-router)# no passive-interface GigabitEthernet 0/1
C	C# configure terminal C(config)# interface GigabitEthernet 0/1 C(config-if-GigabitEthernet 0/1)# ip address 110.11.2.3 255.255.255.0 C(config-if-GigabitEthernet 0/1)# exit C(config)# interface GigabitEthernet 0/2 C(config-if-GigabitEthernet 0/2)# ip address 117.102.0.1 255.255.0.0 C(config-if-GigabitEthernet 0/2)# exit C(config)# router rip C(config-router)# version 2 C(config-router)#no auto-summary C(config-router)# network 0.0.0.0 255.255.255.255 C(config-router)# passive-interface default C(config-router)# no passive-interface GigabitEthernet 0/1
Verification	● Check routing tables on Router A, Router B, and Router C. Verify that RIP learns the routes to remote networks (contents marked in blue).
A	A# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1 C 155.10.1.0/24 is directly connected, GigabitEthernet 0/2 C 155.10.1.1/32 is local host. C 192.168.217.0/24 is directly connected, VLAN 1 C 192.168.217.233/32 is local host. R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
B	B# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default

	Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.2/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1 C 196.38.165.0/24 is directly connected, GigabitEthernet 0/2 C 196.38.165.1/32 is local host. R 117.0.0.0/8 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C	C# show ip route Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default Gateway of last resort is no set C 110.11.2.0/24 is directly connected, GigabitEthernet 0/1 C 110.11.2.3/32 is local host. C 117.102.0.0/16 is directly connected, GigabitEthernet 0/2 C 117.102.0.1/32 is local host. R 155.10.0.0/16 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1 R 196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1

Common Errors

- The IPv4 address is not configured on an interface.
- The RIP version is not defined on a device, or the RIP version on the device is different from that on other routers.
- The address range configured by the **network** command does not cover the IP address of a specific interface.
- The **wildcard** parameter in the **network** command is not correctly configured. The value 0 indicates exact match, and the value 1 indicates that the bit is not compared.
- The interface used for interconnection between devices is configured as a passive interface.

1.4.2 Controlling Interaction of RIP Packets

Configuration Effect

Change the default running mechanism of RIP and manually control the interaction mode of RIP packets, including:

- Allow an interface to send or prohibit it from unicasting RIP packets to a specified neighbor.
- Allow an interface to send or prohibit it from sending unicast RIPv2 packets but not broadcast packets to a specified neighbor.
- Allow an interface to send or prohibit it from receiving RIP packets.
- Allow an interface to send or prohibit it from sending RIP packets.
- Allow an interface to send or prohibit it from receiving RIP packets of a specified version.

- Allow an interface to send or prohibit it from sending RIP packets of a specified version.

Notes

- Basic RIP functions must be configured.
- On an interface connected to a neighbor device, the configured version of sent RIP packets must be the same as the version of received RIP packets.

Configuration Step

Unicasting RIP Route Update Packets to a Specified Neighbor

- Configure this function if only some of devices connected to an interface are required to receive updated routing information.
- By default, RIPv1 uses the IP broadcast address (255.255.255.255) to advertise routing information, whereas RIPv2 uses the multicast address (224.0.0.9) to advertise routing information. If you do not wish all devices on the broadcast network or NBMA network to receive routing information, configure a corresponding interface as the passive interface and specify the neighbors that can receive routing information. This command does not affect the receiving of RIP packets. RIPv2 packets are broadcast on an interface.
- Unless otherwise required, this function must be enabled on a router that unicasts update packets.

Broadcasting RIPv2 Packets on an Interface

- This function must be configured if the neighbor router does not support the receiving of multicast RIPv2 packets.
- Unless otherwise required, this function must be configured on each router interface that broadcasts RIPv2 packets.

Allowing an Interface to Receive RIP Packets

- This function is enabled by default, and must be disabled if an interface is not allowed to receive RIP packets.
- Unless otherwise required, this function must be configured on each router interface that is not allowed to receive RIP packets.

Allowing an Interface to Send RIP Packets

- This function is enabled by default, and must be disabled if an interface is not allowed to send RIP packets.
- Unless otherwise required, this function must be configured on each router interface that is not allowed to send RIP packets.

Allowing an Interface to Send RIP Packets of a Specified Version

- This function must be configured if the version of RIP packets that can be sent on an interface is required to be different from the global configuration.
- Unless otherwise required, this function must be configured on each router interface that is allowed to send RIP packets of a specified version.

Allowing an Interface to Receive RIP Packets of a Specified Version

- This function must be configured if the version of RIP packets that can be received on an interface is required to be different from the global configuration.

- Unless otherwise required, this function must be configured on each router interface that is allowed to receive RIP packets of a specified version.

Verification

Run the **debug ip rip packet** command to verify the packet sending result and packet type.

Related Commands

Unicasting RIP Route Update Packets to a Specified Neighbor

Command Syntax	**neighbor** *ip-address*
Parameter Description	*ip-address:* Indicates the IP address of the neighbor. It should be the address of the network directly connected to the local device.
Command Mode	Routing process configuration mode
Configuration Usage	You can first run the **passive-interface** command in routing process configuration mode to configure the related interface as a passive interface, and then specify the neighbors that can receive routing information. This command does not affect the receiving of RIP packets. After an interface is configured as a passive interface, the interface does not send the request packets even after the device is restarted.

Broadcasting RIPv2 Packets on an Interface

Command Syntax	**ip rip v2-broadcast**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of sending RIP packets on the interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets is determined by the **version** command.

Allowing an Interface to Receive RIP Packets

Command Syntax	**ip rip receive enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	To prohibit an interface from receiving of RIP packets, use the **no** form of this command. This command takes effect only on the interface. You can use the **default** form of the command to restore the default setting, that is, allow the interface to receive RIP packets.

Allowing an Interface to Send RIP Packets

Command Syntax	**ip rip send enable**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	To prohibit an interface from sending RIP packets, use the **no** form of this command in interface configuration mode. This command takes effect only on the interface. You can use the **default** form of the command to restore the default setting, that is, allow the interface to send RIP packets.

Allowing an Interface to Send RIP Packets of a Specified Version

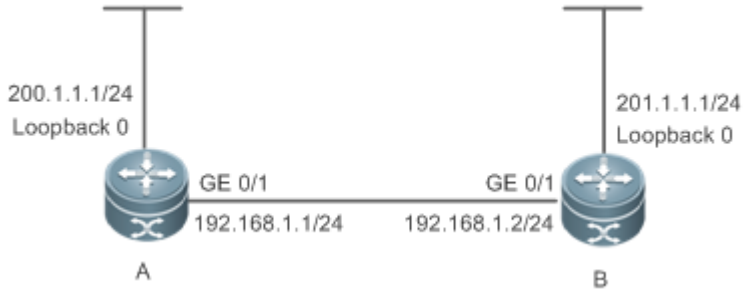
Command Syntax	**ip rip send version** [**1**] [**2**]
Parameter Description	**1**: Indicates that only RIPv1 packets are sent. **2**: Indicates that only RIPv2 packets are sent.
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of sending RIP packets on the interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets is determined by the **version** command.

Allowing an Interface to Receive RIP Packets of a Specified Version

Command Syntax	**ip rip receive version** [**1**] [**2**]
Parameter Description	**1**: Indicates that only RIPv1 packets are received. **2**: Indicates that only RIPv2 packets are received.
Command Mode	Interface configuration mode
Configuration Usage	The default behavior is determined by the **version** command. The configuration result of this command can overwrite the default configuration of the **version** command. This command affects the behavior of sending RIP packets on the interface, and the interface is allowed to send RIPv1 and RIPv2 packets simultaneously. If this command does not contain any parameter, the behavior of receiving RIP packets is determined by the **version** command.

Configuration Example

Prohibiting an Interface from Sending RIP Packets

Scenario **Figure 1-8**	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Prohibit an interface of Router A from sending RIP packets.

A	`A# configure terminal`
	`A(config)# interface GigabitEthernet 0/1`
	`Ruijie(config-if-GigabitEthernet 0/1)# no ip rip send enable`

Verification	● Run the **debug ip rip packet send** command on Router A, and verify that packets cannot be sent.

A	`A# debug ip rip packet recv`
	`*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Prepare to send BROADCAST response...`
	`*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Building update entries on GigabitEthernet 0/1`
	`*Nov 4 08:19:31: %RIP-7-DEBUG: 117.0.0.0/8 via 0.0.0.0 metric 1 tag 0`
	`*Nov 4 08:19:31: %RIP-7-DEBUG: [RIP] Interface GigabitEthernet 0/1 is disabled to send RIP packet!`

Common Errors

- A compatibility error occurs because the RIP version configured on the neighbor is different from that configured on the local device.

1.4.3 Enabling Triggered Update

Configuration Effect

- Enable the RIP triggered update function. When this function is configured, RIP does not periodically send route update packets.

Notes

- Basic RIP functions must be configured.
- It is recommended that split horizon with poison reverse be enabled; otherwise, invalid routing information may exist.
- Ensure that the triggered update function is enabled on each router on the same link; otherwise, routing information cannot be exchanged properly.

Configuration Step

Enabling Triggered Update

- This function must be enabled if on-demand links are configured on the WAN interface.
- The triggered update function can be enabled when the interface has only one neighbor, or when the interface has multiple neighbors but the device interacts with these neighbors in unicast mode.
- It is recommended that triggered update be enabled on a WAN interface running PPP, Frame Relay (FR), or X.25 to meet requirements of on-demand links.
- If the triggered update function is enabled on an interface, source address verification is performed regardless of whether source address verification is enabled by the **validate-update-source** command.
- Unless otherwise required, triggered update must be enabled on on-demand links of each router.

Verification

When the RIP triggered update function is enabled, RIP cannot periodically send route update packets. RIP sends the route update packets to the WAN interface only in one of the following cases:

- A route request packet is received.
- RIP routing information changes.
- The interface state changes.
- The router is started.

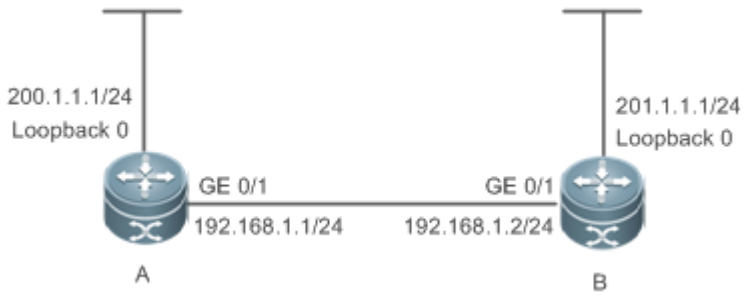
Related Commands

Enabling Triggered Update

Command Syntax	**ip rip triggered** { **retransmit-timer** *timer* | **retransmit-count** *count* }
Parameter Description	**retransmit-timer** *timer*: Configures the interval at which update request or response packets are retransmitted. The default value is 5s. The value range is from 1 to 3600. **retransmit-count** *count*: Configures the maximum retransmission count of update request or response packets. The default value is 36. The value range is from 1 to 3600.
Command Mode	Interface configuration mode
Configuration Usage	You can run the **ip rip triggered** command to enable the triggered update function. When this function is enabled, the RIP periodical update function is automatically disabled. Therefore, the acknowledgment and retransmission mechanisms must be used to ensure that update packets are successfully sent or received on the WAN. You can use the **retransmit-timer** and **retransmit-count** parameters to specify the retransmission interval and maximum retransmission count of request and update packets.

Configuration Example

Enabling Triggered Update

Scenario **Figure 1-9**	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● On Router A, enable the RIP triggered update function, and set the retransmission interval and maximum retransmission count of request and update packets to 10s and 18, respectively.

A	`A# configure terminal`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# encapsulation ppp`
	`A(config-if-GigabitEthernet 0/1)# ip rip triggered`
	`A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-timer 10`
	`A(config-if-GigabitEthernet 0/1)# ip rip triggered retransmit-count 18`
	`A(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse`
	`A(config)# router rip`
	`A(config-router)# network 192.168.1.0`
	`A(config-router)# network 200.1.1.0`

B	`B# configure terminal`
	`B(config)# interface GigabitEthernet 0/1`
	`B(config-if-GigabitEthernet 0/1)# encapsulation ppp`
	`B(config-if-GigabitEthernet 0/1)# ip rip triggered`
	`B(config-if-GigabitEthernet 0/1)# ip rip split-horizon poisoned-reverse`
	`B(config)# router rip`
	`B(config-router)# network 192.168.1.0`
	`B(config-router)# network 201.1.1.0`

Verification	● On Router A and Router B, check the RIP database and verify that corresponding routes are permanent.

A	`A# sho ip rip database`
	`201.1.1.0/24  auto-summary`
	`201.1.1.0/24`
	`[1] via 192.168.12.2 GigabitEthernet 0/1  06:25  permanent`

B	`B# sho ip rip database`
	`200.1.1.0/24  auto-summary`
	`200.1.1.0/24`
	`  [1] via 192.168.12.1 GigabitEthernet 0/1  06:25  permanent`

Common Errors

- The triggered update function is enabled when the RIP configurations at both ends of the link are consistent.
- The triggered update function is not enabled on all routers on the same link.

1.4.4 Enabling Source Address Verification

Configuration Effect

- The source address of the received RIP route update packet is verified.

Notes

- Basic RIP functions must be configured.

Configuration Step

↘ Enabling Source Address Verification

- This function is enabled by default, and must be disabled if not required.
- After split horizon is disabled on an interface, the RIP routing process will perform source address verification on the update packet regardless of whether the **validate-update-source** command is executed in routing process configuration mode.
- Source address verification is invalid for the interface with the unnumbered IP address regardless of whether the **validate-update-source** command is executed in routing process configuration mode.
- Unless otherwise required, this function must be disabled on each router that does not require source address verification.

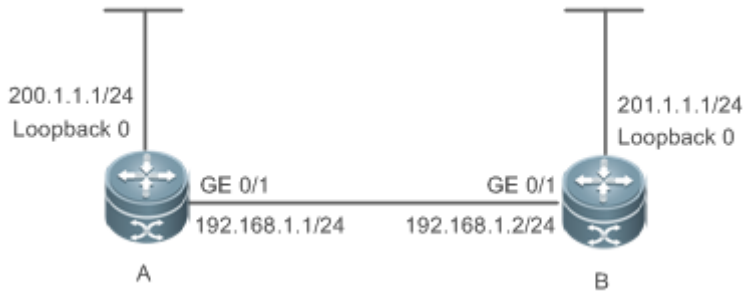
Verification

- Only the route update packets coming from the same IP subnet neighbor are received.

Related Commands

Command Syntax	**validate-update-source**
Parameter Description	N/A
Command Mode	Routing process configuration mode
Configuration Usage	Source address verification of update packets is enabled by default. After this function is enabled, the source address of RIP route update packets is verified. This ensure that the RIP routing process receives only route update packets coming from the same IP subnet neighbor.

Configuration Example

Scenario **Figure 1-10**	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Disable source address verification of update packets on all routers.

A	`A# configure terminal`
	`A(config)# router rip`
	`A(config-router)# no validate-update-source`

B	`B# configure terminal`
	`B(config)# router rip`
	`B(config-router)# no validate-update-source`

Verification	● On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. ● On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
A	`A# show ip route rip` `R    201.1.1.0/24 [120/1] via 192.168.2.2, 00:06:11, GigabitEthernet 0/1`
B	`B# show ip route rip` `R    200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1`

1.4.5 Enabling Authentication

Configuration Effect

- Prevent the device from learning unauthenticated and invalid routes or advertising valid routes to unauthorized devices, ensuring stability of the system and protecting the system against intrusions.

Notes

- Basic RIP functions must be configured.
- Only RIPv2 supports authentication of RIP packets, and RIPv1 does not.

Configuration Step

↘ Enabling Authentication and Specifying the Keychain Used for RIP Authentication

- This configuration is mandatory if authentication must be enabled.
- If the keychain is already specified in interface configuration mode, run the **key chain** command in global configuration mode to define the keychain; otherwise, RIP packets may fail to be authenticated.
- Unless otherwise required, this configuration must be performed on each router that requires authentication.

↘ Defining the RIP Authentication Mode

- This configuration is mandatory if authentication must be enabled.
- The RIP authentication modes configured on all devices that need to directly exchange RIP routing information must be the same; otherwise, RIP packets may fail to be exchanged.
- If cleartext authentication is used, but the keychain for cleartext authentication is not configured or associated, authentication is not performed. Similarly, if MD5 authentication is used, but the keychain is not configured or associated, authentication is not performed.
- Unless otherwise required, this configuration must be performed on each router that requires authentication.

Enabling RIP Cleartext Authentication and Configuring the Keychain

- This configuration is mandatory if authentication must be enabled.
- If RIP cleartext authentication should be enabled, use this command to configure the keychain for cleartext authentication. Alternatively, you can obtain the keychain for cleartext authentication by associating the keychain. The keychain obtained using the second method takes precedence over that obtained using the first method.
- Unless otherwise required, this configuration must be performed on each router that requires authentication.

Verification

- RIP cleartext authentication provides only limited security because the password transferred through packets is visible.
- RIP MD5 authentication can provide higher security because the password transferred through packets is encrypted using the MD5 algorithm.
- Routes can be learned properly if correct authentication parameters are configured.
- Routes cannot be learned if the incorrect authentication parameters are configured.

Related Commands

Enabling Source Address Verification

Command Syntax	**ip rip authentication key-chain** *name-of-keychain*
Parameter Description	*name-of-keychain*: Specifies the name of the keychain used for RIP authentication.
Command Mode	Interface configuration mode
Configuration Usage	The specified keychain must be defined by the **key chain** command in global configuration mode in advance.

Defining the RIP Authentication Mode

Command Syntax	**ip rip authentication mode** { **text** | **md5** }
Parameter Description	**text:** Indicates that the RIP authentication mode is cleartext authentication. **md5:** Indicates that the RIP authentication mode is MD5 authentication.
Command Mode	Interface configuration mode

Configuration Usage	For all devices that need to directly exchange RIP routing information, the RIP authentication mode of these devices must be the same.

Enabling RIP Cleartext Authentication and Configuring the Keychain

Command Syntax	**ip rip authentication text-password** [**0** | **7**] *password-string*
Parameter Description	**0**: Indicates that the key is displayed in cleartext. **7**: Indicates that the key is displayed in cipher text. *password-string*: Indicates the keychain used for cleartext authentication. The keychain is a string of 1 to 16 bytes.
Command Mode	Interface configuration mode
Configuration Usage	This commands takes effect only in cleartext authentication mode.

Configuration Example

Configuring Basic RIP Functions and Enabling MD5 Authentication

Scenario Figure 1-11	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Configure the authentication type and MD5 authentication key on all routers.

A	`A# configure terminal`
	`A(config)# key chain hello`
	`A(config-keychain)# key 1`
	`A(config-keychain-key)# key-string world`
	`A(config-keychain-key)# exit`
	`A(config-keychain)# exit`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5`
	`A(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello`

B	`B# configure terminal`
	`B(config)# key chain hello`
	`B(config-keychain)# key 1`
	`B(config-keychain-key)# key-string world`
	`B(config-keychain-key)# exit`

	B(config-keychain)# exit B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip rip authentication mode md5 B(config-if-GigabitEthernet 0/1)# ip rip authentication key-chain hello
Verification	● On Router A, check the routing table and verify that the entry 201.1.1.0/24 is loaded. ● On Router B, check the routing table and verify that the entry 200.1.1.0/24 is loaded.
A	A# show ip route rip R 201.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1
B	A# show ip route rip R 200.1.1.0/24 [120/1] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1

Common Errors

- The keys configured on routers that need to exchange RIP routing information are different.
- The authentication modes configured on routers that need to exchange RIP routing information are different.

1.4.6 Enabling Route Summarization

Configuration Effect

Route summarization reduces the size of the routing table, improves the routing efficiency, avoids route flapping to some extent, and improves scalability and effectiveness of the network.

- If a summarized route exists, sub-routes included by the summarized route cannot be queried in the routing table, which greatly reduces the size of the routing table.
- Advertising a summarized route is more efficient than advertising individual routes because a summarized route is processed first when RIP looks up the database. Furthermore, all sub-routes are ignored when RIP looks up the database, which reduces the processing time required.

Notes

- Basic RIP functions must be configured.
- The range of supernetting routes is larger than that of the classful network. Therefore, automatic route summarization is invalid for supernetting routes.
- RIPv1 always performs automatic route summarization. If the detailed routes should be advertised, you must set the RIP version to RIPv2.

Configuration Step

Enabling Automatic Route Summarization

- This function is enabled by default.
- To learn specific subnet routes but not summarized network routes, you must disable automatic route summarization.
- You can disable automatic route summarization only in RIPv2. RIPv1 always performs automatic route summarization.

Configuring RIP Route Summarization on an Interface

- This function must be configured if classful subnets need to be summarized.
- The **ip rip summary-address** command is used to summarize an address or a subnet on a specified interface. RIP automatically summarizes subnet routes to the classful network boundary. Each classful subnet can be configured only in the **ip rip summary-address** command.
- The summarization range configured in this command cannot be supernetting routes, that is, the configured subnet mask length cannot be smaller than the natural mask length of the network.
- Unless otherwise required, this configuration should be performed on a router that requires classful subnet summarization.

Verification

Verify that the routes are summarized in the routing table of the peer end.

Related Commands

Enabling Automatic Route Summarization

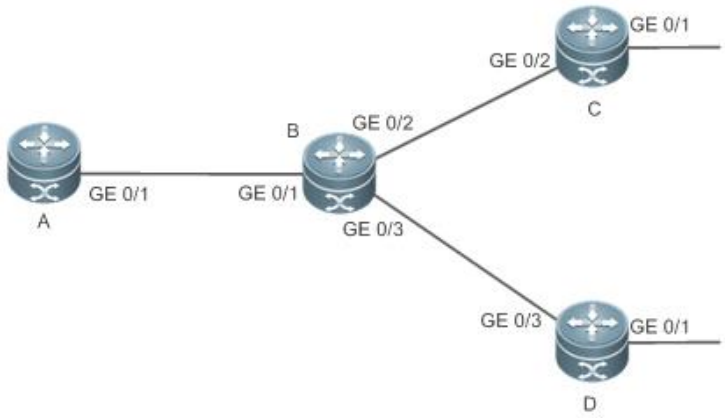
Command Syntax	**auto-summary**
Parameter Description	N/A
Command Mode	Routing process configuration mode
Configuration Usage	Route summarization is enabled by default for RIPv1 and RIPv2. You can disable automatic route summarization only in RIPv2. RIPv1 always performs automatic route summarization.

Configuring RIP Route Summarization on an Interface

Command Syntax	**ip rip summary-address** *ip-address ip-network-mask*
Parameter Description	*ip-address*: Indicates the IP address to be summarized. *ip-network-mask*: Indicates the subnet mask of the IP address to be summarized.
Command Mode	Interface configuration mode
Configuration Usage	This command is used to summarize an address or a subnet on a specified interface.

Configuration Example

Configuring Route Summarization

Scenario **Figure 1-12**	 **Remarks**: Interfaces' IP addresses are as follows: A: GE0/1: 192.168.1.1 B: GE0/1: 192.168.1.2; GE0/2: 172.16.2.1; GE0/3: 172.16.3.1 C: GE0/2: 172.16.2.2; GE0/3: 172.16.4.2 D: GE0/2: 172.16.3.2; GE0/3: 172.16.5.2
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Configure route summarization on Router B.

	`B# configure terminal`
	`B(config)# interface GigabitEthernet 0/1`
	`B(config-if-GigabitEthernet 0/1)# ip rip summary-address 172.16.0.0 255.255.0.0`
	`B(config)# router rip`
	`B(config-router)# version 2`
	`B(config-router)# no auto-summary`

Verification	● Check the routing table on Router A, and verify that the entry 172.16.0.0/16 is generated.
	`A# show ip route rip` `R 172.16.0.0/16 [120/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1`

Common Errors

- Basic RIP functions are not configured or fail to be configured.

1.4.7 Enabling Supernetting Routes

Configuration Effect

- Allow RIP to send RIP supernetting routes on a specified interface.

Notes

- Basic RIP functions must be configured.

Configuration Step

↘ **Enabling Supernetting Routes**

- If a supernetting route is detected when a RIPv1-enabled router detects RIPv2 route response packets, the router will learn an incorrect route because RIPv1 ignores the subnet mask in routing information of packets. In this case, the **no** form of the command must be used on the RIPv2-enabled router to prohibit supernetting routes from being advertised on the related interface. This command takes effect only on the current interface.
- The command is effective only when RIPv2 packets are sent on the interface, and is used to control the sending of supernetting routes.

Verification

Verify that the peer router cannot learn the supernetting route.

Related Commands

Command Syntax	**ip rip send supernet-routes**
Parameter Description	N/A
Command Mode	Interface configuration mode
Configuration Usage	By default, an interface is allowed to send RIP supernetting routes.

Configuration Example

Disabling Supernetting Routes

Scenario Figure 1-13	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Prohibit RIP supernetting routes from being sent on GigabitEthernet 0/1 of Router B.

	`B# configure terminal`
	`B(config)# ip route 207.0.0.0 255.0.0.0 Null 0`
	`B(config)# ip route 208.1.1.0 255.255.255.0 Null 0`
	`B(config)# router rip`
	`B(config-router)# redistribute static`
	`B(config)# interface GigabitEthernet 0/1`
	`B(config-if-GigabitEthernet 0/1)# no ip rip send supernet-routes`

Verification	● Check the routing table on Router A, and verify that Router A can learn only the non-supernetting route 208.1.1.0/24, but not the supernetting route 207.0.0.0/8.
	`A#show ip route rip` `R  208.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1`

1.4.8 Advertising the Default Route or External Routes

Configuration Effect

- In the RIP domain, introduce a unicast route of another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.
- In the RIP domain, inject a default route to another AS so that the unicast routing service to this AS can be provided for users in the RIP domain.

Notes

- Basic RIP functions must be configured.
- Route redistribution cannot introduce default routes of other protocols to the RIP routing domain.

Configuration Step

↘ Advertising the Default Route to Neighbors

This function must be enabled if required.

By default, a default route is not generated, and the metric of the default route is 1.

If the RIP process can generate a default route using this command, RIP does not learn the default route advertised by the neighbor.

Unless otherwise required, this configuration should be performed on a router that needs to advertise the default route.

↘ Advertising the Default Route to Neighbors on an Interface

This function must be enabled if required.

By default, a default route is not configured and the metric of the default route is 1.

After this command is configured on an interface, a default route is generated and advertised through this interface.

Unless otherwise required, this configuration should be performed on a router that needs to advertise the default route.

↘ Redistributes Routes and Advertises External Routes to Neighbors

This function must be enabled if routes of other protocols need to be redistributed.

The default settings are as follows:

- If OSPF redistribution is configured, the device redistributes the routes of all sub-types of the OSPF process.
- If IS-IS redistribution is configured, the device redistributes the level-2 routes of the IS-IS process.
- In other cases, the device redistributes all external routes.
- The metric of a redistributed route is 1 by default.
- The route map is not associated by default.

During route redistribution, the device does not need to convert the metric of one routing protocol to the metric of another routing protocol because different routing protocols use different metric measurement methods. RIP measures the metric based on the hop count, and OSPF measures the metric based on the bandwidth. Therefore, the computed metrics cannot be compared with each other. During route redistribution, configure a symbolic metric; otherwise, route redistribution fails.

Unless otherwise required, this configuration should be performed on a router that needs to redistribute routes.

Verification

- On a neighboring device, verify that a default route exists in the RIP routing table.
- On the local and neighboring devices, verify that external routes (routes to other ASs) exist in the RIP routing table.

Related Commands

Advertising the Default Route to Neighbors

Command Syntax	**default-information originate** [**always**] [**metric** *metric-value*] [**route-map** *map-name*]
Parameter Description	**always:** Enables RIP to generate a default route regardless of whether the local router has a default route. **metric** *metric-value:* Indicates the initial metric of the default route. The value range is from 1 to 15. **route-map** *map-name:* Indicates the associated route map name. By default, no route map is associated.
Command Mode	Routing process configuration mode
Configuration Usage	If a default route exists in the routing table of a router, RIP does not advertise the default route to external entities by default. You need to run the **default-information originate** command in routing process configuration mode to advertise the default route to neighbors. If the **always** parameter is selected, the RIP routing process advertises a default route to neighbors regardless of whether the default route exists, but this default route is not displayed in the local routing table. To check whether the default route is generated, run the **show ip rip database** command to check the RIP routing information database. To further control the behavior of advertising the RIP default route, specify **route-map**. For example, use **set metric** to set the metric of the default route. You can use the **metric** parameter to set the metric of the advertised default value, but the priority of this configuration is lower than that of the set metric rule of the **route-map** parameter. If the **metric** parameter is not configured, the default route uses the default metric configured for RIP. You still need to run the **default-information originate** command to introduce the default route generated by **ip default-network** to RIP.

Advertising the Default Route to Neighbors on an Interface

Command Syntax	**ip rip default-information** { **only** | **originate** } [**metric** *metric-value*]
Parameter Description	**only**: Indicates that only the default route is advertised. **originate**: Indicates that the default route and other routes are advertised. **metric** *metric-value:* Indicates the metric of the default route. The value range is from 1 to 15.
Command Mode	Interface configuration mode
Configuration	If you configure the **ip rip default-information** command for the interface and the

Usage	**default-information originate** command for the RIP process, only the default route configured for the interface is advertised. If **ip rip default-information** is configured for one interface, RIP does not learn the default route advertised by the neighbor.

Redistributes Routes and Advertises External Routes to Neighbors

Command Syntax	**redistribute** { **bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **static** } [{ **level-1 | level-1-2 | level-2** }] [**match** { **internal | external** [**1 | 2**] **| nssa-external** [**1 | 2**] }] [**metric** *metric-value*] [**route-map** *route-map-name*]
Parameter Description	**bgp**: Indicates redistribution from BGP. **connected**: Indicates redistribution from direct routes. **isis** *area-tag*: Indicates redistribution from IS-IS. *area-tag* indicates the IS-IS process ID. **ospf** *process-id*: Indicates redistribution from OSPF. *process-id* indicates the OSPF process ID. The value range is from 1 to 65535. **static**: Indicates redistribution from static routes. **level-1** | **level-1-2** | **level-2**: Is used only when IS-IS routes are redistributed. Only the routes of the specified level are redistributed. **match**: Is used only when OSPF routes are redistributed. Only the routes that match the filtering conditions are redistributed. **metric** *metric-value*: Sets the metric of the redistributed route. The value range is from 1 to 16. **route-map** *route-map-name*: Sets the redistribution filtering rule.
Command Mode	Routing process configuration mode
Configuration Usage	When you configure redistribution of IS-IS routes without specifying the **level** parameter, only level-2 routes can be redistributed by default. If you specify the **level** parameter during initial configuration of redistribution, routes of the specified level can be redistributed. If both **level-1** and **level-2** are configured, the two levels are combined and saved as **level-1-2**. If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can use the **no** form of the command to restore the default value of **match**. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted. For example, if **redistribute isis 112 level-2** is configured, you can run the **no redistribute isis 112 level-2** command to restore the default value of **level-2**. As level-2 itself is the default value of the parameter, the configuration saved is still **redistribute isis 112 level-2** after the preceding **no** form of the command is executed. To delete the entire command, run the **no redistribute isis 112** command.

Configuration Example

Redistributing Routes and Advertising External Routes to Neighbors

Scenario **Figure 1-14**	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● On Router B, configure redistribution of static routes.

B	`B# configure terminal`
	`B(config)# router rip`
	`B(config-router)# redistribute static`

Verification	● On Router A, check the routing table and verify that the entry 172.10.10.0/24 is loaded.
	`A# show ip route rip` `R    172.10.10.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1`

1.4.9 Setting Route Filtering Rules

Configuration Effect

- Routes that do not meet filtering criteria cannot be loaded to the routing table, or advertised to neighbors. In this way, users within the network can be prevented from accessing specified destination networks.

Notes

- Basic RIP functions must be configured.
- For filtering rules of sent routes, you must configure route redistribution first, and then filter the redistributed routes.

Configuration Step

↘ Filtering the Received RIP Routing Information

- This function must be configured if required.
- To prevent the device from receiving some specified routes, you can configure the route distribution control list to process all the received route update packets. If no interface is specified, route update packets received on all interfaces will be processed.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

↘ Filtering the Sent RIP Routing Information

- This function must be configured if required.
- If this command does not contain any optional parameter, route update advertisement control takes effect on all interfaces. If the command contains the interface parameter, route update advertisement control takes effect only on the specified interface. If the command contains other routing process parameters, route update advertisement control takes effect only on the specified routing process.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Verification

- Run the **show ip route rip** command to verify that the routes that have been filtered out are not loaded to the routing table.

Related Commands

Filtering the Received RIP Routing Information

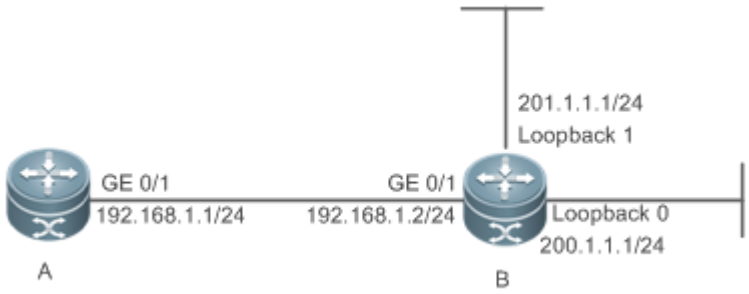
Command Syntax	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]
Parameter Description	*access-list-number* | *name*: Specifies the access list. Only routes permitted by the access list can be received. **prefix** *prefix-list-name*: Uses the prefix list to filter routes. **gateway** *prefix-list-name*: Uses the prefix list to filter the route sources. *interface-type interface-number*: Indicates that the distribution list is applied to the specified interface.
Command Mode	Routing process configuration mode
Configuration Usage	N/A

Filtering the Sent RIP Routing Information

Command Syntax	**distribute-list** { [*access-list-number* | *name*] | **prefix** *prefix-list-name* } **out** [*interface* **|** [**bgp | connected | isis** [*area-tag*] **| ospf** *process-id* **| rip | static**]]
Parameter Description	*access-list-number* | *name*: Specifies the number of an access control list (ACL). Only routes permitted by the ACL can be sent. **prefix** *prefix-list-name*: Uses the prefix list to filter routes. *Interface*: Applies route update advertisement control only on the specified interface. **bgp**: Applies route update advertisement control only on the routes introduced from BGP. **connected**: Applies route update advertisement control only on direct routes introduced through redistribution. **isis** [*area-tag*]: Applies route update advertisement control only on the routes introduced from IS-IS. *area-tag* specifies an IS-IS process. **ospf** *process-id*: Applies route update advertisement control only on the routes introduced from OSPF. *process-id* specifies an OSPF process. **rip**: Applies route update advertisement control only on RIP routes. **static**: Applies route update advertisement control only on static routes introduced through redistribution.
Command Mode	Routing process configuration mode
Configuration Usage	N/A

Configuration Example

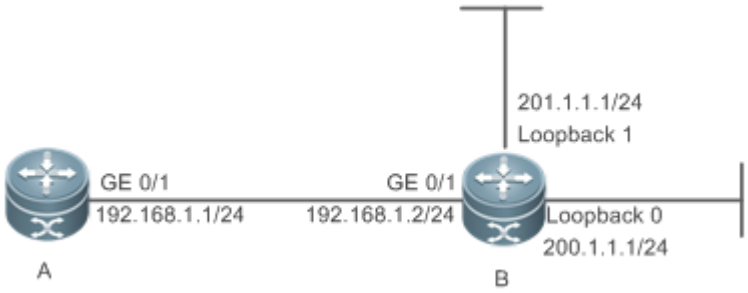
Filtering the Received RIP Routing Information

Scenario **Figure 1-15**	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Enable the RIP routing process to control routes received over GigabitEthernet 0/1 and receive only the route 200.1.1.0.

A	`A# configure terminal`
	`A(config)# router rip`
	`A(config-router)# distribute-list 10 in GigabitEthernet 0/1`
	`A(config-router)# no auto-summary`
	`A(config)# access-list 10 permit 200.1.1.0 0.0.0.255`

Verification	● On Router A, check the routing table and verify that only the entry 200.1.1.0/24 exists.
A	`A# show ip route rip` `R    200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1`

Filtering the Sent RIP Routing Information

Scenario **Figure 1-16**	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Enable the RIP routing process to advertise only the route 200.1.1.0/24.

B	`B# configure terminal`
	`B(config)# router rip`
	`B(config-router)# redistribute connected`
	`B(config-router)# distribute-list 10 out`
	`B(config-router)# version 2`
	`B(config)# access-list 10 permit 200.1.1.0 0.0.0.255`

Verification	● Check the routing table on Router A, and verify that route on the network segment 200.1.1.0 exists.
A	`A# show ip route rip`

	`R  200.1.1.0/24 [120/1] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1`

Common Errors

- Filtering fails because the filtering rules of the access list are not properly configured.

1.4.10 Changing Route Selection Parameters

Configuration Effect

- Change RIP routes to enable the traffic to pass through specified nodes or prevent it passing through specified nodes.
- Change the sequence that a router selects various types of routes so as to change the priorities of RIP routes.

Notes

- Basic RIP functions must be configured.

Configuration Step

Changing the Administrative Distance of a RIP Route

- Optional.
- This configuration is mandatory if you wish to change the priorities of RIP routes on a router that runs multiple unicast routing protocols.

Increasing the Metric of a Received or Sent RIP Route

- Optional.
- Unless otherwise required, this configuration should be performed on a router where the metrics of routes need to be adjusted.

Configuring the Default Metric of an External Route Redistributed to RIP

- Optional.
- Unless otherwise required, this configuration must be performed on an ASBR to which external routes are introduced.

Verification

Run the **show ip rip** command to display the configured administrative distance. Run the **show ip rip data** command to display the metrics of redistributed routes to verify that the configuration takes effect.

Related Commands

Changing the Administrative Distance of a RIP Route

Command Syntax	**distance** *distance* [*ip-address wildcard*]
Parameter Description	*distance*: Sets the administrative distance of a RIP route. The value is an integer ranging from 1 to 255.

	ip-address: Indicates the prefix of the source IP address of the route. *wildcard*: Defines the IP address comparison bit. The value 0 indicates accurate matching, and the value 1 indicates that no comparison is performed.
Command Mode	Routing process configuration mode
Configuration Usage	Run this command to configure the administrative distance of a RIP route.

Increasing the Metric of a Received or Sent RIP Route

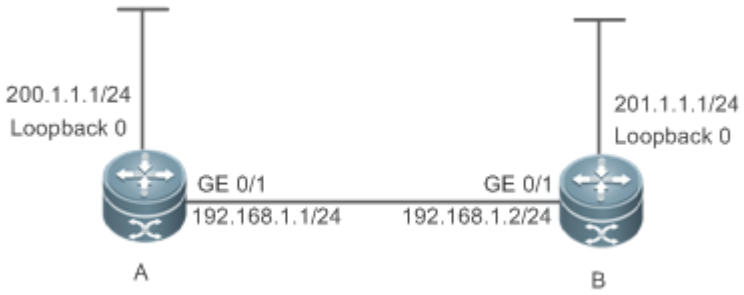
Command Syntax	**offset-list** { *access-list-number* | *name* } { **in** | **out** } *offset* [*interface-type interface-number*]
Parameter Description	*access-list-number* | *name*: Specifies the number of name of an access control list (ACL). **In**: Uses the ACL to modify the metric of a received route. **out**: Uses the ACL to modify the metric of a sent route. *offset*: Indicates the offset of the modified metric. The value range is from 0 to 16. *interface-type*: Uses the ACL on the specified interface. *interface-number*: Specifies the interface number.
Command Mode	Routing process configuration mode
Configuration Usage	Run this command to increase the metric of a received or sent RIP route. If the interface is specified, the configuration takes effect only on the specified interface; otherwise, the configuration takes effect globally.

Configuring the Default Metric of an External Route Redistributed to RIP

Command Syntax	**default-metric** *metric-value*
Parameter Description	*metric-value:* Indicates the default metric. The valid value range is from 1 to 16. If the value is equal to or greater than 16, the RGOS determines that this route is unreachable.
Command Mode	Routing process configuration mode
Configuration Usage	This command must be used together with the routing protocol configuration command **redistribute**.

Configuration Example

Increasing the Metric of a Received or Sent RIP Route

Scenario **Figure 1-17**	

Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Increase by 7 the metric of each RIP route in the range specified by ACL 7. ● Increase by 7 the metric of each learned RIP route in the range specified by ACL 8.

A	`A# configure terminal`
	`A(config)# access-list 7 permit host 200.1.1.0`
	`A(config)# access-list 8 permit host 201.1.1.0`
	`A(config)# router rip`
	`A(config-router)# offset-list 7 out 7`
	`A(config-router)# offset-list 8 in 7`

Verification	● Check the routing table on Router A and Router B to verify that the metrics of RIP routes are 8.
A	`A# show ip route rip` `R    201.1.1.0/24 [120/8] via 192.168.1.2, 00:06:11, GigabitEthernet 0/1`
B	`B# show ip route rip` `R    200.1.1.0/24 [120/8] via 192.168.1.1, 00:06:11, GigabitEthernet 0/1`

1.4.11 Changing Values of Timers

Configuration Effect

- Change values of RIP timers to accelerate or slow down the change of the protocol state or occurrence of an event.

Notes

- Basic RIP functions must be configured.
- Changing protocol control parameters may result in protocol running failures. Therefore, you are advised not to change values of timers.

Configuration Step

↘ Changing Values of the Update Timer, Invalid Timer, and Flush Timer

This configuration must be performed if you need to adjust RIP timers.

By adjusting the timers, you can reduce the convergence time and fault rectification time of the routing protocol. For routers connected to the same network, values of the three RIP timers must be the same. In most situations, you are advised not to modify the RIP timers unless otherwise required.

Setting timers to small values on a low-speed link brings risks because a lot of update packets consume the bandwidth. You can set timers to small values on the Ethernet or a 2 Mbps (or above) link to reduce the convergence time of network routes.

Unless otherwise required, this configuration should be performed on a router where RIP timers need to be modified.

↘ Setting the Sending Delay Between RIP Route Update Packets

This configuration must be performed if you need to adjust the sending delay between RIP update packets.

Run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all update packets.

Unless otherwise required, this configuration should be performed on a router where the sending delay needs to be adjusted.

Verification

Run the **show ip rip** command to display settings of RIP timers.

Related Commands

Modifying the Update Timer, Invalid Timer, and Flush Timer

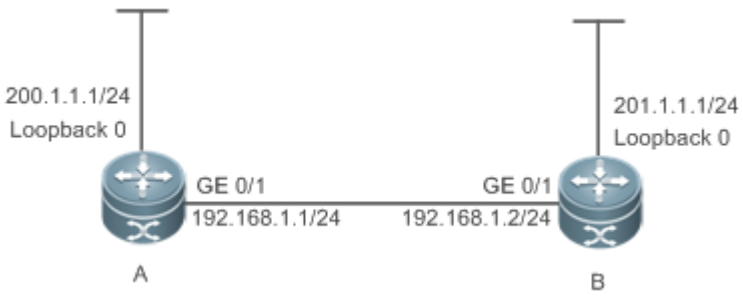
Command Syntax	**timers basic** *update invalid flush*
Parameter Description	*update*: Indicates the interval at which the device sends the route update packets, in seconds. Each time an update packet is received, the invalid timer and flush timer are reset. By default, a routing update packet is sent every 30s. *invalid*: Indicates the time after which the route in the routing list becomes invalid because the route is not updated, in seconds. It is counted from the last time when a valid update packet is received. The duration of the invalid timer must be at least three times the duration of the update timer. If no update packet is received before the invalid timer expires, the corresponding route enters the invalid state. If the update packet is received before the invalid timer expires, the timer is reset. The default value of the invalid timer is 180s. *flush*: Indicates the route flushing time, in seconds. It is counted from the time when the RIP route enters the invalid state. When the flush timer expires, the route in the invalid state will be deleted from the routing table. The default duration of the flush timer is 120s.
Command Mode	Routing process configuration mode
Configuration Usage	By default, the update timer is 30s, the invalid timer is 180s, and the flush timer is 120s.

Setting the Sending Delay Between RIP Route Update Packets

Command Syntax	**output-delay** *delay*
Parameter Description	*delay:* Sets the sending delay between packets, in milliseconds. The value range is from 8 to 50.
Command Mode	Interface configuration mode
Configuration Usage	Typically, a RIP route update packet is 512 bytes long and can contain 25 routes. If the number of routes to be updated exceeds 25, more than one update packet will be sent as fast as possible. When a high-speed device sends a lot of update packets to a low-speed device, the low-speed device may not be able to process all update packets in a timely manner, causing a loss of routing information. In this case, you need to run the **output-delay** command to increase the sending delay between packets on a high-speed device so that a low-speed device can receive and process all update packets.

Configuration Example

Setting the Sending Delay Between RIP Route Update Packets

Scenario **Figure 1-18**	
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● Configure the sending delay of update packets on Router A.

A	`A# configure terminal`
	`A(config)# router rip`
	`A(config-router)# output-delay 30`

Verification	● Capture packets on Router A and compare the sending time of update packets before and after the configuration, and verify that a delay of 30 ms is introduced.

Common Errors

For routers connected to the same network, values of the three RIP timers are not the same.

1.4.12 Enabling GR

Configuration Effect

- When a distributed route switches services from the active card to the standby card, traffic forwarding continues.
- When the RIP process is being restarted, traffic forwarding continues.

Notes

- Basic RIP functions must be configured.
- The GR period is at least twice the RIP route update period.
- During the RIP GR process, ensure that the network is stable.

Configuration Step

Configuring the GR Capability

This configuration must be performed if RIP needs to be gracefully restarted to ensure data forwarding during hot standby switchover.

The GR function is configured based on the RIP process. You can configure different parameters for different RIP processes according to the actual situation.

The GR period is the maximum time from restart of the RIP process to completion of GR. During this period, the forwarding table before the restart is retained, and the RIP route is restored so as to restore the RIP state before the restart. After the restart period expires, RIP exits from the GR state and performs common RIP operations.

Unless otherwise required, this configuration should be performed on every router that needs to be gracefully restarted.

Verification

- Run the **show ip rip** command to display the GR state and configured time.
- Trigger a hot standby switchover, and verify that data forwarding is not interrupted.

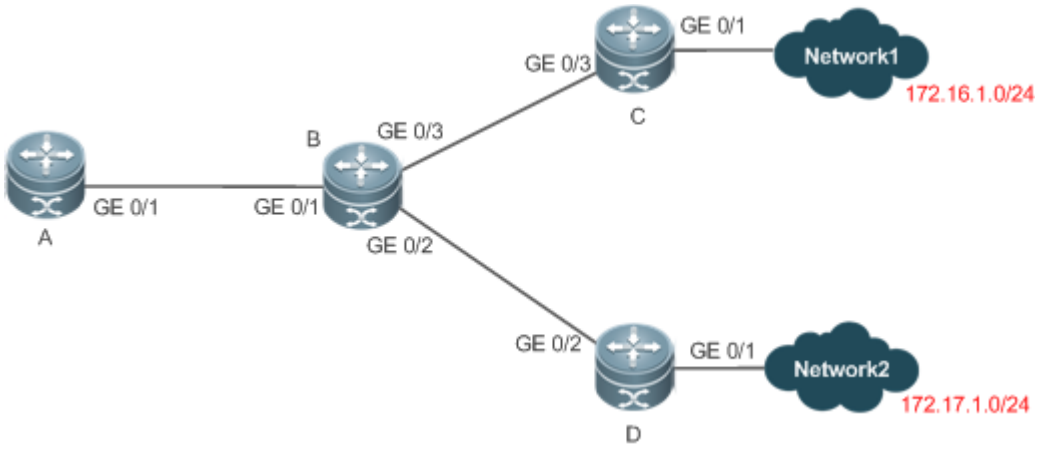
Related Commands

Configuring the GR Capability

Command Syntax	**graceful-restart** [**grace-period** *grace-period*]
Parameter Description	**graceful-restart**: Enables the GR function. **grace-period**: Explicitly configures the grace period. *grace-period*: Indicates the GR period. The value range is from 1s to 1800s. The default value is twice the update time or 60s, which is the smaller.
Command Mode	Routing process configuration mode
Configuration Usage	This command allows you to explicitly modify the GR period. Note that GR must be completed after the update timer of the RIP route expires and before the invalid timer of the RIP route expires. An inappropriate GR period cannot ensure uninterrupted data forwarding during the GR process. A typical case is as follows: If the GR period is longer than the duration of the invalid timer, GR is not completed when the invalid timer expires. The route is not re-advertised to the neighbor, and forwarding of the route of the neighbor stops after the invalid timer expires, causing interruption of data forwarding on the network. Unless otherwise required, you are advised not to adjust the GR period. If it is necessary to adjust the GR period, ensure that the GR period is longer than the duration of the update timer but shorter than the duration of the invalid timer based on the configuration of the **timers basic** command.

Configuration Example

Configuring the GR Capability

Scenario **Figure 1-19**	 **Remarks**: Interfaces' IP addresses are as follows: A: GE 0/1:192.168.1.1 B: GE 0/1: 192.168.1.1; GE 0/2: 192.168.2.1: GE 0/3: 192.168.3.1 C: GE 0/1: 192.168.4.2; GE 0/3: 192.168.3.2 D: GE 0/1: 192.168.5.2; GE 0/2: 192.168.2.2
Configuration Steps	● Configure IP addresses for interfaces on all routers. (The configuration is not mentioned here.) ● Configure basic RIP functions on all routers. (The configuration is not mentioned here.) ● On Router B, enable the GR function.

	`B# configure terminal`
	`B(config)# router rip`
	`B(config-router)# graceful-restart grace-period 90`

Verification	● Trigger a hot standby switchover on Router B, and verify that the routing tables of destination Network 1 and Network 2 remain unchanged on Router A during the switchover. ● Trigger a hot standby switchover on Router B, ping destination Network 1 from Router A, and verify that traffic forwarding is not interrupted during the switchover.

1.5 Monitoring

Displaying

Command	Description
show ip rip	Displays basic information about a RIP process.
show ip rip database [*network-number network-mask*] [**count**]	Displays the RIP routing table.
show ip rip external [**connected** | **ospf** *process-id* | **static**]	Displays information about external routes redistributed by RIP.
show ip rip interface [*interface-type interface-number*]	Displays RIP interface information.
show ip rip peer [*ip-address*]	Displays RIP neighbor information.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description

Command	Description
debug ip rip event	Debugs events that occur when the RIP process is running.
debug ip rip nsm	Debugs interaction with the NSM process.
debug ip rip packet [**interface** *interface-type interface-number* | **recv** | **send**]	Debugs sent and received packets.
debug ip rip restart	Debugs the RIP GR process.
debug ip rip route	Debugs the route changes of the RIP process.

1 Configuring OSPFv2

1.1 Overview

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) that is used within the Autonomous System (AS) to allow routers to obtain a route to a remote network.

OSPF Version 2 (OSPFv2) is applicable to IPv4, and OSPF Version 3 (OSPFv3) is applicable to IPv6. The protocol running mechanism and most configurations are the same.

OSPF has the following characteristics:

- Wide scope of application: OSPF is applicable to a larger-scale network that supports hundreds of routers.
- Fast convergence: Once the network topology changes, notifications can be quickly sent between routers to update routes.
- No self-loop: Only the link status information is synchronized between routers. Each router computes routes independently, and a self-loop will not occur.
- Area division: A large routing domain is divided into multiple small areas to save system resources and network bandwidth and ensure stability and reliability of routes.
- Route classification: Routes are classified into several types to support flexible control.
- Equivalent routes: OSPF supports equivalent routes.
- Authentication: OSPF supports packet authentication to ensure security of protocol interaction.
- Multicast transmission: Protocol packets are sent using the multicast address to avoid interfering with irrelevant entities and save system resources.

In this chapter, the term "router" refers to any network device that supports the routing function. These network devices can be L3 switches, routers, or firewall.

Unless otherwise specified, "OSPF" in the following descriptions refers to OSPFv2.

Protocols and Standards

RFC2328	This memo documents version 2 of the OSPFprotocol. OSPF is a link-state routing protocol.
RFC 2370	This memo defines enhancements to the OSPFprotocol to support a new class of link-state advertisements (LSA) called Opaque LSAs. Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF.
RFC3137	This memo describes a backward-compatible technique that may be used by OSPF (Open Shortest Path First) implementations to advertise unavailability to forward transit traffic or to lower the preference level for the paths through such a router.
RFC3623	This memo documents an enhancement to the OSPF routing protocol, whereby an OSPF router can stay on the forwarding path even as its OSPF software is restarted.

RFC3630	This document describes extensions to the OSPFprotocol version 2 to support intra-area Traffic Engineering (TE), using Opaque Link State Advertisements.
RFC3682	The use of a packet's Time to Live (TTL) (IPv4)or Hop Limit (IPv6) to protect a protocol stack from CPU-utilization based attacks has been proposed in many settings.
RFC3906	This document describes how conventional hop-by-hop link-state routing protocols interact with new Traffic Engineering capabilities to create Interior Gateway Protocol (IGP) shortcuts.
RFC4576	This document specifies the necessary procedure, using one of the options bits in the LSA (Link State Advertisements) to indicate that an LSA has already been forwarded by a PE and should be ignored by any other PEs that see it.
RFC4577	This document extends that specification by allowing the routing protocol on the PE/CE interface to be the OSPF protocol.
RFC4750	This memo defines a portion of the Management Information Base (MIB) for use with network management protocols in TCP/IP-based Internets. In particular, it defines objects for managing version 2 of the Open Shortest Path First Routing Protocol. Version 2 of the OSPF protocol is specific to the IPv4 address family.

1.2 Applications

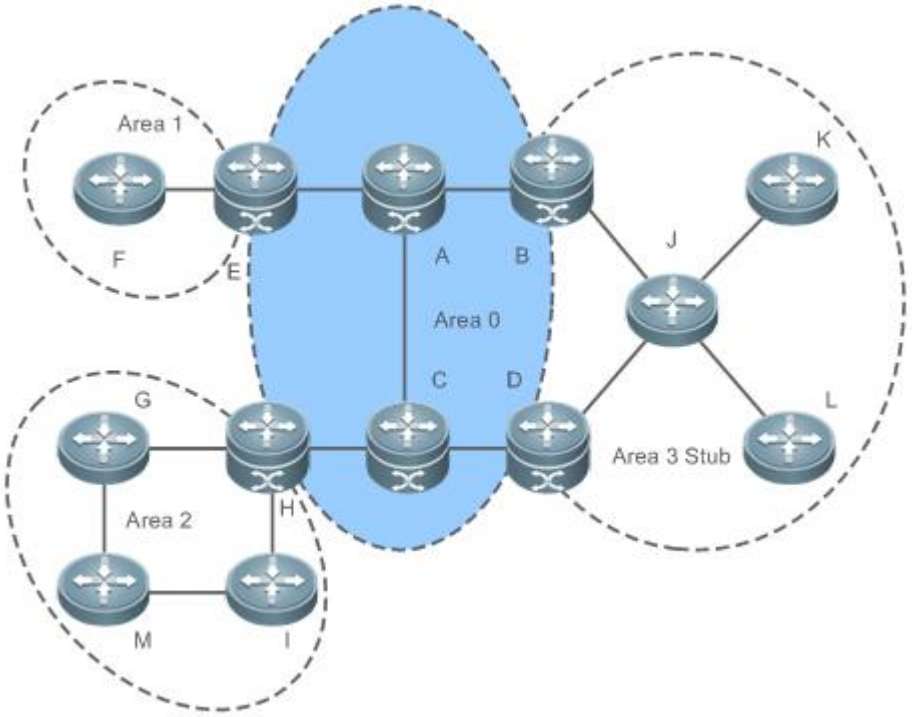
Application	Description
Intra-Domain Interworking	OSPF runs within the AS, which is divided into several areas.

1.2.1 Intra-Domain Interworking

Scenario

OSPF runs within the AS. If the number of routers exceeds 40, it is recommended that the AS be divided into several areas. Generally, high-end devices featuring reliable performance and fast processing speed are deployed in a backbone area, and low-end or medium-range devices with relatively lower performance can be deployed in a normal area. All normal areas must be connected to the backbone area. It is recommended that a normal area located on the stub be configured as a stub area. As shown in Figure 1-1, the network is divided into four areas. Communication between these areas must go through the backbone area, which is area 0.

Figure 1-1 Division of the OSPF Areas



Remarks	A, B, C, D, E, and H are located in the backbone area, and are backbone routers. Area 3 is configured as a stub area.

Deployment

- OSPF runs on all routers within the AS to implement unicast routing.

1.3 Features

Basic Concepts

Routing Domain

All routers in an AS must be interconnected and use the same routing protocol. Therefore, the AS is also called routing domain.

An AS on which OSPF runs is also called OSPF routing domain, or OSPF domain for short.

OSPF Process

OSPF supports multiple instances, and each instance corresponds to an OSPF process.

One or more OSPF processes can be started on a router. Each OSPF process runs OSPF independently, and the processes are mutually isolated.

The process ID takes effect only on the local router, and does not affect exchange of OSPF packets on adjacent interfaces.

RouterID

The router ID uniquely identifies a router in an OSPF domain. Router IDs of any two routers cannot be the same.

If multiple OSPF processes exist on a router, each OSPF process uses one router ID. Router IDs of any two OSPF processes cannot be the same.

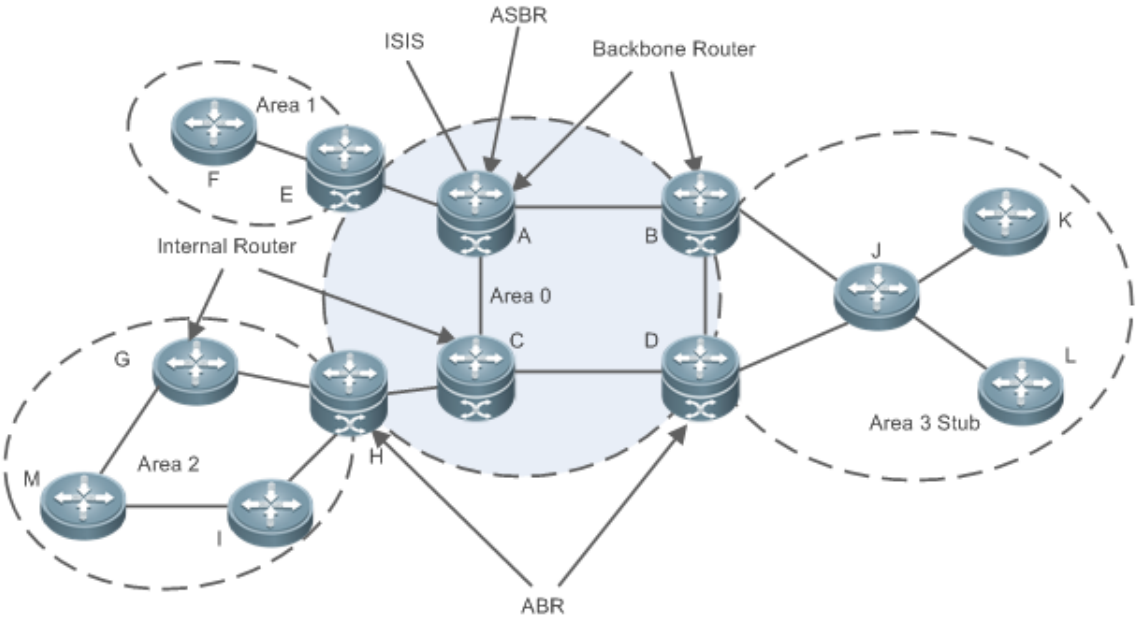
Area

OSPF supports multiple areas. An OSPF domain is divided into multiple areas to ease the computing pressure of a large-scale network.

An area is a logical group of routers, and each group is identified by an area ID. The border between areas is a router. A router may belong to one area or multiple areas. One network segment (link) can belong to only one area, or each OSPF-enabled interface must belong to a specified area.

Area 0 is the backbone area, and other areas are normal areas. Normal areas must be directly connected to the backbone area.

Figure 1-2 Division of the OSPF Areas



OSPF Router

The following types of routers are defined in OSPF, and assigned with different responsibilities:

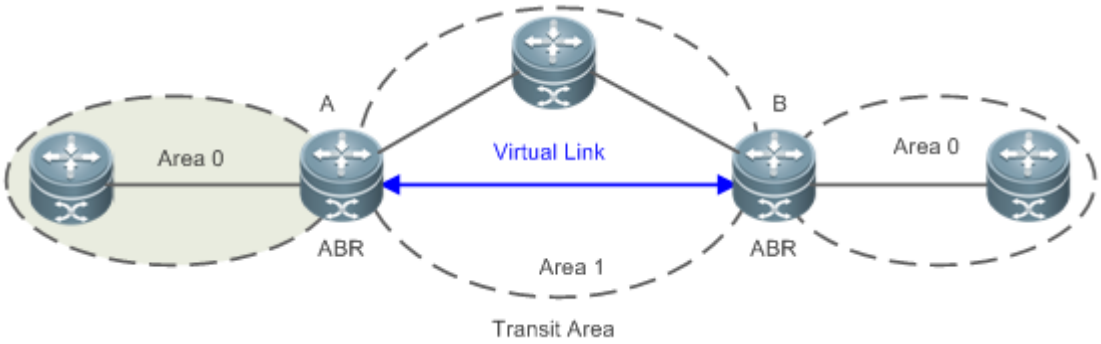
- Internal router
  All interface of an interval router belong to the same OSPF area. As shown in Figure 1-3, A, C, F, G, I, M, J, K, and L are internal routers.
- Area border router (ABR)
  An ABR is used to connect the backbone area with a normal area. An ABR belongs to two or more areas, and one of the areas must be the backbone area. As shown in Figure 1-3, B, D, E, and H are ABRs.
- Backbone router
  A backbone router has at least one interface that belongs to the backbone area. All ABRs and all routers in area 0 are backbone routers. As shown in Figure 1-, A, B, C, D, E, and H are backbone routers.

- AS boundary router (ASBR)
  An ASBR is used to exchange routing information with other ASs. An ASBR is not necessarily located on the border of an AS. It may be a router inside an area, or an ABR. As shown in Figure 1-3, A is an ASBR.

Virtual Link

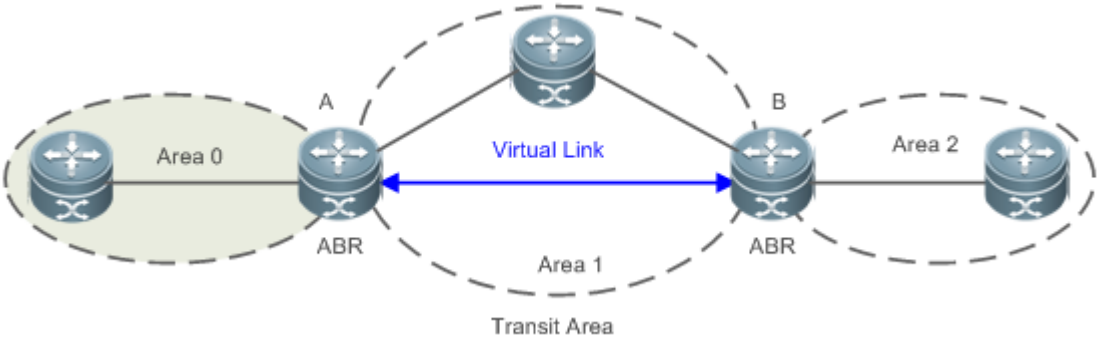
OSPF supports virtual links. A virtual link is a logical link that belongs to the backbone area. It is used to resolve the problems such as a discontinuous backbone area or a failure to directly connect a normal area to the backbone area on the physical network. A virtual link supports traversal of only one normal area, and this area is called transit area. Routers on both ends of a virtual link are ABRs.

Figure 1-3 Discontinuous Backbone Area on the Physical Network



As shown in Figure 1-, a virtual link is set up between A and B to connect two separated area 0s. Area 1 is a transit area, and A and B are ABRs of area 1.

Figure 1-4 Failure to Directly Connect a Normal Area to the Backbone Area on the Physical Network



As shown in Figure 1-, a virtual link is set up between A and B to extend area 0 to B so that area 0 can be directly connected to area 2 on B. Area 1 is a transit area, A is an ABR of area 1, and B is an ABR of area 0 and area 2.

LSA

OSPF describes the routing information by means of Link State Advertisement (LSA).

LSA Type	Description
Router-LSA(Type 1)	This LSA is originated by every router. It describes the link state and cost of the router, and is advertised only within the area where the originating router is located.
Network-LSA(Type 2)	This LSA is originated by a designated routers (DR) on the NBMA network. It describes the link state in the current network segment, and is advertised only within the area where the DR is located.

LSA Type	Description
Network-summary-LSA(Type 3)	This LSA is originated by an ABR. It describes a route to another area, and is advertised to areas except totally stub areas or Not-So-Stubby Area (NSSA) areas.
ASBR-summary-LSA(Type 4)	This LSA is originated by an ABR. It describes a route to an ASBR, and is advertised to areas except areas where the ASBR is located.
AS-external-LSA(Type 5)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised to all areas except the stub and NSSA areas.
NSSA LSA(Type 7)	This LSA is originated by an ABR. It describes a route to a destination outside the AS, and is advertised only within the NASSA areas.
Opaque LSA(Type 9/Type 10/Type 11)	Opaque LSAs provide a generalized mechanism to allow for the future extensibility of OSPF, wherein, ● Type 9 LSAs are only advertised within the network segment where interfaces resides. The Grace LSA used to support graceful restart (GR) is one of Type 9 LSAs. ● Type 10 LSAs are advertised within an area. The LSA used to support Traffic Engineering (TE) is one of Type 10 LSAs. ● Type 11 LSAs are advertised within an AS. At present, there are no application examples of Type 11 LSAs.

Stub areas, NSSA areas, totally stub areas, and totally NSSA areas are special forms of normal areas and help reduce the load of routers and enhance reliability of OSPF routes.

OSPF Packet

The following table lists the protocol packets used by OSPF. These OSPF packets are encapsulated in IP packets and transmitted in multicast or unicast mode.

Packet Type	Description
Hello	Hello packets are sent periodically to discover and maintain OSPF neighbor relationships.
Database Description (DD)	DD packets carry brief information about the local Link-State Database (LSDB) and are used to synchronize the LSDBs between OSPF neighbors.
Link State Request (LSR)	LSR packets are used to request the required LSAs from neighbors. LSR packets are sent only after DD packets are exchanged successfully between OSPF neighbors.
Link State Update (LSU)	LSU packets are used to send the required LSAs to peers.
Link State Acknowledgment (LSAck)	LSAck packets are used to acknowledge the received LSAs.

Overview

Feature	Description
Link-State Routing Protocols	Run OSPF on the router to obtain routes to different destinations on the network.
OSPF Route Management	Plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.

Feature	Description
Enhanced Security and Reliability	Use authentication, MTU verification and GR to enhance security, stability, and reliability of OSPF.
Network Management	Use functions such as the management information base (MIB) and Syslog to facilitate OSPF management.

1.3.1 Link-State Routing Protocols

OSPF is a type of link-state routing protocols. Its working process is as follows:

- Neighbor discovery → Bidirectional communication
  An OSPF neighbor relationship is set up between adjacent routers, and bidirectional communication is maintained.
- Database synchronization → Full adjacency
  A router uses LSAs to advertise all its link states. LSAs are exchanged between neighbors and the link state database (LSDB) is synchronized to achieve full adjacency.
- Shortest Path Tree (SPT) computation → Formation of a routing table
  The router computes the shortest path to each destination network based on the LSDB and forms an OSPF routing table.

Working Principle

↘ Neighbor Discovery → Bidirectional Communication

Routers send Hello packets through all OSPF-enabled interfaces (or virtual links). If Hello packets can be exchanged between two routers, and parameters carried in the Hello packets can be successfully negotiated, the two routers become neighbors. Routers that are mutually neighbors find their own router IDs from Hello packets sent from neighbors, and bidirectional communication is set up.

A Hello packet includes, but is not limited to, the following information:

- Router ID of the originating router
- Area ID of the originating router interface (or virtual link)
- Subnet mask of the originating router interface (or virtual link)
- Authentication information of the originating router interface (or virtual link)
- Hello interval of the originating router interface (or virtual link)
- Neighbor dead interval of the originating router interface (or virtual link)
- Priority of the originating router interface (used for DR/BDR election)
- IP addresses of the DR and Backup Designated Router (BDR)
- Router ID of the neighbor of the originating router

↘ Database Synchronization → Full Adjacency

After bidirectional communication is set up between neighbor routers, the DD, LSR, LSU, and LSAck packets are used to exchange LSAs and set up the adjacency. The brief process is as follows:

- A router generates an LSA to describe all link states on the router.

- The LSA is exchanged between neighbors. When a router receives the LSA from its neighbor, it copies the LSA and saves the copy in the local LSDB, and then advertises the LSA to other neighbors.
- When the router and its neighbors obtain the same LSDB, full adjacency is achieved.

OSPF will be very quiet without changes in link costs or network addition or deletion. If any change takes place, the changed link states are advertised to quickly synchronize the LSDB.

SPT Computation → Formation of a Routing Table

After the complete LSDB is obtained from the router, the Dijkstra algorithm is run to generate an SPT from the local router to each destination network. The SPT records the destination networks, next-hop addresses, and costs. OSPF generates a routing table based on the SPT.

If changes in link costs or network addition or deletion take place, the LSDB will be updated. The router again runs the Dijkstra algorithm, generates a new SPT, and updates the routing table.

The Dijkstra algorithm is used to find a shortest path from a vertex to other vertices in a weighted directed graph.

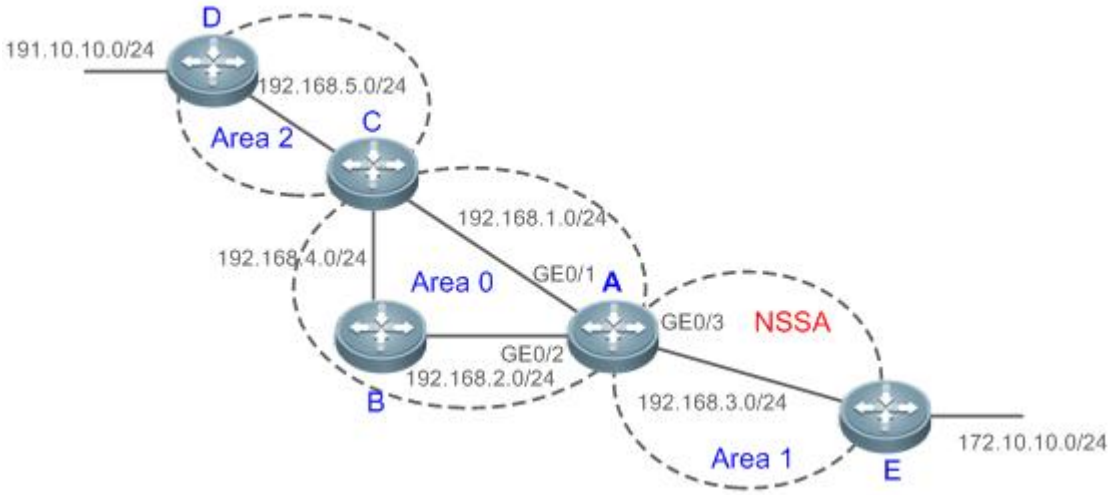
OSPF Network Types

A router does not necessarily need to exchange LSAs with every neighbor and set up an adjacency with every neighbor. To improve efficiency, OSPF classifies networks that use various link layer protocols into five types so that LSAs are exchanged in different ways to set up an adjacency:

- Broadcast
  Neighbors are discovered, and the DR and BDR are elected.
  The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
  Ethernet and fiber distributed data interface (FDDI) belong to the broadcast network type by default.
- Non-broadcast multiple access (NBMA)
  Neighbors are manually configured, and the DR and BDR are elected.
  The DR (or BDR) exchanges LSAs with all other routers to set up an adjacency. Except the DR and BDR, all other routers do not exchange LSAs with each other, and the adjacency is not set up.
  X.25, frame relay, and ATM belong to NBMA networks by default.
- Point-to-point (P2P)
  Neighbors are automatically discovered, and the DR or BDR is not elected.
  LSAs are exchanged between routers at both ends of the link, and the adjacency is set up.
  PPP,HDLC, and LAPB belongs to the P2P network type by default.
- Point-to-multipoint (P2MP)
  Neighbors are automatically discovered, and the DR or BDR is not elected.
  LSAs are exchanged between any two routers, and the adjacency is set up.
  Networks without any link layer protocol belong to the P2MP network type by default. P2MP broadcast
  Neighbors are manually configured, and the DR or BDR is not elected.
  LSAs are exchanged between any two routers, and the adjacency is set up.
  Networks without any link layer protocol belong to the P2MP network type by default.

OSPF Route Types

Figure 1-5



Display the OSPF routes (marked in red) in the routing table of Router A.

```
A#show ip route


Codes:  C - connected, S - static, R - RIP, B - BGP

O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2

E1 - OSPF external type 1, E2 - OSPF external type 2

i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2

ia - IS-IS inter area, * - candidate default


Gateway of last resort is no set

O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:01:00,GigabitEthernet 0/3

O E2 191.10.10.0/24 [110/20] via 192.168.1.2, 01:11:26,GigabitEthernet 0/1

C    192.168.1.0/24 is directly connected,GigabitEthernet 0/1

C    192.168.1.1/32 is local host.

C    192.168.2.0/24 is directly connected,GigabitEthernet 0/2

C    192.168.2.1/32 is local host.

C    192.168.3.0/24 is directly connected,GigabitEthernet 0/3

C    192.168.3.1/32 is local host.

O    192.168.4.0/24 [110/2] via 192.168.2.2, 00:00:02,GigabitEthernet 0/2

O IA 192.168.5.0/24 [110/3] via 192.168.1.2, 00:01:02,GigabitEthernet 0/1
```

A mark is displayed in front of each OSPF route to indicate the type of the route. There are six types of OSPF routes:

- O: Intra-area route

  This type of route describes how to arrive at a destination network in the local area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.

- IA: Inter-area route
  This type of route describes how to arrive at a destination network in another area. The cost of this type of route is equal to the cost of the route from the local router to the destination network.
- E1: Type 1 external route
  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.
- E2: Type 2 external route
  This type of route describes how to arrive at a destination network outside the AS. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route does not exist on routers in the stub or NSSA area.
- N1: Type 1 external route of the NSSA area
  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the local router to the ASBR plus the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.
- N2: Type 2 external route of the NSSA area
  This type of route describes how to arrive at a destination network outside the AS through the ASBR in the NSSA area. The cost of this type of route is equal to the cost of the route from the ASBR to the destination network. This type of route exists only on routers in the NSSA area.

Reliability of E2 and N2 routes is poor. OSPF believes that the cost of the route from the ASBR to a destination outside an AS is far greater than the cost of the route to the ASBR within the AS. Therefore, when the route cost is computed, only the cost of the route from the ASBR to a destination outside an AS is considered.

Related Configuration

Enabling OSPF

OSPF is disabled by default.

Run the **router ospf** command to create an OSPF process on the router.

Run the **network area** command to enable OSPF on the interface and specify the area ID.

Run the **area virtual-link** command to create a virtual link on the router. The virtual link can be treated as a logical interface.

Router ID

By default, the OSPF process elects the largest IP address among the IP addresses of all the loopback interfaces as the router ID. If the loopback interfaces configured with IP addresses are not available, the OSPF process elects the largest IP address among the IP addresses of all the loopback interfaces as the router ID.

Alternatively, you can run the **router-id** command to manually specify the router ID.

Protocol Control Parameters

Run the **ip ospf hello-interval** command to modify the Hello interval on the interface. The default value is 10s (or 30s for NBMA networks).

Run the **ip ospf dead-interval** command to modify the neighbor dead interval on the interface. The default value is four times the Hello interval.

Use the **poll-interval** parameter in the **neighbor** command to modify the neighbor polling interval on the NBMA interface. The default value is 120s.

Run the **ip ospf transmit-delay** command to modify the LSU packet transmission delay on the interface. The default value is 1s.

Run the **ip ospf retransmit-interval** command to modify the LSU packet retransmission interval on the interface. The default value is 5s.

Use the **hello-interval** parameter in the **area virtual-link** command to modify the Hello interval on the virtual link. The default value is 10s.

Use the **dead-interval** parameter in the **area virtual-link** command to modify the neighbor dead interval on the virtual link. The default value is four times the Hello interval.

Use the **transmit-delay** parameter in the **area virtual-link** command to modify the LSU packet transmission delay on the virtual link. The default value is 1s.

Use the **retransmit-interval** parameter in the **area virtual-link** command to modify the LSU packet retransmission interval on the virtual link. The default value is 5s.

Run the **timers throttle lsa all** command to modify parameters of the exponential backoff algorithm that generates LSAs. The default values of these parameters are 0 ms, 5000 ms, and 5000 ms.

Run the **timerspacinglsa-group** command to modify the LSA group update interval. The default value is 30s.

Run the **timers pacing lsa-transmit** command to modify the LS-UPD packet sending interval and the number of sent LS-UPD packets. The default values are 40 ms and 1.

Run the **timers lsa arrival** command to modify the delay after which the same LSA is received. The default value is 1000 ms.

Run the **timers throttle spf** command to modify the SPT computation delay, minimum interval between two SPT computations, and maximum interval between two SPT computations. The default values are 1000 ms, 5000 ms, and 10000 ms.

Run the **timers spf** command to modify the SPF computation delay and interval between two SPF computations. The default value is based on the **timers throttle spf** command configuration.

↘ OSPF Network Types

By default, Ethernet and FDDI belong to the broadcast type, X.25, frame relay, and ATM belong to the NBMA type, and PPP, HDLC, and LAPB belong to the P2P type.

Run the **ip ospf network** command to manually specify the network type of an interface.

Run the **neighbor** command to manually specify a neighbor. For the NBMA and P2MP non-broadcast types, you must manually specify neighbors.

Run the **ip ospf priority** command to adjust the priorities of interfaces, which are used for DR/BDR election. The DR/BDR election is required for the broadcast and NBMA types. The router with the highest priority wins in the election, and the router with the priority of 0 does not participate in the election. The default value is 1.

1.3.2 OSPF Route Management

Plan or optimize OSPF routes through manual configuration to implement management of OSPF routes.

Working Principle

(Totally) Stub Area and (Totally)NSSA Area

The (totally) stub and (totally)NSSA areas help reduce the protocol interaction load and the size of the routing table.

- If an appropriate area is configured as a (totally) stub or NSSA area, advertisement of a large number of Type 5 and Type 3 LSAs can be avoided within the area.

Area	Type1 and Type2 LSAs	Type 3 LSA	Type 4 LSA	Type 5 LSA	Type 7 LSA
Non (totally) stub area and NSSA area	Allowed	Allowed	Allowed	Allowed	Not allowed
Stub area	Allowed	Allowed (containing one default route)	Not allowed	Not allowed	Not allowed
Totally stub area	Allowed	Only one default route is allowed.	Not allowed	Not allowed	Not allowed
NSSA area	Allowed	Allowed (containing one default route)	Allowed	Not allowed	Allowed
Totally NSSA area	Allowed	Only one default route is allowed.	Allowed	Not allowed	Allowed

The ABR uses Type 3LSAs to advertise a default route to the (totally) stub or NSSA area.

The ABR converts Type 7 LSAs in the totally NSSA area to Type 5LSAs, and advertise Type5LSAs to the backbone area.

- If an area is appropriately configured as a (totally) stub area or an NSSA area, a large number of E1, E2, and IA routes will not be added to the routing table of a router in the area.

Area	Routes Available in the Routing Table of a Router Inside the Area
Non (totally) stub area and NSSA area	O: a route to a destination network in the local area IA: a route to a destination network in another area E1 or E2: a route or default route to a destination network segment outside the AS (via any ASBR in the AS)
Stub area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area
Totally stub area	O: a route to a destination network in the local area IA: a default route
NSSA area	O: a route to a destination network in the local area IA: a route or a default route to a destination network in another area N1 or N2: a route or default route to a destination network segment outside the AS (via any ASBR in the local area)
Totally NSSA area	O: a route to a destination network in the local area IA: a default route N1 or N2: a route or default route to a destination network segment outside the AS (via any

	ASBR in the local area)

Route Redistribution

Route redistribution refers to the process of introducing routes of other routing protocols, routes of other OSPF processes, static routes, and direct routes that exist on the device to an OSPF process so that these routes can be advertised to neighbors using Type 5 and Type 7 LSAs. A default route cannot be introduced during route redistribution.

Route redistribution is often used for interworking between ASs. You can configure route redistribution on an ASBR to advertise routes outside an AS to the interior of the AS, or routes inside an AS to the exterior of the AS.

Default Route Introduction

By configuring a command on an ASBR, you can introduce a default route to an OSPF process so that the route can be advertised to neighbors using Type 5 and Type 7 LSAs.

Default route introduction is often used for interworking between ASs. One default route is used to replace all the routes outside an AS.

Route Summarization

Route summarization is a process of summarizing routing information with the same prefix into one route, and advertising the summarized route (replacing a large number of individual routes) to neighbors. Route summarization helps reduce the protocol interaction load and the size of the routing table.

By default, the ABR advertises inter-area routing information by using Type3 LSAs within a network segment, and advertises redistributed routing information by using Type 5 and Type 7 LSAs. If continuous network segments exist, it is recommended that you configure route summarization.

When configuring route summarization, the summarization range may exceed the actual network scope of routes. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, the ABR or ASBR automatically adds a discard route to the routing table. This route will not be advertised.

Route Filtering

OSPF supports route filtering to ensure security and facilitate control when the routing information is being learned, exchanged, or used.

Using configuration commands, you can configure route filtering for the following items:

- Interface: The interface is prevented from sending routing information (any LSAs) or exchanging routing information (any LSAs) with neighbors.
- Routing information advertised between areas: Only the routing information that meets the filtering conditions can be advertised to another area (Type 3 LSAs).
- Routing information outside an AS: Only the routing information that meets the filtering conditions can be redistributed to the OSPF process(Type 5 and Type 7 LSAs).
- LSAs received by a router: In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

If redundancy links or devices exist on the network, multiple paths may exist from the local device to the destination network. OSPF selects the path with the minimum total cost to form an OSPF route. The total cost of a path is equal to the sum of the costs of individual links along the path. The total cost of a path can be minimized by modifying the costs of individual links along the path. In this way, OSPF selects this path to form a route.

Using configuration commands, you can modify the link costs:

- Cost from an interface to a directly connected network segment and cost from the interface to a neighbor
- Cost from an ABR to the inter-area summarization network segment and cost from the ABR to the default network segment
- Cost from an ASBR to an external network segment and cost from the ASBR to the default network segment

Both the cost and the metric indicate the cost and are not differentiated from each other.

OSPF Administrative Distance

The administrative distance (AD) evaluates reliability of a route, and the value is an integer ranging from 0 to 255. A smaller AD value indicates that the route is more trustworthy. If multiples exist to the same destination, the route preferentially selects a route with a smaller AD value. The route with a greater AD value becomes a floating route, that is, a standby route of the optimum route.

By default, the route coming from one source corresponds to an AD value. The AD value is a local concept. Modifying the AD value affects route selection only on the current router.

Route Source	Directly-Connected Network	Static Route	EBGP Route	OSPF Route	ISIS Route	RIP Route	IBGP Route	Unreachable Route
Default AD	0	1	20	110	115	120	200	255

Related Configuration

Stub Area and NSSA Area

No stub or NSSA area is configured by default.

Run the **area stub** command to configure a specified area as a stub area.

Run the **area nssa** command to configure a specified area as an NSSA area.

The backbone area cannot be configured as a stub or an NSSA area.

A transit area (with virtual links going through) cannot be configured as a stub or an NSSA area.

An area containing an ASBR cannot be configured as a stub area.

Route Redistribution and Default Route Introduction

By default, routes are not redistributed and the default route is not introduced.

Run the **redistribute** command to configure route redistribution.

Run the **default-information originate** command to introduce the default route.

After configuring route redistribution and default route introduction, the route automatically becomes an ASBR.

Route Summarization

By default, routes are not summarized. If route summarization is configured, a discard route will be automatically added.

Run the **arearange** command to summarize routes distributed between areas (Type 3 LSA) on the ABR.

Run the **summary-address** command to summarize redistributed routes (Type 5 and Type 7 LSAs) on the ASBR.

Run the **discard-route** command to add a discard route to the routing table.

Route Filtering

By default, routes are not filtered.

Run the **passive-interface** command to configure a passive interface. Routing information (any LSAs) cannot be exchanged on a passive interface.

Run the **ip ospf database-filter all out** command to prohibit an interface from sending routing information (any LSAs).

Run the **area filter-list** command to filter routing information advertised between areas on the ABR. Only the routing information that meets the filtering conditions can be advertised to another area (Type 3 LSAs).

Use the **route-map** parameter in the **redistribute** command, or use the **distribute-list out** command to filter the external routing information of the AS on the ASBR. Only the routing information that meets the filtering conditions can be redistributed to the OSPF process (Type 5 and Type 7 LSAs).

Run the **distribute-list in** command to filter LSAs received by the router. In the OSPF routing table, only the routes that are computed based on the LSAs meeting the filtering conditions can be advertised.

Route Cost

- Cost from the interface to the directly-connected network segment (cost on the interface)
  The default value is the auto cost. Auto cost = Reference bandwidth/Interface bandwidth
  Run the **auto-cost reference-bandwidth** command to set the reference bandwidth of auto cost. The default value is 100 Mbps.
  Run the **ip ospf cost** command to manually set the cost of the interface. The configuration priority of this item is higher than that of the auto cost.
- Cost from the interface to a specified neighbor (that is, cost from the local device to a specified neighbor)
  The default value is the auto cost.
  Use the **cost** parameter in the **neighbor** command to modify the cost from the interface to a specified neighbor. The configuration priority of this item is higher than that of the cost of the interface.
  This configuration item is applicable only to P2MP-type interfaces.
- Cost from the ABR to the inter-area summarization network segment (that is, the cost of the summarized inter-area route)
  If OSPF routing is compatible with RFC1583, the default value is the minimum cost among all costs of the summarized links; otherwise, the default value is the maximum cost among all costs of the summarized links.
  Run the **compatible rfc1583** command to make OSPF routing compatible with RFC1583. By default, OSPF routing is compatible with RFC1583.
  Use the **cost** parameter in the **area range** command to modify the cost of inter-area route summarization.
- Cost from the ABR to the default network segment (that is, the cost of the default route that is automatically advertised by the ABR to the stub or NSSA areas)
  The default value is 1.

Run the **area default-cost** command to modify the cost of the default route that the ABR automatically advertise to the stub or NSSA areas.

- Cost from the ASBR to an external network segment (that is, the metric of an external route)
  By default, the metric of the redistributed BGP route is 1, the metric of other redistributed routes is 20, and the route type is Type 2 External.
  Run the **default-metric** command to modify the default metric of the external route.
  Use the **metric**, **metric-type** and **route-map** parameters in the **redistribute** command to modify the metric and route type of the external route.
- Cost from the ASBR to the default network segment (that is, the metric of the default route that is manually introduced)
  By default, the metric is 1, and the route type is Type 2 External.
  Use the **metric**, **metric-type** and **route-map** parameters in the **default-information originate** command to modify the metric and route type of the default route that is manually introduced.
  Use the **metric** and **metric-type** parameters of **default-information originate** in the **area nssa** command to modify the metric and type of the default route that is manually introduced to the NSSA area.
- Run the **max-metric router-lsa** command to set metrics of all routes advertised on the router to the maximum value. In this way, the total cost of any path that passes through this router will become very large, and the path can hardly become the shortest path.

OSPF Administrative Distance

By default, the OSPF AD is 110.

Run the **distance** command to set the AD of an OSPF route.

1.3.3 Enhanced Security and Reliability

Use authentication, MTU verification and GR to enhance security, stability, and reliability of OSPF.

Working Principle

Authentication

Authentication prevents routers that illegally access the network and hosts that forge OSPF packet from participating in the OSPF process. OSPF packets received on the OSPF interface (or at both ends of the virtual link) are authenticated. If authentication fails, the packets are discarded and the adjacency cannot be set up.

Enabling authentication can avoid learning unauthenticated or invalid routes, thus preventing advertising valid routes to unauthenticated devices. In the broadcast-type network, authentication also prevents unauthenticated devices from becoming designated devices, ensuring stability of the routing system and protecting the routing system against intrusions.

MTU Verification

On receiving a DD packet, OSPF checks whether the MTU of the neighbor interface is the same as the MTU of the local interface. If the MTU of the interface specified in the received DD packet is greater than the MTU of the interface that receives the packet, the adjacency cannot be set up. Disabling MTU verification can avoid this problem.

Source Address Verification

Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF determines that the packet is invalid and discards this packet. In particular, for unnumbered interfaces, OSPF never performs address verification.

In some scenarios, the source address of a packet received by OSPF may not be in the same network segment as the receiving interface, and therefore OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

Two-Way Maintenance

OSPF routers periodically send Hello packets to each other to maintain the adjacency. On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed.

If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors, which makes the adjacency more stable.

Concurrent Neighbor Interaction Restriction

When a router simultaneously exchanges data with multiple neighbors, its performance may be affected. If the maximum number of neighbors that concurrently initiate or accept interaction with the OSPF process, the router can interact with neighbors by batches, which ensures data forwarding and other key services.

Overflow

OSPF requires that routers in the same area store the same LSDB. The number of routers keeps increasing on the network. Some routers, however, cannot store so much routing information due to the limited system resources. The large amount of routing information may exhaust the system resources of routers, causing failures of the routers.

The overflow function limit the number of external routes in the LSDB to control the size of the LSDB.

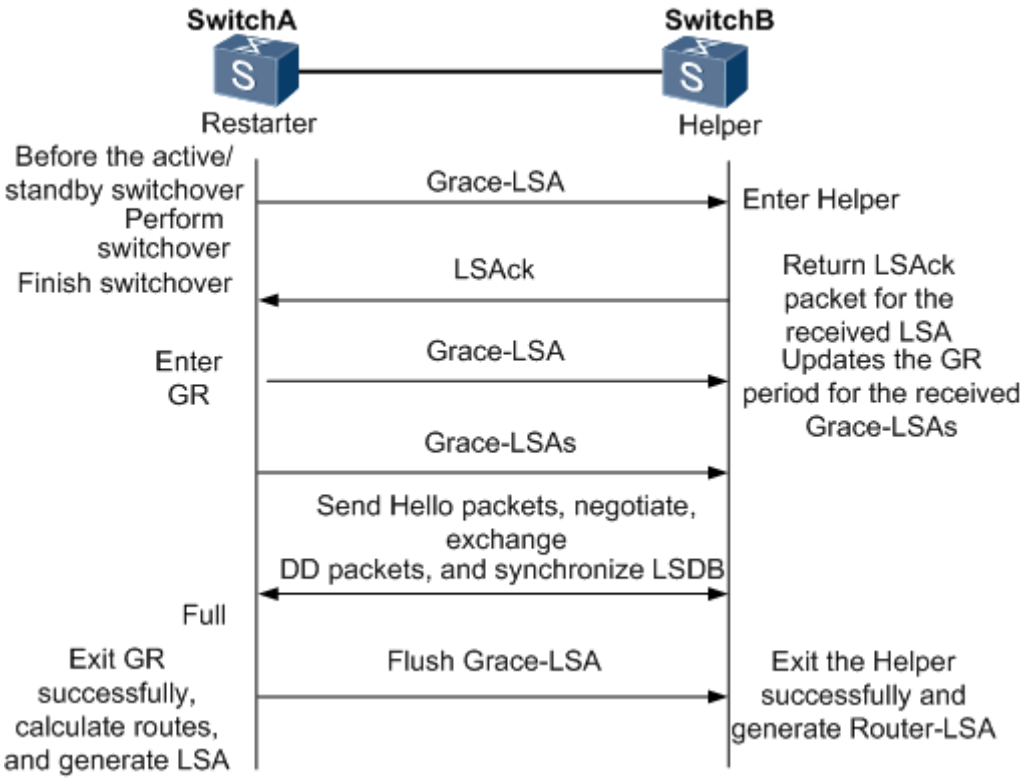
When the number of external routes on a router exceeds the upper limit, the router enters the overflow state. The router deletes the external routes generated by itself from the LSDB, and does not generate new external routes. In addition, the router discards the newly received external routes. After the overflow state timer (5s) expires, if the number of external routes is lower than the upper limit, the normal state is restored.

GR

The control and forwarding separated technology is widely used among routers. On a relatively stable network topology, when a GR-enabled router is restarted on the control plane, data forwarding can continue on the forwarding plane. In addition, actions (such as adjacency re-forming and route computation) performed on the control plane do not affect functions of the forwarding plane. In this way, service interruption caused by route flapping can be avoided, thus enhancing reliability of the entire network.

Currently, the GR function is used only during active/standby switchover and system upgrade.

Figure 1-6 Normal OSPF GR Process



- The GR process requires collaboration between the restarter and the helper. The restarter is the router where GR occurs. The helper is a neighbor of the restarter.
- When entering or exiting the GR process, the restarter sends a Grace-LSA to the neighbor, notifying the neighbor to enter or exit the helper state.
- When the adjacency between the restarter and the helper reaches the Full state, the router can exit the GR process successfully.

Fast Hello

After a link failure occurs, OSPF takes some time (about 40s) to detect the death of a neighbor. Then it broadcasts this information and recalculates the SPT. During this period, the traffic may be interrupted.

When the Fast Hello function is enabled (that is, the neighbor dead time is set to 1s), OSPF can detect the death of a neighbor within 1s after a link failure occurs. This significantly accelerates route convergence and avoids traffic interruptions.

Related Configuration

OSPF Packet Authentication

By default, authentication is disabled.

- Run the **area authentication** command to enable the authentication function in the entire area so that the function takes effect on all interfaces in this area. If authentication is enabled in area 0, the function takes effect on the virtual link.

- Run the **ip ospf authentication** command to enable authentication on an interface. This configuration takes precedence over the area-based configuration.
- Run the **ip ospf authentication-key** command to set the text authentication key on an interface.
- Run the **ip ospf message-digest-key** command to set the message digest 5 (MD5) authentication key on an interface.
- Use the **authentication** parameter in the **area virtual-link** command to enable authentication at both ends of a virtual link. This configuration takes precedence over the area-based configuration.
- Use the **authentication-key** parameter in the **area virtual-link** command to set the text authentication key at both ends of a virtual link.
- Use the **message-digest-key** parameter in the **area virtual-link** command to set the MD5 authentication key at both ends of a virtual link.

MTU Verification

By default, MTU verification is disabled.

Run the **ip ospf mtu-ignore** command to disable MTU verification on an interface.

Source address verification

By default, source address verification is enabled on a P2P interface.

Run the **ip ospf source-check-ignore** command to disable source address verification on an interface.

Two-Way Maintenance

By default, bidirectional maintenance is enabled.

Run the **two-way-maintain** command to enable two-way maintenance.

Concurrent neighbor Interaction Restriction

Run the **max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with the current OSPF process. The default value is 5.

Run the **ip router ospf max-concurrent-dd** command to modify the maximum number of neighbors that are concurrently interacting with all OSPF processes on the router. The default value is 10.

Overflow

Run the **overflow memory-lack** command to allow the router to enter the overflow state when the memory is insufficient. By default, the router is allowed to enter the overflow state when the memory is insufficient.

Run the **overflow database** command to allow the router to enter the overflow state when the number of LSAs is too large. By default, the router is not allowed to enter the overflow state when the number of LSAs is too large.

Run the **overflow database external** command to allow the router to enter the overflow state when the number of external LSAs is too large. By default, the router is not allowed to enter the overflow state when the number of external-LSAs is too large.

GR

By default, the restarter function is disabled, and the helper function is enabled.

Run the **graceful-restart** command to configure the restarter function.

Run the **graceful-restart helper** command to configure the helper function.

Fast Hello

By default, the neighbor dead time on an interface is 40s.

Run the **ip ospf dead-interval minimal hello-multiplier** command to enable the Fast Hello function (neighbor dead time is 1s) on an interface.

1.3.4 Network Management

Use functions such as the MIB and Syslog to facilitate OSPF management.

Working Principle

MIB

MIB is the device status information set maintained by a device. You can use the management program to view and set the MIB node.

Multiple OSPF processes can be simultaneously started on a router, but the OSPF MIB can be bound with only one OSPF process.

Trap

A Trap message is a notification generated when the system detects a fault. This message contains the related fault information.

If the Trap function is enabled, the router can proactively send the Trap messages to the network management device.

Syslog

The Syslog records the operations (such as command configuration) performed by users on routers and specific events (such as network connection failures).

If the Syslog is allowed to record the adjacency changes, the network administrator can view the logs to learn the entire process that the OSPF adjacency is set up and maintained.

Related Configuration

MIB

By default, the MIB is bound with the OSPF process with the smallest process ID.

Run the **enable mib-binding** command to bind the MIB with the current OSPF process.

Trap

By default, all traps are disabled, and the device is not allowed to send OSPF traps.

Run the **enable traps** command to enable a specified trap for an OSPF process.

Run the **snmp-server enable traps ospf** command to allow the device to send OSPF traps.

SYSLOG

By default, the Syslog is allowed to record the adjacency changes.

Run the **log-adj-changes** command to allow the Syslog to record the adjacency changes.

1.4 Configuration

Configuration	Description and Command	
Configuring OSPF Basic Functions	(Mandatory) It is used to build an OSPF routing domain.	
	routerospf	Creates an OSPF process.
	router-id	Configures a router ID.
	network area	Enables OSPF on an interface and specifies an area ID.
	area virtual-link	Creates a virtual link.
Setting the Network Type	(Optional) The configurations are mandatory if the physical network is the X.25, frame relay, or ATM network.	
	ip ospf network	Defines the network type.
	neighbor	Specifies a neighbor.
	ip ospf priority	Configures the DR priority.
Configuring Route Redistribution and Default Route	(Optional) The configurations are recommended if the OSPF routing domain is connected with an external network.	
	redistribute	Configures route redistribution.
	default-information originate	Introduces a default route.
Configuring Stub Area and NSSA Area	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	areastub	Configures a stub area.
	areanssa	Configures an NSSA area.
Configuring Route Summarization	(Optional) It is used to reduce interaction of routing information and the size of routing table, and enhance stability of routes.	
	arearange	Summarizes routes that are advertised between areas.
	summary-address	Summarizes routes that are introduced through redistribution.
	discard-route	Adds a discard route to the routing table.
Configuring Route Filtering	(Optional) It is used to manually control interaction of routing information and filter available OSPF routes.	
	passive-interface	Configures a passive interface.
	ip ospfdatabase-filter all out	Prohibits an interface from sending LSAs.
	area filter-list	Filters routes that are advertised between areas..

Configuration	Description and Command	
	distribute-list out	Filters routes that are introduced through redistribution.
	distribute-listin	Filters routes that are calculated based on the received LSAs.
Modifying Route Cost and AD	(Optional) It is used to manually control the shortest route computed by OSPF and determine whether to select an OSPF route preferentially.	
	auto-costreference-bandwidth	Modifies the reference bandwidth of the auto cost.
	ip ospf cost	Modifies the cost in the outbound direction of an interface.
	areadefault-cost	Modifies the cost of the default route in a stub or an NSSA area.
	default-metric	Modifies the default metric of a redistributed route.
	max-metric router-lsa	Configures the maximum metric.
	compatible rfc1583	Enables the routing rules to be compatible with RFC1583.
	distance	Modifies the OSPF AD.
Enabling Authentication	(Optional) It is used to prevent routers that illegally access the network and hosts that forge OSPF packets from participating in the OSPF protocol process.	
	areaauthentication	Enables authentication and sets the authentication mode in an area.
	ip ospf authentication	Enables authentication and sets the authentication mode on an interface.
	ip ospf authentication-key	Sets the text authentication key on an interface.
	ip ospfmessage-digest-keymd5	Sets the MD5 authentication key on an interface.
Enabling Overflow	(Optional) It is used to prevent the problem that OSPF processes stop running due to over-consumption of the memory.	
	overflow memory-lack	Allows the router to enter the overflow state when the memory is insufficient.
	overflow database	Allows the router to enter the overflow state when the number of LSAs exceeds the preset limit.
	overflow database external	Allows the router to enter the overflow state when the number of external LSAs exceeds the preset limit.
Modifying the Maximum Number of Concurrent	(Optional) It is used to prevent the problem of performance deterioration caused by over-consumption of the CPU.	

Configuration	Description and Command	
Neighbors	**max-concurrent-dd**	Modifies the maximum number of con current neighbors on the current OSPF process.
	router ospf max-concurrent-dd	Modifies the maximum number of con current neighbors on all OSPF processes.
Disabling Source Address Verification	⚠ (Optional) It is used to prevent the problem that the adjacency cannot be set up due to the failure to obtain the peer address.	
	ip ospf source-check-ignore	Disables source address verification on an interface.
Disabling MTU Verification	⚠ (Optional) It is used to prevent the problem that the adjacency cannot be set up due to MTU inconsistency on the neighbor interface.	
	ip ospf mtu-ignore	Disables MTU verification on an interface.
Enabling Two-Way Maintenance	⚠ (Optional) It is used to prevent termination of the adjacency due to the delay or loss of Hello packets.	
	two-way-maintain	Enables two-way maintenance.
Enabling GR	⚠ (Optional) It is used to maintain OSPF route forwarding and prevent traffic interruption during an OSPF process restart or active/standby switchover.	
	graceful-restart	Configures the Restarter function.
	graceful-restart helper	Configures the Helper function.
Configuring Fast Hello Function	⚠ (Optional) It is used to quickly detect neighbor death during link failure to avoid traffic interruption.	
	ip ospf dead-intervalminimal hello-multiplier	Enables the Fast Hello function on an interface.
Configuring the Network Management Function	⚠ (Optional) The configurations enable users to use the SNMP network management software to manage OSPF.	
	enable mib-binding	Binds the MIB with the current OSPF process.
	enable traps	Enables a specified trap for an OSPF process.
	snmp-server enable traps ospf	Allows the device to send OSPF traps.
	log-adj-changes	Allows the Syslog to record the adjacency changes.
Modifying Protocol Control Parameters	⚠ (Optional) You are advised not to modify protocol control parameters unless necessary.	
	ip ospf hello-interval	Modifies the Hello interval.
	ip ospf dead-interval	Modifies the neighbor death interval.
	timers throttle lsa all	Modifies parameters of the exponential backoff algorithm that generates LSAs.

Configuration	Description and Command	
	timers throttle route inter-area	Modifies the inter-area route computation delay.
	timers throttle route ase	Modifies the external route computation delay.
	timerspacinglsa-group	Modifies the LSA group update interval.
	timers pacing lsa-transmit	Modifies the LS-UPD packet sending interval.
	ip ospf transmit-delay	Modifies the LSU packet transmission delay.
	ip ospf retransmit-interval	Modifies the LSU packet retransmission interval.
	timers lsa arrival	Modifies the delay after which the same LSA is received.
	timers throttlespf	Modifies the SPT computation timer.

1.4.1 Configuring OSPF Basic Functions

Configuration Effect

- Set up an OSPF routing domain on the network to provide IPv4 unicast routing service for users on the network.

Notes

- Ensure that the IP unitcast routing function is enabled, that is, **ip routing** is not disabled; otherwise, OSPF cannot be enabled.
- It is strongly recommended that you manually configure the router ID.
- After **ip ospf disable all** is configured, the interface neither sends or receives any OSPF packet, nor participates in OSPF computation even if the interface belongs to the network.

Configuration Steps

Creating an OSPF Process

- Mandatory.
- The configuration is mandatory for every router.

Configuring a Router ID

- (Optional) It is strongly recommended that you manually configure the router ID.
- If the router ID is not configured, OSPF selects an interface IP address. If the IP address is not configured for any interface, or the configured IP addresses have been used by other OSPF instances, you must manually configure the router ID.

Adding Interface IPs to OSPF and Specifying an Area ID

- (Mandatory) If OSPF is enabled using the command under an interface, this configuration can be omitted.
- The configuration is mandatory for every router.

Enabling OSPF on an Interface and Specifying an Area ID

- (Mandatory) If an interface joins OSPF through the OSPF instance, this configuration can be omitted.
- The configuration is mandatory for every router.

Verification

- Run the **show ip route ospf** command to verify that the entries of the OSPF routing table are correctly loaded.
- Run the **ping** command to verify that the IPv4 unicast service is correctly configured.

Related Commands

Creating an OSPF Process

Command	**router ospf** *process-id*
Parameter Description	*process-id:* Indicates the OSPF process ID. If the process ID is not specified, the process ID is 1.
Command Mode	Global configuration mode
Usage Guide	Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently.

Configuring a Router ID

Command	**router-id** *router-id*
Parameter Description	*router-id:* Indicates the router ID to be configured. It is expressed in the IP address.
Command Mode	OSPF routing process configuration mode
Usage Guide	Different OSPF processes are independent of each other, and can be treated as different routing protocols that run independently. Each OSPF process uses a unique router ID.

Enabling OSPF on an Interface and Specifying an Area ID

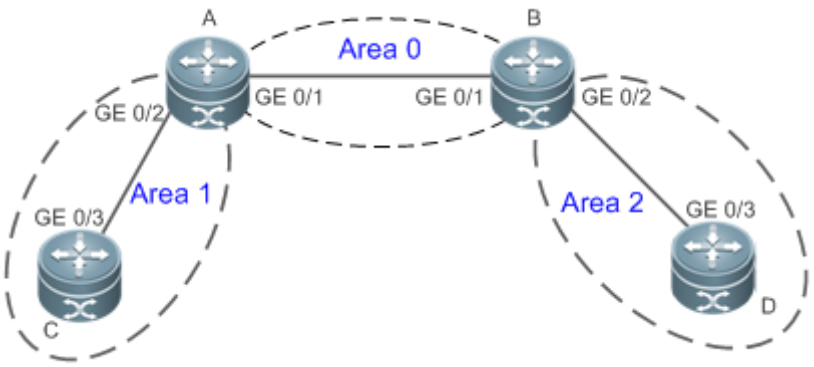
Command	**network** *ip-address wildcard* **area** *area-id*
Parameter Description	*ip-address*: Indicates the IP address of the interface. *wildcard:* Indicates the IP address comparison mode. **0** indicates accurate matching, and **1** indicates that no comparison is performed. *area-id:* Indicates the ID of an OSPF area. An OSPF area is always associated with an address range. To facilitate management, you can use a subnet as the ID of an OSPF area.
Command Mode	OSPF routing process configuration mode
Usage Guide	By defining *ip-address* and *wildcard*, you can use one command to associate multiple interfaces with one OSPF area. To run OSPF on one interface, you must include the primary IP address of the interface in the IP address range defined by **network area**. If the IP address range defined by **network area** contains only the secondary IP address of the interface, OSPF does not run on this interface. If the interface address matches the IP address ranges defined in the **network** commands of multiple OSPF processes, the OSPF process that the interface is associated with is determined based on the best match method.

Creating a Virtual Link

Command	**area** *area-id* **virtual-link** *router-id* [**authentication** [**message-digest** | **null**] | **dead-interval** { *seconds* | **minimal hello-multiplier** *multiplier* } | **hello-interval** *seconds* | **retransmit-interval** *seconds* | **transmit-delay** *seconds*] * [**authentication-key** [**0** | **7**] *key* | **message-digest-key** *key-id* **md5** [**0** | **7**] *key*]
Parameter Description	*area-id:* Indicates the ID of the OSPF transit area. The area ID can be a decimal integer or an IP address. *router-id:* Indicates the ID of a neighbor router on the virtual link. **authentication:** Sets the authentication type to plain text authentication. **message-digest:** Sets the authentication type to MD5 authentication. **null:** Indicates that authentication is disabled. **dead-interval** *seconds:* Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 0 to 2,147,483,647. The setting of this parameter must be consistent with that on a neighbor. **minimal**: Enables the Fast Hello function and sets the dead time to 1s. **hello-multiplier**: Indicates the multiplier of the dead interval to the hello interval in the Fast Hello function. *multiplier*: Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20. **hello-interval** *seconds:* Indicates the interval at which OSPF sends the Hello packet to the virtual link. The unit is second. The value ranges from 1 to 65,535. The setting of this parameter must be consistent with that on a neighbor. **retransmit-interval** *seconds:* Indicates the OSPF LSA retransmission time. The unit is second. The value ranges from 1 to 65,535. **transmit-delay** *seconds:* Indicates the delay after which OSPF sends the LSA. The unit is second. The value ranges from 1 to 65,535. **authentication-key** [**0** | **7**]*key:* Defines the key for OSPF plain text authentication. **message-digest-key** *key-id***md5** [**0** | **7**]key: Defines the key ID and key for OSPF MD5 authentication.
Command Mode	OSPF routing process configuration mode
Usage Guide	In the OSPF routing domain, all areas must be connected to the backbone area. If the backbone area is disconnected, a virtual link must be configured to connect to the backbone area; otherwise, network communication problems will occur. A virtual link must be created between two ABRs, and the area to which both ABRs belong is the transit area. A stub area or an NSSA area cannot be used as a transit area. A virtual link can also be used to connect other non-backbone areas. **router-id** is the ID of an OSPF neighbor router. If you are sure about the value of **router-id**, run the **show ip ospf neighbor** command to confirm the value. You can configure the loopback address as the router ID. The **area virtual-link** command defines only the authentication key of the virtual link. To enable OSPF packet authentication in the areas connected to the virtual link, you must run the **area authentication** command. OSPF supports the Fast Hello function: Enabling the OSPF Fast Hello function accelerates neighbor discovery and rapid detection of neighbor failures in OSPF. The OSPF Fast Hello function is enabled by specifying the **minimal** and **hello-multiplier** keywords and the *multiplier* parameter. The **minimal** keyword sets the dead time to 1s, and the **hello-multiplier** value specifies the number of Hello packets sent per second, reducing the Hello packet

	interval to less than 1s. When a virtual link is configured with the Fast Hello function, the Hello interval field of the Hello packets advertised from that virtual link is set to 0, and the Hello interval field of the Hello packets received from that virtual link is ignored. The dead interval at both ends of a virtual link must be consistent regardless of whether Fast Hello is enabled or not. The hello-multiplier value does not need to be the same, as long as at least one Hello packet can be received within the dead interval. The **show ip ospf virtual-links** command can be used to monitor the dead interval and Fast Hello interval configured for virtual links. The **dead-interval minimal hello-multiplier** parameter and the **hello-interval** parameter introduced for Fast Hello function cannot be configured simultaneously.

Configuration Example

Scenario **Figure 1-7**	 **Remarks** The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/3 192.168.2.2 D: GE 0/3 192.168.3.2
Configuration Steps	● Configure the interface IP addresses on all routers. ● Enable the IPv4 unicast routing function on all routers. (This function is enabled by default.) ● Configure the OSPF instances and router IDs on all routers. ● Enable OSPF on the interfaces configured on all routers.

A	`A#configure terminal`
	`A(config)#interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0`

	A(config-if-GigabitEthernet 0/1)#exit A(config)#interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)#ip address 192.168.2.1 255.255.255.0 A(config-if-GigabitEthernet 0/2)#exit A(config)#router ospf 1 A(config-router)#router-id192.168.1.1 A(config-router)#network 192.168.1.0 0.0.0.255 area 0 A(config-router)#network 192.168.2.0 0.0.0.255 area 1
B	B#configure terminal B(config)#interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)#ip address 192.168.1.2 255.255.255.0 B(config-if-GigabitEthernet 0/1)#exit B(config)#interface GigabitEthernet 0/2 B(config-if-GigabitEthernet 0/2)#ip address 192.168.3.1 255.255.255.0 B(config-if-GigabitEthernet 0/2)#exit B(config)#router ospf 1 B(config-router)#router-id192.168.1.2 B(config-router)#network 192.168.1.0 0.0.0.255 area 0 B(config-router)#network 192.168.3.0 0.0.0.255 area 2
C	C#configure terminal C(config)#interface GigabitEthernet 0/3 C(config-if-GigabitEthernet 0/3)#ip address 192.168.2.2 255.255.255.0 C(config-if-GigabitEthernet 0/3)#exit C(config)#router ospf 1 C(config-router)#router-id192.168.2.2 C(config-router)#network 192.168.2.0 0.0.0.255 area 1
D	D#configure terminal D(config)#interface GigabitEthernet 0/3 D(config-if-GigabitEthernet 0/3)#ip address 192.168.3.2 255.255.255.0 D(config-if-GigabitEthernet 0/3)#exit D(config)#router ospf 1 D(config-router)#router-id192.168.3.2 D(config-router)#network 192.168.3.0 0.0.0.255 area 2

Verification	● Verify that the OSPF neighbors are correct on all routers. ● Verify that the routing table is correctly loaded on all routers. ● On Router D, verify that the IP address 192.168.2.2 can be pinged successfully.
A	A# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.2 1 Full/DR 00:00:40192.168.1.2 GigabitEthernet 0/1 192.168.2.2 1 Full/BDR00:00:34 192.168.2.2 GigabitEthernet 0/2 A# show ip route ospf O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
B	B# show ip ospf neighbor OSPF process 1, 2 Neighbors, 2 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.1.1 GigabitEthernet 0/1 192.168.3.2 1 Full/BDR00:00:30 192.168.3.2 GigabitEthernet 0/2 B# show ip route ospf O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
C	C# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.1 1 Full/BDR 00:00:32 192.168.2.1 GigabitEthernet 0/3 C# show ip route ospf O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3 O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
D	D# show ip ospf neighbor OSPF process 1,1 Neighbors,1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.168.1.21 Full/BDR00:00:30 192.168.3.1 GigabitEthernet 0/3

```
D# show ip route ospf
O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3
O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:19:05, GigabitEthernet 0/3

D# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms.
```

Common Errors

- OSPF cannot be enabled because the IP unicast routing function is disabled.
- The network segment configured by the **network** command does not include the interface IP addresses.
- The area IDs enabled on adjacent interfaces are inconsistent.
- The same router ID is configured on multiple routers, resulting in a router ID conflict.
- The same interface IP address is configured on multiple routers, resulting in a running error of the OSPF network.

1.4.2 Setting the Network Type

Configuration Effect

- Run OSPF to provide the IPv4 unicast routing service if the physical network is X.25, frame relay, or ATM.

Notes

- The OSPF basic functions must be configured.
- The broadcast network sends OSPF packets in multicast mode. Neighbors are automatically discovered, and the DR/BDR election is required.
- The P2P network sends OSPF packets in multicast mode. Neighbors are automatically discovered.
- The NBMA network sends OSPF packets in unicast mode. Neighbors must be manually specified, and the DR/BDR election is required.
- The P2MP network (without the **non-broadcast** parameter) sends OSPF packets in multicast mode. Neighbors are automatically discovered.
- The P2MP network (with the **non-broadcast** parameter) sends OSPF packets in unicast mode. Neighbors must be manually specified.

Configuration Steps

↘ Configuring the Interface Network Type

- Optional.

- The configuration is required on routers at both ends of the link.

Configuring Neighbors

- (Optional) If the interface network type is set to NBMA or P2MP (with the **non-broadcast** parameter), neighbors must be configured.
- Neighbors are configured on routers at both ends of the NBMA or P2MP (with the **non-broadcast** parameter) network.

Configuring the Interface Priority

- (Optional) You must configure the interface priority if a router must be specified as a DR, or a router cannot be specified as a DR.
- Configure the interface priority on a router that must be specified as a DR, or cannot be specified as a DR.

Verification

- Run the **show ip ospf interface** command to verify that the network type of each interface is correct.

Related Commands

Configuring the Interface Network Type

Command	**ip ospf network** { **broadcast** | **non-broadcast**| **point-to-multipoint** [**non-broadcast**] | **point-to-point** }
Parameter Description	**broadcast**: Sets the interface network type to broadcast. **non-broadcast:** Sets the interface network type to non-broadcast. **point-to-multipoint** [**non-broadcast**]: Sets the interface network type to P2MP. If the interface does not have the broadcast capability, the **non-broadcast** parameter must be available. **point-to-point:** Sets the interface network type to P2P.
Command Mode	Interface configuration mode
Usage Guide	The broadcast type requires that the interface must have the broadcast capability. The P2P type requires that the interfaces are interconnected in one-to-one manner. The NBMA type requires full-meshed connections, and all interconnected routers can directly communicate with each other. The P2MP type does not raise any requirement.

Configuring Neighbors

Command	**neighbor** *ipv4-address* [**cost** *cost* | [**poll-interval** *poll-interval* | **priority** *priority*] *]
Parameter Description	*ipv4-address*: Indicates the IP address of the neighbor interface. **cost** *cost***:** Indicates the cost required to reach each neighbor. There is no default value. The value ranges from 0 to 65,535. This parameter is applicable only to the P2MP interface. **poll-interval** *poll-interval***:** Indicates the neighbor polling interval. The unit is second. The value ranges from 0 to 2,147,483,647. This parameter is applicable only to the NBMA interface. **priority** *priority*: Indicates the neighbor priority. The value ranges from 0 to 255. This parameter is applicable only to the NBMA interface.
Command Mode	OSPF routing process configuration mode

Usage Guide	Neighbors must be specified for the NBMA or P2MP (non-broadcast) interfaces. The neighbor IP address must be the primary IP address of this neighbor interface. If a neighbor router becomes inactive on the NBMA network, OSPF still sends Hello packets to this neighbor even if no Hello packet is received within the router death time. The interval at which the Hello packet is sent is called polling interval. When running for the first time, OSPF sends Hello packets only to neighbors whose priorities are not 0. In this way, neighbors with priorities set to 0 do not participate in the DR/BDR election. After a DR/BDR is elected, the DR/BDR sends the Hello packets to all neighbors to set up the adjacency. The P2MP (non-broadcast) network cannot dynamically discover neighbors because it does not have the broadcast capability. Therefore, you must use this command to manually configure neighbors for the P2MP (non-broadcast) network. In addition, you can use the **cost** parameter to specify the cost to reach each neighbor on the P2MP network.

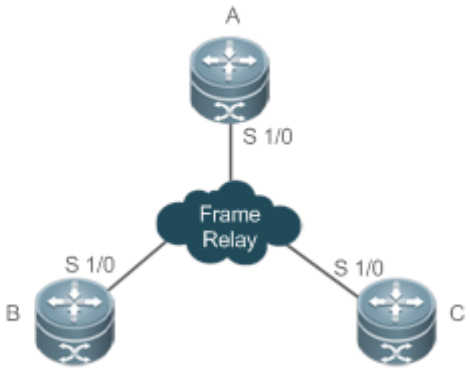
Configuring the Interface Priority

Command	**ip ospf priority** *priority*
Parameter Description	*priority*: Indicates the OSPF priority of an interface. The value ranges from 0 to 255.
Command Mode	Interface configuration mode
Usage Guide	The OSPF interface priority is contained in the Hello packet. When the DR/BDR election occurs on the OSPF broadcast network, the router with the highest priority becomes the DR or BDR. If the priorities are the same, the router with the largest router ID becomes the DR or BDR. A router with the priority set to 0 does not participate in the DR/BDR election. This command is applicable only to the OSPF broadcast and NBMA interfaces.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Setting the Interface Network Type to P2MP

Scenario **Figure 1-8**	 **Remarks** The interface IP addresses are as follows: A: S1/0 192.168.1.2 B: S1/0 192.168.1.3 C: S1/0 192.168.1.4
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Set the interface network type to P2MP on all routers.

A	`A#configure terminal`
	`A(config)# interface Serial1/0`
	`A(config-Serial1/0)# encapsulation frame-relay`
	`A(config-Serial1/0)# ip ospf network point-to-multipoint`

B	`B#configure terminal`
	`B(config)# interface Serial1/0`
	`B(config-Serial1/0)# encapsulation frame-relay`
	`B(config-Serial1/0)# ip ospf network point-to-multipoint`

C	`C#configure terminal`
	`C(config)# interface Serial1/0`
	`C(config-Serial1/0)# encapsulation frame-relay`
	`C(config-Serial1/0)# ip ospf network point-to-multipoint`

Verification	Verify that the interface network type is P2MP.
	`A# show ip ospf interface Serial1/0`
	`Serial1/0 is up, line protocol is up`
	`Internet Address 192.168.1.2/24, Ifindex 2, Area 0.0.0.1, MTU 1500`
	`Matching network config: 192.168.1.0/24`
	`Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1`
	`Transmit Delay is 1 sec, State Point-To-Point`
	`Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5`
	`Hello due in 00:00:02`
	`Neighbor Count is 1, Adjacent neighbor count is 0`
	`Crypt Sequence Number is 4787`
	`Hello received 465 sent 466, DD received 8 sent 8`
	`LS-Req received 2 sent 2, LS-Upd received 8 sent 21`
	`LS-Ack received 14 sent 7, Discarded 3`

Common Errors

- The network types configured on interfaces at two ends are inconsistent, causing abnormal route learning.
- The network type is set to NBMA or P2MP (with the **non-broadcast** parameter), but neighbors are not specified.

1.4.3 Configuring Route Redistribution and Default Route

Configuration Effect

- In the OSPF domain, introduce a unicast route to other AS domains so that the unicast routing service to other AS domains can be provided for users in the OSPF domain.
- In the OSPF domain, inject a default route to other AS domains so that the unicast routing service to other AS domains can be provided for users in the OSPF domain.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Configuring External Route Redistribution

- (Optional) This configuration is required if external routes of the OSPF domain should be introduced to an ASBR.
- This configuration is performed on an ASBR.

↘ Generating a Default Route

- (Optional) This configuration is required if the default route should be introduced to an ASBR so that other routers in the OSPF domain access other AS domains through this ASBR by default.

- This configuration is performed on an ASBR.

Verification

- On a router inside the OSPF domain, run the **show ip route** command to verify that the unicast routes to other AS domains are loaded.
- On a router inside the OSPF domain, run the **show ip route** command to verify that the default route to the ASBR is loaded.
- Run the **ping** command to verify that the IPv4 unicast service to other AS domains is correct.

Related Commands

Configuring External Route Redistribution

Command	**redistribute** { **connected** | **ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1 | 2**] } *] | **rip** | **static** } [**metric** *metric-value* | **metric-type** { **1** | **2** } | **route-map** *route-map-name* | **subnets** | **tag** *tag-value*] *
Parameter Description	**connected:** Indicates redistribution from direct routes. **ospf** *process-id:* Indicates redistribution from OSPF. *process-id* specifies an OSPF process. The value ranges from 1 to 65,535. **match:** Used only when OSPF routes are redistributed. Only the routes meeting the filtering conditions are redistributed. By default, all OSPF routes can be redistributed. **external [** 1 **|** 2 **]:** E1, E2, or all external routes. **internal**: Intra-area route and inter-area route. **nssa-external [1 | 2]:** N1, N2, or all external routes in the NSSA area. **rip:** Indicates redistribution from RIP. **static:** Indicates redistribution from static routes. **metric** *metric-value:* Specifies the metric of the OSPF external LSA. *metric-value* specifies the size of the metric. The value ranges from 0 to 16,777,214. **metric-type** { **1** | **2** }: Sets the external route type, which can be E-1 or E-2. **route-map** *route-map-name:* Sets the redistribution filtering rules. **subnets:** Specifies the non-standard networks for redistribution. **tag** *tag-value:* Specifies the tag value of the route that is redistributed into the OSPF routing domain. The value ranges from 0 to 4,294,967,295.
Command Mode	OSPF routing process configuration mode
Usage Guide	After this command is configured, the router becomes an ASBR, imports related routing information to the OSPF domain, and advertises the routing information as Type 5 LSAs to other OSPF routers in the domain. If you configure redistribution of OSPF routes without specifying the **match** parameter, OSPF routes of all sub-types can be distributed by default. The latest setting of the **match** parameter is used as the initial **match** parameter. Only routes that match the sub-types can be redistributed. You can use the **no** form of the command to restore the default value of **match**. For details, see the configuration example. If **route-map** is specified, the filtering rules specified in **route-map** are applicable to original parameters of redistribution. For redistribution of OSPF, the route map is used for filtering only when the redistributed routes meet criteria specified by **match**. The **set metric** value associated with **route-map** should fall into the range of 0 to 16,777,214. If the value

	exceeds this range, routes cannot be introduced. The configuration rules for the **no** form of the **redistribute** command are as follows: 1. If some parameters are specified in the **no** form of the command, default values of these parameters will be restored. 2. If no parameter is specified in the **no** form of the command, the entire command will be deleted.

Introducing a Default Route

Command	**default-information originate** [**always** | **metric** *metric* | **metric-type** *type* | **route-map** *map-name*] *
Parameter Description	**always:** Enables OSPF to generate a default route regardless of whether the local router has a default route. **metric** *metric:* Indicates the initial metric of the default route. The value ranges from 0 to 16,777,214. **metric-type** *type:* Indicates the type of the default route. OSPF external routes are classified into two types: Type 1: The metric varies with routers; Type 2: The metric is the same for all routers. Type 1 external routes are more trustworthy than Type 2 external routes. **route-map** *map-name:* Indicates the associated route-map name. By default, no route-map is associated.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the **redistribute** or **default-information** command is executed, the OSPF router automatically becomes an ASBR. The ASBR, however, does not automatically generate or advertise a default route to all routers in the OSPF routing domain. To have the ASBR generates a default route, configure the **default-information originate** command. If **always** is specified, the OSPF routing process advertises an external default route to neighbors regardless of whether a default route exists. This default route, however, is not displayed on the local router. To confirm whether the default route is generated, run the **show ip ospf database** command to display the OSPF link status database. The external link with the ID 0.0.0.0 describes the default route. On an OSPF neighbor, you can run the **show ip route** command to see the default route. The metric of the external default route can only be defined in the **default-information originate** command, instead of the **default-metric** command. OSPF has two types of external routes. The metric of the Type 1 external route changes, but the metric of the Type 2 external route is fixed. If two parallel paths to the same destination have the same route metric, the priority of the Type 1 route is higher than that of the Type 2 route. Therefore, the **show ip route** command displays only the Type 1 route. A router in the stub area cannot generate an external default route. The **set metric** value associated with **route-map** should fall into the range of 0 to 16,777,214. If the value exceeds this range, routes cannot be introduced.

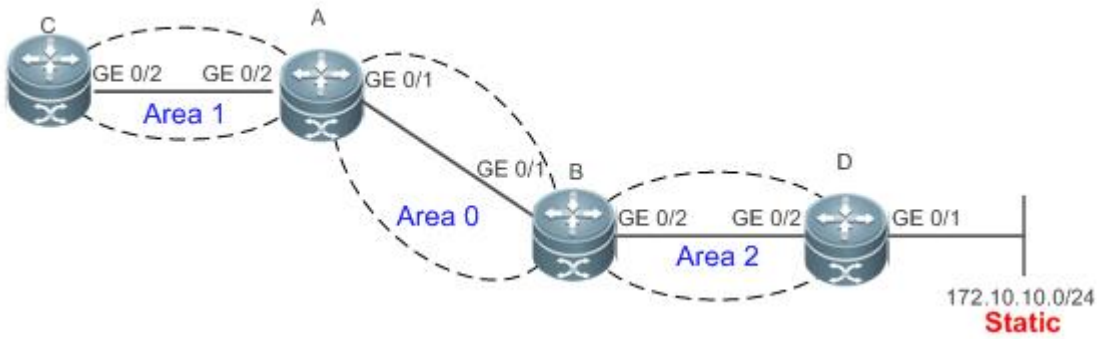
Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Configuring Static Route Redistribution

Scenario

Figure 1-9



Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

Configuration Steps

- Configure the interface IP addresses on all routers. (Omitted)
- Configure the OSPF basic functions on all routers. (Omitted)
- Introduce an external static route to Router D.

D

```
D# configure terminal
D(config)# ip route 172.10.10.0 255.255.255.0 192.168.6.3
D(config)#router ospf 1
D(config-router)# redistribute staticsubnets
```

Verification

- On Router D, run the **show ip ospf database external brief** command to verify that an LSA corresponding to an external route is generated.
- On Router C, run the **show ip route ospf** command to verify that the external static route has been introduced.

D

```
D# show ip ospf database external brief
          OSPF Router with ID (192.168.22.30) (Process ID 1)
              AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route              Tag
172.10.10.0     192.168.22.30   11   0x80000001 0xa4bb E2 172.10.10.0/24    0
```

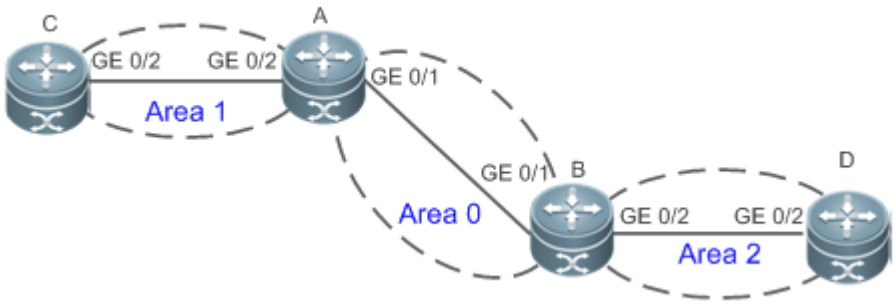
C

```
C# show ip route ospf
O E2 172.10.10.0/24 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2
```

Configuring the Default Route

Scenario

Figure 1-10



Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/2 192.168.3.2

Configuration Steps

- Configure the interface IP addresses on all routers. (Omitted)
- Configure the OSPF basic functions on all routers. (Omitted)
- Configure the default route on Router D.

D

```
D# configure terminal
D(config)#router ospf 1
D(config-router)#default-information originate always
```

Verification

- On Router D, run the **show ip ospf database external brief** command to verify that an LSA corresponding to the default route is generated.
- On Router C, run the **show ip route ospf** command to verify that the OSPF default route exists.

D

```
D#show ip ospf database external brief

          OSPF Router with ID (192.168.22.30) (Process ID 1)

              AS External Link States


Link ID         ADV Router      Age  Seq#       CkSum  Route              Tag
0.0.0.0         192.168.22.30   565  0x80000002 0xa190 E2 0.0.0.0/0         1
```

C

```
C# show ip route ospf
O E20.0.0.0/0 [110/20] via 192.168.2.1, 00:18:03, GigabitEthernet 0/2
```

Common Errors

- The subnet route is not introduced because the **subnets** parameter in the **redistribute** command is not configured.
- A routing loop is formed because the **default-information originate always** command is configured on multiple routers.
- Routes cannot be introduced because route redistribution is configured on a router in the stub area.

1.4.4 Configuring Stub Area and NSSA Area

Configuration Effect

- Configure an area located on the stub as a stub area to reduce interaction of routing information and the size of routing table, and enhance stability of routes.

Notes

- The OSPF basic functions must be configured.
- A backbone or transit area cannot be configured as a stub or an NSSA area.
- A router in the stub area cannot introduce external routes, but a router in the NSSA area can introduce external routes.

Configuration Steps

↘ Configuring a Stub Area

- (Optional) This configuration is required if you wish to reduce the size of the routing table on routers in the area.
- The area must be configured as a stub area on all routers in this area.

↘ Configuring an NSSA Area

- (Optional) This configuration is required if you wish to reduce the size of the routing table on routers in the area and introduce OSPF external routes to the area.
- The area must be configured as an NSSA area on all routers in this area.

Verification

↘ Verifying the Stub Area

- On a router in the stub area, run the **show ip route** command to verify that the router is not loaded with any external routes.

↘ Verifying the NSSA Area

- On a router in the NSSA area, run the **show ip ospf database** command to verify that the introduced external route generates Type 7 LSAs.
- On a router in the backbone area, run the **show ip route** command to verify that the router is loaded with external routes introduced from the NSSA area.

Related Commands

Configuring a Stub Area

Command	**area** *area-id* **stub** [**no-summary**]
Parameter Description	*area-id:* Indicates the ID of the stub area. **no-summary:** Prohibits the ABR from sending network summary LSAs. At this time, the stub can be called totally stub area. This parameter is configured only when the router is an ABR.
Command Mode	OSPF routing process configuration mode
Usage Guide	You must run the **area stub** command on all routers in the OSPF stub area. The ABR sends only three types of LSAs to the stub area: (1) Type 1: Router LSA; (2) Type 2: Network LSA; (3) Type 3: Network Summary LSA. From the routing table point of view, a router in the stub area can learn only the internal routes of the OSPF routing domain, including the internal default route generated by an ABR. A router in the stub area cannot learn external routes of the OSPF routing domain. To configure a totally stub area, add the **no-summary** keyword when running the **area stub** command on the ABR. A router in the totally stub area can learn only the internal routes of the local area, including the internal default route generated by an ABR. You can run either the **area stub** or **area default-cost** command to configure an OSPF area as a stub area. If **area stub** is used, you must configure this command on all routers connected to the stub area. If **area default-cost** is used, run this command only on the ABR in the stub area. The **area default-cost** command defines the initial cost (metric) of the internal default route.

Configuring an NSSA Area

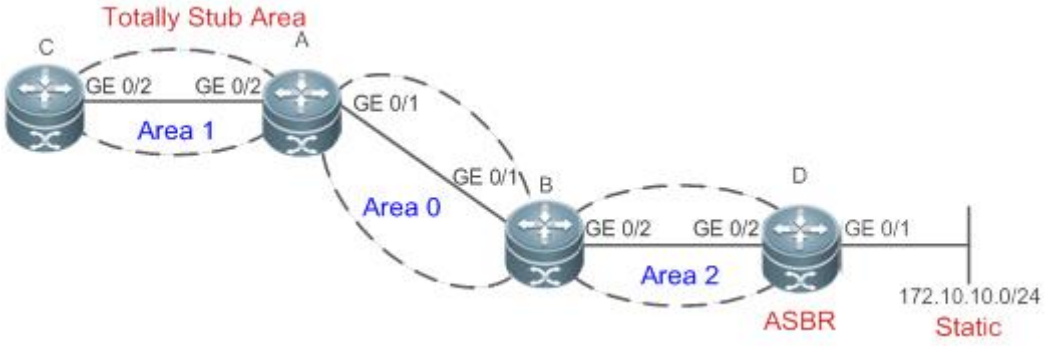
Command	**area** *area-id* **nssa** [**default-information-originate** [**metric** *metric* | **metric-type** *metric-type*] * | **no-redistribution** | **no-summary** | **translator** [**always** | **stability-interval** *stability-interval*] *] *
Parameter Description	*area-id:* Indicates the ID of the NSSA area. **default-information-originate:** Indicates that a default Type 7 LSA is generated and introduced to the NSSA area. This option takes effect only on an NSSA ABR or ASBR. **metric** *metric:* Specifies the metric of the generated default LSA. The value ranges from 0 to 16,777,214. The default value is 1. **metric-type** *metric-type e:* Specifies the route type of the generated default LSA. The values include 1 and 2. **1** represents N-1, and **2** represents N-2. The default value is 2. **no-redistribution:** Select this option if the router is an NSSA ABR and you want to use only the **no-summary:** Prohibits the ABR in the NSSA area from sending summary LSAs (Type-3 LSA). **translator:** Indicates that the NSSA ABR is a translator. **always:** Indicates that the current NSSA ABR always acts as a translator. The default value is the standby translator. **stability-interval** *seconds:* Indicates the stability interval after the NSSA ABR is changed from a translator to a non-translator. The unit is second. The default value is 40. The value ranges from 0 to 2,147,483,647.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-information-originate** parameter is used to generate a default Type 7 LSA. This parameter has different functions on the ABR and the ASBR in the NSSA area. On the ABR, a Type 7 LSA default route is generated regardless of whether the default route exists in the routing table. On the ASBR (not an ABR), a Type 7 LSA default route is generated only when the default route exists in the routing table. If the **no-redistribution** parameter is configured on the ASBR, other external routes introduced by OSPF

	through the **redistribute** command cannot be advertised to the NSSA area. This parameter is generally used when a router in the NSSA area acts both as the ASBR and the ABR. It prevents external routing information from entering the NSSA area. To further reduce the number of LSAs sent to the NSSA area, you can configure the **no-summary** parameter on the ABR to prevent the ABR from sending the summary LSAs (Type 3 LSA) to the NSSA area. **area default-cost** is used on an ABR or ASBR connected to the NSSA area. This command configures the cost of the default route sent from the ABR/ASBR to the NSSA area. By default, the cost of the default route sent to the NSSA area is 1. If an NSSA area has two or more ABRs, the ABR with the largest router ID is elected by default as the translator for converting Type 7 LSAs into Type 5 LSAs. If the current device is always the translator ABR for converting Type 7 LSAs into Type 5 LSAs, use the **translator always** parameter. If the translator role of the current device is replaced by another ABR, the conversion capability is retained during the time specified by **stability-interval**. If the router does not become a translator again during **stability-interval**, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS after **stability-interval** expires. To prevent a routing loop, LSAs that are converted from Type 7 to Type 5 will be deleted from the AS immediately after the current device loses the translator role even if **stability-interval** does not expire. In the same NSSA area, it is recommended that **translator always** be configured on only one ABR.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Configuring a Stub Area

Scenario **Figure 1-11**	
	Remarks The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 1 as the stub area on Router A and Router C.

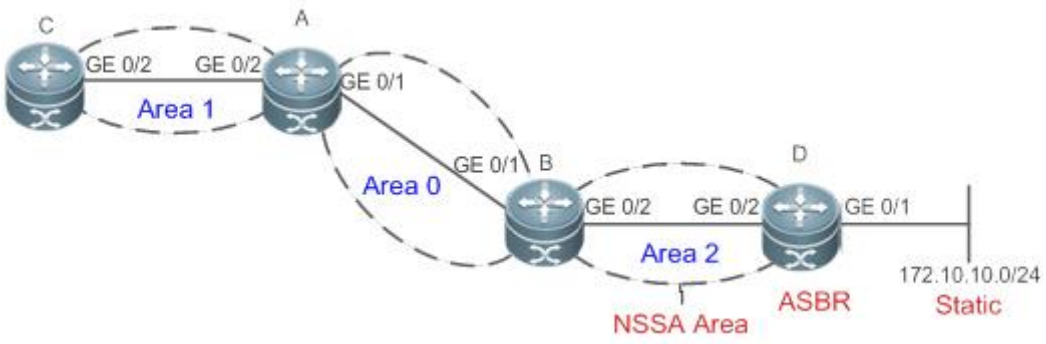
D	`D# configure terminal`
	`D(config)#router ospf 1`
	`D(config-router)# redistribute staticsubnets`

A	`A# configure terminal`
	`A(config)#router ospf 1`
	`A(config-router)#area 1 stubno-summary`

C	`C# configure terminal`
	`C(config)#router ospf 1`
	`C(config-router)#area 1 stub`

Verification	On Router C, run the **show ip route ospf** command to display the routing table. Verify that there is only one default inter-area route, and no external static route is introduced from Router D.
	`C#show ip route ospf` `O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/2`

Configuring an NSSA Area

Scenario Figure 1-12	

Remarks	The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 B: GE 0/1 192.168.1.2 GE 0/2 192.168.3.1 C: GE 0/2 192.168.2.2 D: GE 0/1 192.168.6.2 GE 0/2 192.168.3.2

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Introduce an external static route to Router D. ● Configure area 2 as the NSSA area on Router B and Router D.

B	`B# configure terminal`
	`B(config)#router ospf 1`
	`B(config-router)#area 2 nssa`

D	`D# configure terminal`
	`D(config)#ip route 172.10.10.0 255.255.255.0 192.168.6.2`
	`D(config)#router ospf 1`
	`D(config-router)#redistribute static subnets`
	`D(config-router)#area 2 nssa`

Verification	● On Router D, verify that the Type 7 LSA, 172.10.10.0/24, is generated. ● On Router B, verify that Type 5 and Type 7 LSAs coexist on 172.10.10.0/24. ● On Router B, verify that the N-2 route of 172.10.10.0/24 is generated.

D	`D# show ip ospf database nssa-external`
	`OSPF Router with ID (192.168.6.2) (Process ID 1)`
	`NSSA-external Link States (Area 0.0.0.1 [NSSA])`
	`LS age: 61`
	`Options: 0x8 (-|-|-|-|N/P|-|-|-)`
	`LS Type: AS-NSSA-LSA`
	`Link State ID: 172.10.10.0 (External Network Number For NSSA)`
	`Advertising Router: 192.168.6.2`
	`LS Seq Number: 80000001`
	`Checksum: 0xc8f8`
	`Length: 36`
	`Network Mask: /24`
	`Metric Type: 2 (Larger than any link state path)`
	`TOS: 0`
	`Metric: 20`
	`NSSA: Forward Address: 192.168.6.2`

```
      External Route Tag: 0
```

B

```
B# show ip ospf database nssa-external

          OSPF Router with ID (192.168.3.1) (Process ID 1)

              NSSA-external Link States (Area 0.0.0.1 [NSSA])

  LS age: 314

  Options: 0x8 (-|-|-|-|N/P|-|-|-)

  LS Type: AS-NSSA-LSA

  Link State ID: 172.10.10.0 (External Network Number For NSSA)

  Advertising Router: 192.168.6.2

  LS Seq Number: 80000001

  Checksum: 0xc8f8

  Length: 36

  Network Mask: /24

       Metric Type: 2 (Larger than any link state path)

       TOS: 0

       Metric: 20

       NSSA: Forward Address: 192.168.6.2

       External Route Tag: 0

B# show ip ospf database external

          OSPF Router with ID (192.168.3.1) (Process ID 1)

              AS External Link States

  LS age: 875

  Options: 0x2 (-|-|-|-|-|-|E|-)

  LS Type: AS-external-LSA

  Link State ID: 172.10.10.0 (External Network Number)

  Advertising Router: 192.168.3.1

  LS Seq Number: 80000001

  Checksum: 0xd0d3

  Length: 36

  Network Mask: /24

       Metric Type: 2 (Larger than any link state path)

       TOS: 0

       Metric: 20

       Forward Address: 192.168.6.2
```

	External Route Tag: 0 B# show ip route ospf O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:06:53, GigabitEthernet 0/2

Common Errors

- Configurations of the area type are inconsistent on routers in the same area.
- External routes cannot be introduced because route redistribution is configured on a router in the stub area.

1.4.5 Configuring Route Summarization

Configuration Effect

- Summarize routes to reduce interaction of routing information and the size of routing table, and enhance stability of routes.
- Shield or filter routes.

Notes

- The OSPF basic functions must be configured.
- The address range of summarized routes may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table or shield or filter routes.

Configuration Steps

↘ Configuring Inter-Area Route Summarization

- (Optional) This configuration is required when routes of the OSPF area need to be summarized.
- Unless otherwise required, this configuration should be performed on an ABR in the area where routes to be summarized are located.

↘ Configuring External Route Summarization

- (Optional) This configuration is required when routes external to the OSPF domain need to be summarized.
- Unless otherwise required, this configuration should be performed on an ASBR to which routes to be summarized are introduced.

Verification

Run the **show ip route ospf** command to verify that individual routes do not exist and only the summarized route exists.

Related Commands

↘ Configuring Inter-Area Route Summarization

Command	**area** *area-id* **range** *ipv4-address net-mask* [**advertise** | **not-advertise**] [**cost** *cost*]
Parameter	*area-id*: Specifies the ID of the OSPF area to which the summarized route should be injected. The area ID

Description	can be a decimal integer or an IP address. *ipv4-address net-mask*: Defines the network segment of the summarized route. **advertise** | **not-advertise**: Specifies whether the summarized route should be advertised. **cost** *cost:* Indicates the metric of the summarized route. The value ranges from 0 to 16777215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command can be executed only on the ABR. It is used to combine or summarize multiple routes of an area into one route, and advertise the route to other areas. Combination of the routing information occurs only on the boundary of an area. Routers inside the area can learn specific routing information, whereas routers in other areas can learn only one summarized route. In addition, you can set **advertise** or **not-advertise** to determine whether to advertise the summarized route to shield and filter routes. By default, the summarized route is advertised. You can use the **cost** parameter to set the metric of the summarized route. You can configure route summarization commands for multiple areas. This simplifies routes in the entire OSPF routing domain, and improve the network forwarding performance, especially for a large-sized network. When multiple route summarization commands are configured and have the inclusive relationship with each other, the area range to be summarized is determined based on the maximum match principle.

Configuring External Route Summarization

Command	**summary-address** *ipv4-address net-mask* [[**cost** *cost* | **tag** *value*] * | **not-advertise**]
Parameter Description	*ipv4-addres*: Indicates the IP address of the summarized route. *net-mask*: Indicates the subnet mask of the summarized route. **cost** *cost*: Sets the cost value of the aggregation route. The value ranges from 0 to 16,777,214. **tag** *value:* Indicates the tag of the summarized route. The value ranges from 0 to 4,294,967,295. **not-advertise**: Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised.
Command Mode	OSPF routing process configuration mode
Usage Guide	When routes are redistributed from other routing processes and injected to the OSPF routing process, each route is advertised to the OSPF routers using an external LSA. If the injected routes are a continuous address space, the ABR can advertised only one summarized route to significantly reduce the size of the routing table. **area range** summarizesthe routes between OSPF routes, whereas **summary-address** summarizes external routes of the OSPF routing domain. When configured on the NSSA ABR translator, **summary-address** summarizes redistributed routes and routes obtained based on the LSAs that are converted from Type 7 to Type 5. When configured on the ASBR (not an NSSA ABR translator), **summary-address** summarizes only redistributed routes.

Configuring a Discard Route

Command	**discard-route** { **internal** | **external** }
Parameter Description	**internal:** Indicates that the discard route generated by the **area range** command can be added. **external:** Indicates that the discard route generated by the **summary-address** command can be added.

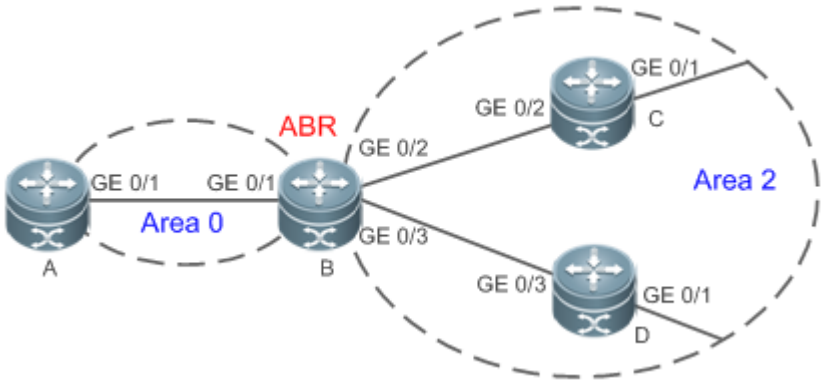
Command Mode	OSPF routing process configuration mode
Usage Guide	The address range of summarized routes may exceed the actual network range in the routing table. If data is sent to a network beyond the summarization range, a routing loop may be formed and the router processing load may increase. To prevent these problems, a discard route must be added to the routing table on the ABR or ASBR. This route is automatically generated, and is not advertised.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Scenario

Figure 1-13



Remarks	The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/1 172.16.4.2 D: GE0/2 172.16.3.2 GE0/1 172.16.5.2

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Summarize routes of area 2 on Router B.

B	`B# configure terminal`
	`B(config)#router ospf 1`
	`B(config-router)#area 2 range 172.16.0.0 255.255.0.0`

Verification	On Router A, verify that the entry 172.16.0.0/16 is added to the routing table.
A	`A#show ip route ospf` `O IA 172.16.0.0/16 [110/2] via 192.168.1.2, 00:01:04, GigabitEthernet 0/1`

Common Errors

- Inter-area route summarization cannot be implemented because the **area range** command is configured on a non-ABR device.

1.4.6 Configuring Route Filtering

Configuration Effect

- Routes that do not meet filtering conditions cannot be loaded to the routing table, or advertised to neighbors. Network users cannot access specified destination network.

Notes

- The OSPF basic functions must be configured.
- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated. In this case, you can run the **area filter-list** or **area range** (containing the **not-advertise** parameter) command on the ABR to prevent generation of black-hole routes.

Configuration Steps

↘ Configuring Inter-Area Route Filtering

- (Optional) This configuration is recommended if users should be restricted from accessing the network in a certain OSPF area.
- Unless otherwise required, this configuration should be performed on an ABR in the area where filtered routes are located.

↘ Configuring Redistributed Route Filtering

- (Optional) This configuration is required if external routes introduced by the ASBR need to be filtered.
- Unless otherwise required, this configuration should be performed on an ASBR to which filtered routes are introduced.

↘ Configuring Learned Route Filtering

- (Optional) This configuration is required if users should be restricted from accessing a specified destination network.
- Unless otherwise required, this configuration should be performed on a router that requires route filtering.

Verification

- Run the **show ip route** command to verify that the router is not loaded with routes that have been filtered out.
- Run the **ping** command to verify that the specified destination network cannot be accessed.

Related Commands

↘ Configuring a Passive Interface

Command	**passive-interface** { **default** | *interface-type interface-number* | *interface-type interface-number*

	ipv4-address}
Parameter Description	*interface-type interface-number*: Indicates the interface that should be configured as a passive interface. **default:** Indicates that all interface will be configured as passive interfaces. *interface-type interface-number ipv4-address:* Specifies an address of the interface as the passive address.
Command Mode	OSPF routing process configuration mode
Usage Guide	To prevent other routers on the network from learning the routing information of the local router, you can configure a specified network interface of the local router as the passive interface, or a specified IP address of a network interface as the passive address.

Configuring the LSA Update Packet Filtering

Command	**ip ospf database-filter all out**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Enable this function on an interface to prevent sending the LSA update packet on this interface. After this function is enabled, the local router does not advertise the LSA update packet to neighbors, but still sets up the adjacency with neighbors and receives LSAs from neighbors.

Configuring Inter-Area Route Filtering

Command	**area** *area-id* **filter-list** { **access** *acl-name* | **prefix** *prefix-name* } {**in** | **out**}
Parameter Description	*area-id*: Indicates the area ID. **access** *acl-name*: Indicates the associated ACL. **prefix** *prefix-name*: Indicates the associated prefix list. **in** | **out:** Filters routes that are received by or sent from the area.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command can be configured only on an ABR. Use this command when it is required to configure filtering conditions for inter-area routes on the ABR.

Configuring Redistributed Route Filtering

Command	**distribute-list** { *acl-name* | *acl-number* | **prefix** *prefix-list-name* } **out** [**connected** | **ospf** *process-id* **| rip | static**]
Parameter Description	*acl-name* | *acl-number*: Uses the ACL for filtering. **prefix** *prefix-list-name*: Uses the prefixlist for filtering. **connected**: Filters directly connected routes. **ospf** *process-id*: Filters OSPF routes. **rip**: Filters RIP routes. **static**: Filters static routes.
Command Mode	OSPF routing process configuration mode
Usage Guide	**distribute-list out** is similar to **redistribute route-map**, and is used to filter routes that are redistributed from other protocols to OSPF. The **distribute-list out** command itself does not redistribute routes, and is

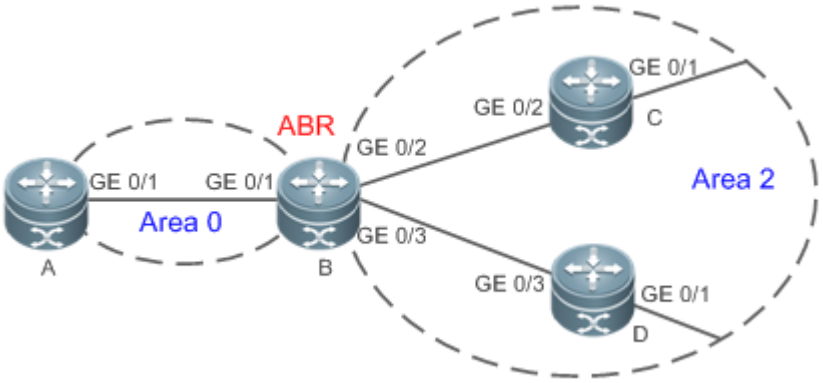
	generally used together with the **redistribute** command. The ACL and the prefixlist filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes coming from a certain source, the prefixlist cannot be configured to filter the same routes.

Configuring Learned Route Filtering

Command	**distribute-list** { *acl-name* | *acl-number* | [**prefix** *prefix-list-name*] [**gateway** *prefix-list-name*] } **in** [*interface-type interface-number*]
Parameter Description	*acl-name* | *acl-number*: Uses the ACL for filtering. **prefix** *prefix-list-name*: Uses the prefixlist for filtering. **gateway** *prefix-list-name*: Uses the gateway for filtering. **route-map** *route-map-name:* Uses the route map for filtering. *interface-type interface-number:* Specifies the interface for which LSA routes are filtered.
Command Mode	OSPF routing process configuration mode
Usage Guide	Filter routes that are computed based on received LSAs. Only routes meeting the filtering conditions can be forwarded. The command does not affect the LSDB or the routing tables of neighbors. The ACL, prefix list, and route map filtering rules are mutually exclusive in the configuration. That is, if the ACL is used for filtering routes of a specified interface, the prefix list or router map cannot be configured for filtering routes of the same interface.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Scenario **Figure 1-14**	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 B: GE0/1 192.168.1.2 GE0/2 172.16.2.1 GE0/3 172.16.3.1 C: GE0/2 172.16.2.2 GE0/3 172.16.4.2 D: GE0/2 172.16.3.2 GE0/3 172.16.5.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted)

	● On Router A, configure route filtering.

A	`A# configure terminal`
	`A(config)#access-list 3 permit host 172.16.5.0`
	`A(config)#router ospf 1`
	`A(config-router)#distribute-list 3 in GigabitEthernet 0/1`

Verification	● On Router A, check the routing table. Verify that only the entry 172.16.5.0/24 is loaded.
A	`A# show ip route ospf` `O  172.16.5.0/24 [110/2] via 192.168.1.2, 10:39:40, GigabitEthernet 0/1`

Common Errors

- Filtering routes by using the **distribute-list in** command affects forwarding of local routes, but does not affect route computation based on LSAs. Therefore, if route filtering is configured on the ABR, Type 3 LSAs will still be generated and advertised to other areas because routes can still be computed based on LSAs. As a result, black-hole routes are generated.

1.4.7 Modifying Route Cost and AD

Configuration Effect

- Change the OSPF routes to enable the traffic pass through specified nodes or avoid passing through specified nodes.
- Change the sequence that a router selects routes so as to change the priorities of OSPF routes.

Notes

- The OSPF basic functions must be configured.
- If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuration Steps

↘ Configuring the Reference Bandwidth

- Optional.
- A router is connected with lines with different bandwidths. This configuration is recommended if you wish to preferentially select the line with a larger bandwidth.

↘ Configuring the Cost of an Interface

- Optional.
- A router is connected with multiple lines. This configuration is recommended if you wish to manually specify a preferential line.

Configuring the Default Metric for Redistribution

- Optional.
- This configuration is mandatory if the cost of external routes of the OSPF domain should be specified when external routes are introduced to an ASBR.

Configuring the Maximum Metric

- Optional.
- A router may be unstable during the restart process or a period of time after the router is restarted, and users do not want to forward data through this router. In this case, this configuration is recommended.

Configuring the AD

- Optional.
- This configuration is mandatory if you wish to change the priorities of OSPF routes on a router that runs multiple unicast routing protocols.

Verification

- Run the **show ip ospf interface** command to verify that the costs of interfaces are correct.
- Run the **show ip route** command to verify that the costs of external routes introduced to the ASBR are correct.
- Restart the router. Within a specified period of time, data is not forwarded through the restarted router.

Related Commands

Configuring the Reference Bandwidth

Command	**auto-cost reference-bandwidth** *ref-bw*
Parameter Description	*ref-bw*: Indicates the reference bandwidth. The unit is Mbps. The value ranges from 1 to 4,294,967.
Command Mode	OSPF routing process configuration mode
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the **bandwidth** command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps serial line: The cost is 1562. E1 line: The cost is 48. 10M Ethernet: The cost is 10. 100M Ethernet: The cost is 1. If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuring the Cost of an Interface

Command	**ip ospf cost** *cost*

Parameter Description	*cost*: Indicates the cost of an OSPF interface. The value ranges from 0 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	By default, the cost of an OSPF interface is equal to the reference value of the auto cost divided by the interface bandwidth. Run the **auto-cost** command to obtain the reference value of the auto cost. The default value is 100 Mbps. Run the **bandwidth** command to set the interface bandwidth. The costs of OSPF interfaces on several typical lines are as follows: 64Kbps serial line: The cost is 1562. E1 line: The cost is 48. 10M Ethernet: The cost is 10. 100M Ethernet: The cost is 1. If you run the **ip ospf cost** command to configure the cost of an interface, the configured cost will automatically overwrite the cost that is computed based on the auto cost.

Configuring the Cost of the Default Route in a Stub or an NSSA Area

Command	**area** *area-id* **default-cost** *cost*
Parameter Description	*area-id*: Indicates the ID of the stub or NSSA area. *cost*: Indicates the cost of the default summarized route injected to the stub or NSSA area. The value ranges from 0 to 16,777,215.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command takes effect only on an ABR in a stub area or an ABR/ASBR in an NSSA area. An ABR in a stub area or an ABR/ASBR in an NSSA area is allowed to advertise an LSA indicating the default route in the stub or NSSA area. You can run the **area default-cost** command to modify the cost of the advertised LSA.

Configuring the Default Metric for Redistribution

Command	**default-metric** *metric*
Parameter Description	*metric*: Indicates the default metric of the OSPF redistributed route. The value ranges from 1 to 16,777,214.
Command Mode	OSPF routing process configuration mode
Usage Guide	The **default-metric** command must be used together with the **redistribute** command to modify the initial metrics of all redistributed routes. The **default-metric**command does not take effect on external routes that are injected to the OSPF routing domain by the **default-information originate** command.

Configuring the Maximum Metric

Command	**max-metric router-lsa** [**external-lsa** [*max-metric-value*] | **include-stub** | **on-startup** [*startup-interval-time*] | **summary-lsa** [*max-metric-value*]] *
Parameter Description	**router-lsa**: Sets the metrics of non-stub links in the Router LSA to the maximum value (0xFFFF). **external-lsa**: Allows a router to replace the metrics of external LSAs (including Type 5 and Type 7 LSAs)

	with the maximum metric. *max-metric-value*: Indicates the maximum metric of the external LSA. The default value is 16711680. The value ranges from 1 to 16,777,215. **include-stub:** Sets the metrics of stub links in the Router LSA advertised by the router to the maximum value. **on-startup:** Allows a router to advertise the maximum metric when started. *startup-interval-time:* Indicates the interval at which the maximum metric is advertised. The default value is 600s. The value ranges from 5 to 86,400. **summary-lsa:** Allows a router to replace the metrics of summary LSAs (including Type 3 and Type 4 LSAs) with the maximum metric. *max-metric-value*: Sets the maximum metric value for summary LSAs. The default value is 16,711,680. The value ranges from 1 to 16,777,215.
Command Mode	OSPF routing process configuration mode
Usage Guide	After the **max-metric router-lsa** command is executed, the metrics of the non-stub links in the Router LSAs generated by the router will be set to the maximum value (0xFFFF). If you cancel this configuration or the timer expires, the normal metrics of the links are restored. By default, if the **max-metric router-lsa** command is executed, the stub links still advertise common metrics, that is, the costs of outbound interfaces. If the **include-stub** parameter is configured, the stub links will advertise the maximum metric. If an ABR does not wish to transfer inter-area traffic, use the **summary-lsa** parameter to set the metric of the Summary LSA to the maximum metric. If an ASBR does not wish to transfer external traffic, use the **external-lsa** parameter to set the metric of the external LSA to the maximum metric. The **max-metric router-lsa** command is generally used in the following scenarios: Restart a device. After the device is restarted, IGP generally converges faster, and other devices attempt to forward traffic through the restarted device. If the current device is still building the BGP routing table and some BGP routes have not been learned yet, packets destined for these networks will be discarded. In this case, the **on-startup** parameter can be used to set a certain delay, so that transmission as a transit node will start after the timer expires. ● Add a device to the network but the device is not used to transfer traffic. The device is added to the network. If a candidate path exists, the current device is not used to transfer traffic. If a candidate path does not exist, the current device is still used to transfer traffic. ● Delete a device gracefully from the network. After the **max-metric router-lsa** command is executed, the current device advertises the maximum metric among all metrics of routes. In this way, other devices on the network can select the standby path for data transmission before the device is shut down. In the earlier OSPF version (RFC1247 or earlier), the links with the maximum metric (0xFFFF) in the LSAs do not participate in the SPF computation, that is, no traffic is sent to routers that generate these LSAs.

Configuring RFC1583Compatibility

Command	**compatible rfc1583**
Parameter	N/A

Description	
Command Mode	OSPF routing process configuration mode
Usage Guide	When there are multiple paths to an ASBR or the forwarding address of an external route, RFC1583 and RFC2328 define different routing rules. If RFC1583 compatibility is configured, a path in the backbone area or an inter-area path is preferentially selected. If RFC1583 compatibility is not configured, a path in a non-backbone area is preferentially selected.

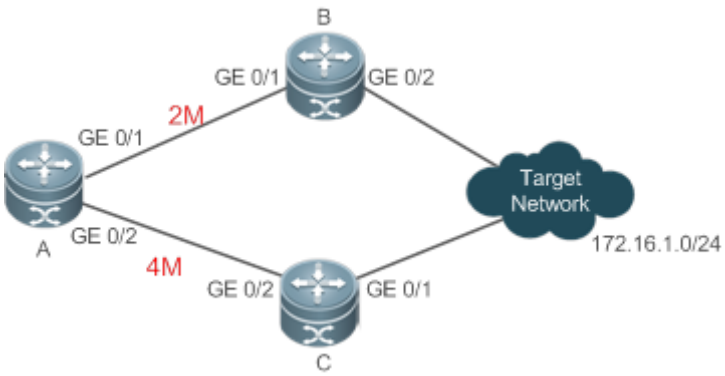
Configuring the AD

Command	**distance** { *distance* | **ospf** { **external** *distance* | **inter-area** *distance* | **intra-area** *distance* } * }
Parameter Description	*distance*: Indicates the AD of a route. The value ranges from 1 to 255. **intra-area** *distance*: Indicates the AD of an intra-area route. The value ranges from 1 to 255. **inter-area** *distance*: Indicates the AD of an inter-area route. The value ranges from 1 to 255. **external** *distance:* Indicates the AD of an external route. The value ranges from 1 to 255.
Command Mode	OSPF routing process configuration mode
Usage Guide	N/A

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Configuring the Cost of an Interface

Scenario Figure 1-15	 **Remarks**: The interface IP addresses are as follows: A: GE0/1 192.168.1.1 GE0/2 192.168.2.1 B: GE0/1 192.168.1.2 GE0/2 192.168.3.2 C: GE0/1 192.168.4.2 GE0/2 192.168.2.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, configure the cost of each interface.

A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf cost 10 A(config)# interface GigabitEthernet 0/2 A(config-if-GigabitEthernet 0/2)# ip ospf cost 20
Verification	On Router A, check the routing table. The next hop of the optimum path to 172.16.1.0/24 is Router B.
A	A# show ip route ospf O E2172.16.1.0/0 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1

Common Errors

- If the cost of an interface is set to 0 in the **ip ospf cost** command, a route computation error may occur. For example, a routing loop is obtained.

1.4.8 Enabling Authentication

Configuration Effect

- All routers connected to the OSPF network must be authenticated to ensure stability of OSPF and protect OSPF against intrusions.

Notes

- The OSPF basic functions must be configured.
- If authentication is configured for an area, the configuration takes effect on all interfaces that belong to this area.
- If authentication is configured for both an interface and the area to which the interface belongs, the configuration for the interface takes effect preferentially.

Configuration Steps

↘ Configuring the Authentication Type of an Area

- (Optional) This configuration is recommended if the same authentication type should be used on all interfaces in the same area.
- This configuration is required if a router accesses a network that requires authentication.

↘ Configuring the Authentication Type of an Interface

- (Optional) This configuration is recommended if the different authentication types should be used on different interfaces in the same area.
- This configuration is required if a router accesses a network that requires authentication.

↘ Configuring a Plain Text Authentication Key for an Interface

- Optional.

- This configuration is required if a router accesses a network that requires plain text authentication.

Configuring an MD5 Authentication Key for an Interface

- (Optional) MD5 authentication features a high security, and therefore is recommended. You must configure either plain text authentication or MD5 authentication.
- This configuration is required if a router accesses a network that requires MD5 authentication.

Verification

- If routers are configured with different authentication keys, run the **show ip ospf neighbor** command to verify that there is no OSPF neighbor.
- If routers are configured with the same authentication key, run the **show ip ospf neighbor** command to verify that there are OSPF neighbors.

Related Commands

Configuring the Authentication Type of an Area

Command	**area** *area-id* **authentication** [**message-digest**]
Parameter Description	*area-id*: Indicates the ID of the area where OSPF authentication is enabled. The area ID can be a decimal integer or an IP address. **message-digest**: Enables MD5 authentication.
Command Mode	OSPF routing process configuration mode
Usage Guide	The RGOS supports three authentication types: (1) Type 0: No authentication is required. If this command is not configured to enable OSPF authentication, the authentication type in the OSPF data packet is 0. (2) Type 1: The authentication type is plain text authentication if this command is configured but does not contain the **message-digest** parameter. (3) Type 3: The authentication type is MD5 authentication if this command is configured and contains the **message-digest** parameter. All routers in the same OSPF area must use the same authentication type. If authentication is enabled, the authentication key must be configured on interfaces that are connected to neighbors. You can run the interface configuration command **ip ospf authentication-key** to configure the plain text authentication key, or **ip ospf message-digest-key** to configure the MD5 authentication key.

Configuring the Authentication Type of an Interface

Command	**ip ospf authentication** [**message-digest** | **null**]
Parameter Description	**message-digest**: Indicates that MD5 authentication is enabled on the current interface. **null**: Indicates that authentication is disabled.
Command Mode	Interface configuration mode
Usage Guide	If the **ip ospf authentication** command does not contain any option, it indicates that plain text authentication is enabled. If you use the **no** form of the command to restore the default authentication mode, whether authentication is enabled is determined by the authentication type that is configured in the area to which the interface belongs. If the authentication type is set to null, authentication is disabled forcibly. When

	authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

Configuring a Plain Text Authentication Key for an Interface

Command	**ip ospf authentication-key** [**0** |**7**]*key*
Parameter Description	**0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *key*: Indicates the key. The key is a string of up to eight characters.
Command Mode	Interface configuration mode
Usage Guide	The key configured by the **ip ospf authentication-key** command will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF adjacency and therefore cannot exchange the routing information. Different keys can be configured for different interface, but all routers connected to the same physical network segment must be configured with the same key. You can enable or disable authentication in an OSPF area by running the **areaauthentication** command in OSPF routing process configuration mode. You can also enable authentication on an individual interface by running the **ip ospf authentication** command in interface configuration mode. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially.

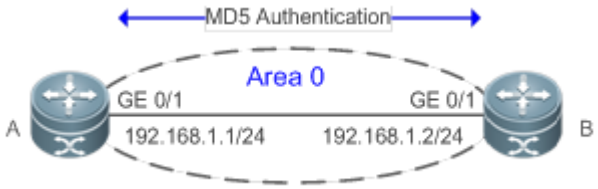
Configuring an MD5 Authentication Key for an Interface

Command	**ip ospf message-digest-key** *key-id* **md5** [**0** |**7**]*key*
Parameter Description	*key-id:* Indicates the key ID. The value ranges from 1 to 255. **0**: Indicates that the key is displayed in plain text. **7**: Indicates that the key is displayed in cipher text. *key:* Indicates the key. The key is a string of up to 16 characters.
Command Mode	Interface configuration mode
Usage Guide	The key configured by the **ip ospf message-digest-key** command will be inserted to the headers of all OSPF packets. If the keys are inconsistent, two directly connected devices cannot set up the OSPF adjacency and therefore cannot exchange the routing information. Different keys can be configured for different interface, but all routers connected to the same physical network segment must be configured with the same key. The same key ID on neighbor routers must correspond to the same key. You can enable or disable authentication in an OSPF area by running the **area authentication** command in OSPF routing process configuration mode. You can also enable authentication on an individual interface by running the **ip ospf authentication** command in interface configuration mode. When authentication is configured for both an interface and the area to which the interface belongs, the authentication type configured for the interface is used preferentially. The RGOS software supports smooth modification of the MD5 authentication key. A new MD5 authentication key must be first added before the old key can be deleted. When an OSPF MD5 authentication key is added to a router, the router determines that other routers do not use the new key yet and therefore uses different keys to send multiple OSPF packets until it confirms that the new key has been configured on neighbors.

	After configuring the new key all routers, you can delete the old key.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

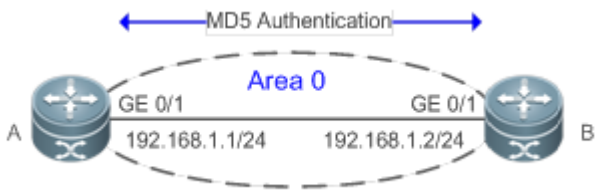
Scenario **Figure 1-16**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the authentication type and MD5 authentication key on all routers.

A	`A# configure terminal`
	`A(config)#router ospf 1`
	`A(config-router)#area 0 authentication message-digest`
	`A(config-router)#exit`
	`A(config)#interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)#ip ospf message-digest-key 1 md5 hello`

B	`B# configure terminal`
	`B(config)#router ospf 1`
	`B(config-router)#area 0 authentication message-digest`
	`B(config-router)#exit`
	`B(config)#interface GigabitEthernet 0/3`
	`B(config-if-GigabitEthernet 0/3)#ip ospf message-digest-key 1 md5 hello`

Verification	On Router A and Router B, verify that the OSPF neighbor status is correct.

A	`A#show ip ospf neighbor`
	`OSPF process 1, 1 Neighbors, 1 is Full:`
	`Neighbor ID Pri State Dead Time Address Interface`
	`192.168.1.2 1 Full/DR 00:00:32 192.168.1.2 GigabitEthernet 0/1`

Scenario **Figure 1-16**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the authentication type and MD5 authentication key on all routers.

A	`A# configure terminal`
	`A(config)#router ospf 1`
	`A(config-router)#area 0 authentication message-digest`
	`A(config-router)#exit`
	`A(config)#interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)#ip ospf message-digest-key 1 md5 hello`

B	`B# configure terminal`
	`B(config)#router ospf 1`
	`B(config-router)#area 0 authentication message-digest`
	`B(config-router)#exit`
	`B(config)#interface GigabitEthernet 0/3`
	`B(config-if-GigabitEthernet 0/3)#ip ospf message-digest-key 1 md5 hello`

Verification	On Router A and Router B, verify that the OSPF neighbor status is correct.

B	`A#show ip ospf neighbor`
	`OSPF process 1, 1 Neighbors, 1 is Full:`
	`Neighbor ID Pri State Dead Time Address Interface`
	`192.168.1.1 1 Full/DR 00:00:32 192.168.1.1 GigabitEthernet 0/1`

Common Errors

- The authentication modes configured on routers are inconsistent.
- The authentication keys configured on routers are inconsistent.

1.4.9 Enabling Overflow

Configuration Effect

- New routes are not loaded to routers when the router memory is insufficient.
- New routes are not loaded to routers when the usage of the database space reaches the upper limit.

Notes

- The OSPF basic functions must be configured.
- After a router enters the overflow state, you can run the **clear ip ospf process** command, or stop and then restart the OSPF to exit the overflow state.

Configuration Steps

Configuring the Memory Overflow Function

- Optional.
- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

Configuring the Database Overflow Function

- Optional.
- This configuration is recommended if a large number of routes exist in the domain and may cause insufficiency of the router memory.

Configuring the External LSA Database Overflow Function

- Optional.
- This configuration is recommended if the ASBR introduces a large number of external routes and the router memory may be insufficient.

Verification

- After the memory becomes insufficient, add new routers to the network, and run the **show ip route** command to verify that new routes are not loaded.
- After the usage of the database space reaches the upper limit, add new routers to the network, and run the **show ip route** command to verify that new routes are not loaded.

Related Commands

Configuring the Memory Overflow Function

Command	**overflow memory-lack**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	The OSPF process enters the overflow state to discard newly-learned external routes. This behavior can effectively ensure that the memory usage does not increase. After the overflow function is enabled, the OSPF process enters the overflow state and discards newly-learned external routes, which may cause a routing loop on the entire network. To reduce the

	occurrence probability of this problem, OSPF generates a default route to the null interface, and this route always exists in the overflow state. You can run the **clear ip ospf process** command to reset the OSPF process so that the OSPF process can exit the overflow state. You can use the **no** form of the command to prevent the OSPF process from entering the overflow state when the memory is insufficient. This, however, may lead to over-consumption of the memory resource, after which the OSPF process will stop and delete all the learned routes.

Configuring the Database Overflow Function

Command	**overflow database** *number* [**hard | soft**]
Parameter Description	*number*: Indicates the maximum number of LSAs. The value ranges from 1 to 4,294,967,294. **hard**: Indicates that the OSPF process will be stopped if the number of LSAs exceeds the limit. **soft:** Indicates that a warning will be generated if the number of LSAs exceeds the limit.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs exceeds the limit, use the **hard** parameter if the OSPF process should be stopped, and use the **soft** parameter if a warning should be generated without stopping the OSPF process.

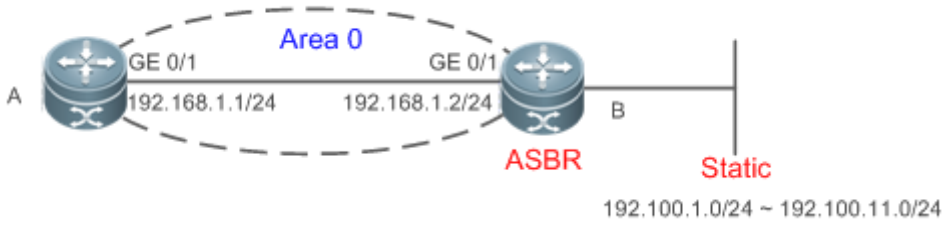
Configuring the External LSA Database Overflow Function

Command	**overflow database external** *max-dbsize wait-time*
Parameter Description	*max-dbsize*: Indicates the maximum number of external LSAs. This value must be the same on all routers in the same AS. The value ranges from 0 to 2,147,483,647. *wait-time*: Indicates the waiting time after a router in overflow state attempts to restore the normal state. The value ranges from 0 to 2,147,483,647.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the number of external LSAs of a router exceeds the configured **max-dbsize**, the router enters the overflow state. In this state, the router no longer loads external LSAs and deletes external LSAs that are generated locally. After *wait-time* elapses, the device restores the normal state, and loads external LSAs again. When using the overflow function, ensure that the same **max-dbsize** is configured on all routers in the OSPF backbone area and common areas; otherwise, the following problems may occur: Inconsistent LSDBs throughout network are inconsistent, and the failure to achieve the full adjacency Incorrect routes, including routing loops Frequent retransmission of AS external LSAs

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Configuring the External LSA Database Overflow Function

Scenario **Figure 1-17**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router B, configure redistribution and introduce external static routes. ● On Router B, configure the maximum number of external LSAs.

B	`B# configure terminal`
	`B(config)# router ospf 1`
	`B(config-router)# redistribute static subnets`

A	`A# configure terminal`
	`A(config)# router ospf 1`
	`A(config-router)# overflow database external 10 3`

Verification	On Router B, configure 11 static routes (192.100.1.0/24 to 192.100.11.0/24). On Router A, verify that only 10 static routes are loaded.

A	`A# show ip route ospf`
	`O E2 192.100.1.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.2.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.3.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.4.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.5.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.6.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.7.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.8.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.9.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`
	`O E2 192.100.10.0/24 [110/20] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1`

Common Errors

- The OSPF adjacency is abnormal because the maximum number of LSAs is inconsistent on different routers.

1.4.10 Modifying the Maximum Number of Concurrent Neighbors

Configuration Effect

- Control the maximum number of concurrent neighbors on the OSPF process to ease the pressure on the device.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

↘ Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

- (Optional) This configuration is recommended if you wish to set up the OSPF adjacency more quickly when a router is connected with a lot of other routers.
- This configuration is performed on a core router.

Verification

- Run the **show ip ospf neighbor** command to display the number of neighbors that are concurrently interacting with the OSPF process.

Related Commands

↘ Configuring the Maximum Number of Concurrent Neighbors on the Current Process

Command	**max-concurrent-dd** *number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	OSPF routing process configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which one OSPF process can concurrently initiates or accepts interaction.

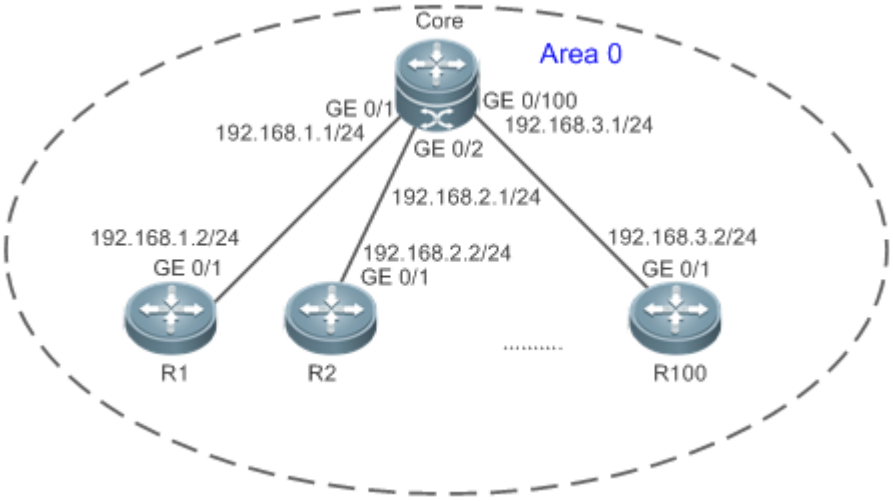
↘ Configuring the Maximum Number of Concurrent Neighbors on All Processes

Command	**router ospf max-concurrent-dd** *number*
Parameter Description	*number:* Specifies the maximum number of neighbors that are concurrently interacting with the OSPF process. The value ranges from 1 to 65,535.
Command Mode	Global configuration mode
Usage Guide	When the performance of a router is affected because the router exchanges data with multiple neighbors, you can configure this command to restrict the maximum of neighbors with which all OSPF processes can concurrently initiate or accept interaction.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Configuring the Maximum Number of Concurrent Neighbors on the OSPF Process

Scenario **Figure 1-18**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On the router Core, set the maximum number of concurrent neighbors to 4.
Core	`Core# configure terminal` `Core(config)# router ospf max-concurrent-dd 4`
Verification	On the router Core, check the neighbor status and verify that at most eight neighbors concurrently interact with the OSPF process.

1.4.11 Disabling Source Address Verification

Configuration Effect

- The unicast routing service can be provided even if the interface IP addresses of neighbor routers are not in the same network segment.

Notes

- The OSPF basic functions must be configured.
- Source address verification cannot be disabled on a broadcast or NBMA network.

Configuration Steps

Disabling Source Address Verification

- (Optional) This configuration is mandatory if an adjacency should be set up between routers with interface IP addresses in different network segments.
- This configuration is performed on routers with interface IP addresses in different network segments.

Verification

- An adjacency can be set up between routers in different network segments.

Related Commands

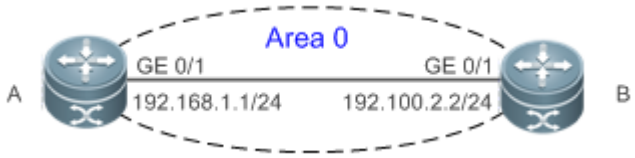
Disabling Source Address Verification

Command	ip ospf source-check-ignore
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	Generally, the source address of a packet received by OSPF is in the same network segment as the receiving interface. The addresses at both ends of a P2P link are configured separately and are not necessarily in the same network segment. In this scenario, as the peer address information will be notified during the P2P link negotiation process, OSPF checks whether the source address of the packet is the address advertised by the peer during negotiation. If not, OSPF determines that the packet is invalid and discards this packet. In some scenarios, the source address may not meet the preceding requirement, and therefore OSPF address verification fails. For example, the negotiated peer address cannot be obtained on a P2P link. In this scenario, source address verification must be disabled to ensure that the OSPF adjacency can be properly set up.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Disabling Source Address Verification

Scenario	
Figure 1-19	
Configuration Steps	• Configure the interface IP addresses on all routers. (Omitted) • Configure the OSPF basic functions on all routers. (Omitted) • Set the network types of interfaces on all routers to P2P. • Disable source address verification on all routers.

A	A# configure terminal A(config)# interface GigabitEthernet 0/1 A(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point A(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
B	B# configure terminal B(config)# interface GigabitEthernet 0/1 B(config-if-GigabitEthernet 0/1)# ip ospf network point-to-point B(config-if-GigabitEthernet 0/1)# ip ospf source-check-ignore
Verification	On Router A, verify that the OSPF neighbor information is correct.
A	A# show ip ospfneighbor OSPF process 1, 1 Neighbors, 1 is Full: Neighbor ID Pri State Dead Time Address Interface 192.100.2.2 1 Full/- 00:00:34 192.100.2.2 GigabitEthernet 0/1

1.4.12 Disabling MTU Verification

Configuration Effect

- The unicast routing service can be provided even if the MTUs of interfaces on neighbor routers are different.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Disabling MTU Verification

- (Optional) MTU verification is disabled by default. You are advised to retain the default configuration.
- This configuration is performed on two routers with different interface MTUs.

Verification

The adjacency can be set up between routers with different MTUs.

Related Commands

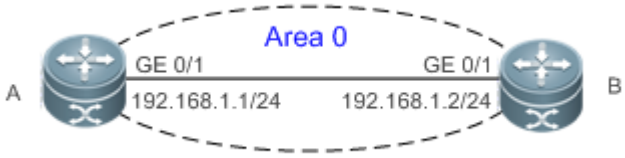
Disabling MTU Verification

Command	**ip ospf mtu-ignore**
Parameter Description	N/A
Command	Interface configuration mode

Mode	
Usage Guide	On receiving the database description packet, OSPF checks whether the MTU of the interface on the neighbor is the same as the MTU of its own interface. If the interface MTU specified in the received database description packet is greater than the MTU of the local interface, the adjacency cannot be set up. To resolve this problem, you can disable MTU verification.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Scenario Figure 1-20	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure different MTUs for interfaces on two routers. ● Disable MTU verification on all routers. (By default, the function of disabling MTU verification is enabled.)

A	`A# configure terminal`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ip mtu 1400`
	`A(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore`

B	`B# configure terminal`
	`B(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ip mtu 1600`
	`B(config-if-GigabitEthernet 0/1)# ip ospf mtu-ignore`

Verification	● On Router A, verify that the OSPF neighbor information is correct.

A	`A# show ip ospfneighbor`
	`OSPF process 1, 1 Neighbors, 1 is Full:`
	`Neighbor ID Pri State Dead Time Address Interface`
	`192.168.1.2 1 Full/DR 00:00:34 192.168.1.2 GigabitEthernet 0/1`

1.4.13 Enabling Two-Way Maintenance

Configuration Effect

- Non-Hello packets can also be used to maintain the adjacency.

Notes

- The OSPF basic functions must be configured.

Configuration Steps

Enabling Two-Way Maintenance

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

Non-Hello packets can also be used to maintain the adjacency.

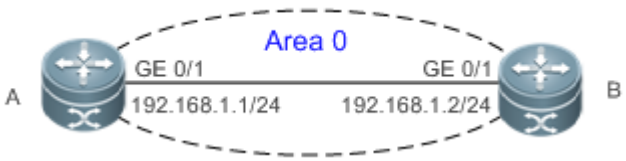
Related Commands

Enabling Two-Way Maintenance

Command	two-way-maintain
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	On a large network, a lot of packets may be sent or received, occupying too much CPU and memory. As a result, some packets are delayed or discarded. If the processing time of Hello packets exceeds the dead interval, the adjacency will be destroyed due to timeout. If the two-way maintenance function is enabled, in addition to the Hello packets, the DD, LSU, LSR, and LSAck packets can also be used to maintain the bidirectional communication between neighbors when a large number of packets exist on the network. This prevents termination of the adjacency caused by delayed or discarded Hello packets.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Scenario Figure 1-21	

Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, enable the two-way maintenance function. (This function is enabled by default.)

A	`A# configure terminal`
	`A(config)#routerospf 1`
	`A(config-router)#two-way-maintain`

Verification	When the adjacency is being set up, Router A checks the neighbor dead interval and updates the dead interval without waiting for Router B to send a Hello packet.

A	`A# show ip ospfneighbor`
	`OSPF process 1, 1 Neighbors, 1 is Full:`
	`Neighbor ID Pri State Dead Time Address Interface`
	`192.168.1.2 1 Full/BDR 00:00:40 192.168.1.2 GigabitEthernet 0/1`

1.4.14 Enabling GR

Configuration Effect

- When a distributed router switches services from the active board to the standby board, data forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Notes

- The OSPF basic functions must be configured.
- The neighbor router must support the GR helper function.
- The grace period cannot be shorter than the neighbor dead time of the neighbor router.

Configuration Steps

↘ Enabling Opaque LSA Processing Capability

- This function is enabled by default. You are advised to retain the default configuration..
- This configuration is performed on all routers..

↘ Configuring the OSPF GR Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

↘ Configuring the OSPF GR Helper Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration.
- This configuration is performed on all routers.

Verification

- When a distributed router switches services from the active board to the standby board, data forwarding continues and is not interrupted.
- When the OSPF process is being restarted, data forwarding continues and is not interrupted.

Related Commands

Enabling Opaque LSA Processing Capability

Command	**capability opaque**
Parameter Description	-
Command Mode	OSPF routing process configuration mode
Usage Guide	Opaque LSA processing capability is supported by default.

Configuring the OSPF GR Function

Command	**graceful-restart** [**grace-period** *grace-period* | **inconsistent-lsa-checking**]
Parameter Description	**grace-period** *grace-period*: Indicates the grace period, which is the maximum time from occurrence of an OSPF failure to completion of the OSPF GR. The value of the grace period varies from 1s to 1800s. The default value is 120s. **inconsistent-lsa-checking**: Enables topological change detection. If any topological change is detected, OSPF exits the GR process to complete convergence. After GR is enabled, topological change detection is enabled by default.
Command Mode	OSPF routing process configuration mode
Usage Guide	The GR function is configured based on the OSPF process. You can configure different parameters for different OSPF processes based on the actual conditions. This command is used to configure the GR restarter capability of a device. The grace period is the maximum time of the entire GR process, during which link status is rebuilt so that the original state of the OSPF process is restored. After the grace period expires, OSPF exits the GR state and performs common OSPF operations. Run the **graceful-restart** command to set the grace period to 120s. The **graceful-restart grace-period** command allows you to modify the grace period explicitly. The precondition for successful execution of GR and uninterrupted forwarding is that the topology remains stable. If the topology changes, OSPF quickly converges without waiting for further execution of GR, thus avoiding long-time forwarding black-hole. Disabling topology detection: If OSPF cannot converge in time when the topology changes during the hot standby process, forwarding black-hole may appear in a long time. Enabling topology detection: Forwarding may be interrupted when topology detection is enabled, but the interruption time is far shorter than that when topology detection is disabled. In most cases, it is recommended that topology detection be enabled. In special scenarios, topology detection can be disabled if the topology changes after the hot standby process, but it can be ensured that

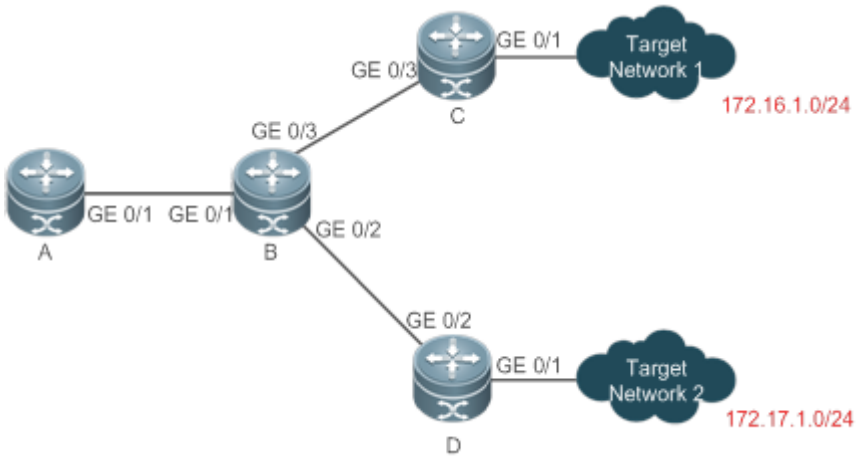
	the forwarding black-hole will not appear in a long time. This can minimize the forwarding interruption time during the hot standby process. Under the Fast Hello function, graceful restart is not supported.

Configuring the OSPF GR Helper Function

Command	**graceful-restart helper** { **disable | strict-lsa-checking | internal-lsa-checking**}
Parameter Description	**disable**: Prohibits a device from acting as a GR helper for another device. **strict-lsa-checking**: Indicates that changes in Type 1 to Type 5 and Type 7 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper. **internal-lsa-checking:** Indicates that changes in Type 1 to Type 3 LSAs will be checked during the period that the device acts as a GR helper to determine whether the network changes. If the network changes, the device will stop acting as the GR helper.
Command Mode	OSPF routing process configuration mode
Usage Guide	This command is used to configure the GR helper capability of a router. When a neighbor router implements GR, it sends a Grace-LSA to notify all neighbor routers. If the GR helper function is enabled on the local router, the local router becomes the GR helper on receiving the Grace-LSA, and helps the neighbor to complete GR. The **disable** option indicates that GR helper is not provided for any device that implements GR. After a device becomes the GR helper, the network changes are not detected by default. If any change takes place on the network, the network topology converges after GR is completed. If you wish that network changes can be quickly detected during the GR process, you can configure **strict-lsa-checking** to check Type 1 to 5 and Type 7 LSAs that indicate the network information or **internal-lsa-checking** to check Type 1 to 3 LSAs that indicate internal routes of the AS domain. When the network scale is large, it is recommended that you disable the LSA checking options (**strict-lsa-checking** and **internal-lsa-checking**) because regional network changes may trigger termination of GR and consequently reduce the convergence of the entire network.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Scenario **Figure 1-22**	 **Remarks**: The interface IP addresses are as follows: A: GE 0/1 192.168.1.1 B: GE 0/1 192.168.1.1 GE 0/2 192.168.2.1 GE 0/3 192.168.3.1 C: GE 0/1 192.168.4.2 GE 0/3 192.168.3.2 D: GE 0/1 192.168.5.2 GE 0/2 192.168.2.2
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● On Router A, Router C, and Router D, enable the GR helper function. (This function is enabled by default.) ● On Router B, enable the GR function.

B	`B# configure terminal`
	`B(config)# router ospf1`
	`B(config-router)# graceful-restart`

Verification	● Trigger a hot standby switchover on Router B, and verify that the routing tables of destination networks 1 and 2 remain unchanged on Router A during the switchover. ● Trigger a hot standby switchover on Router B, ping destination network 1 from Router A, and verify that data forwarding is not interrupted during the switchover.

Common Errors

- Traffic forwarding is interrupted during the GR process because the configured grace period is shorter than the neighbor dead time of the neighbor router.

1.4.15 Configuring Fast Hello Function

Configuration Effect

- Discovery of OSPF neighbor is accelerated and quick detection of neighbor failure can be realized.

Notes

- The OSPF basic functions must be configured.
- Dead interval must be consistent within the same network segment.
- The **dead-interval minimal hello-multiplier** parameter and the **hello-interval** parameter cannot be configured simultaneously on the interface.

Configuration Steps

↘ Configuring Fast Hello Function

- (Optional) This function is disabled by default.
- Configure it on router interfaces.

Verification

- Run the **show ip ospf interface** command to check the correct number of Hello packets sent per second on the interface and the correct neighbor dead time.

Related Commands

↘ Configuring Fast Hello Function

Command	**ip ospf dead-interval minimal hello-multiplier** *multiplier*
Parameter Description	**minimal**: Enables the Fast Hello function and sets the dead time to 1s. **hello-multiplier** *multiplier*: Indicates the number of Hello packets sent per second in the Fast Hello function. The value ranges from 3 to 20.
Command Mode	OSPF route configuration mode
Usage Guide	Enabling the OSPF Fast Hello function accelerates neighbor discovery and rapid detection of neighbor failures in OSPF. The OSPF Fast Hello function is enabled by specifying the **minimal** and **hello-multiplier** keywords and the *multiplier* parameter. The minimal keyword sets the dead time to 1s, and the hello-multiplier value specifies the number of Hello packets sent per second, reducing the Hello packet interval to less than 1s. When an interface is configured with the Fast Hello function, the Hello interval field of the Hello packets advertised from that interface is set to 0, and the Hello interval field of the Hello packets received from that interface is ignored. The dead interval must always remain consistent within the same network segment regardless of whether Fast Hello is enabled or not. The hello-multiplier value does not need to be the same, as long as at least one Hello packet can be received within the dead interval. The **show ip ospf interface** command can be used to monitor the dead interval and Fast Hello interval configured for interfaces. The **dead-interval minimal hello-multiplier** parameter and the **hello-interval** parameter introduced for Fast Hello function cannot be configured simultaneously. Under the Fast Hello function, graceful restart is not supported.

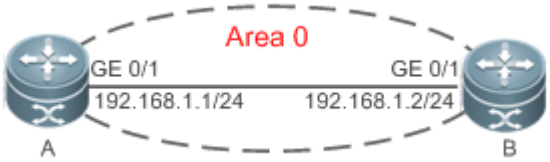
Configuration Example

The following configuration example is performed based on OSPF basic functions. For details about OSPF basic functions, see preceding descriptions.

Configuring Fast Hello Function

Scenario

Figure 1-23



Configuration Steps

- Configure IP addresses on all routers' interfaces. Omitted.
- Configure OSPF basic functions for all routers. Omitted.
- Enable the Fast Hello function on an interface of router A.

A

```
A# configure terminal
A(config)# interface GigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval minimal hello-multiplier
10
```

Verification

Router A checks the interface parameters: The neighbor dead time is 1s, and the sending interval of Hello packets is 100 ms.

A

```
A# show ip ospf interface GigabitEthernet 0/1
GigabitEthernet 0/1 is up, line protocol is up
  Internet Address 192.168.1.1/24, Ifindex 2, Area 0.0.0.0, MTU 1500
  Matching network config: 192.168.1.0/24
  Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1
  Transmit Delay is 1 sec, State Point-To-Point
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 100 msec, Dead 1, Wait 1, Retransmit 5
```

Common Errors

- Configured at the same time as the **ip ospf hello-interval** command.

1.4.16 Configuring the Network Management Function

Configuration Effect

- Use the network management software to manage OSPF parameters and monitor the OSPF running status.

Notes

- The OSPF basic functions must be configured.
- You must enable the MIB function of the SNMP-Server before enabling the OSPF MIB function.
- You must enable the Trap function of the SNMP-Server before enabling the OSPF Trap function.
- You must enable the logging function of the device before outputting the OSPF logs.

Configuration Steps

Binding the MIB with the OSPF Process

- (Optional) This configuration is required if you want to use the network management software to manage parameters of a specified OSPF process.
- This configuration is performed on all routers.

Enabling the Trap Function

- (Optional) This configuration is required if you want to use the network management software to monitor the OSPF running status.
- This configuration is performed on all routers.

Configuring the Logging Function

- (Optional) This function is enabled by default. You are advised to retain the default configuration. If you want to reduce the log output, disable this function.
- This configuration is performed on all routers.

Verification

- Use the network management software to manage the OSPF parameters.
- Use the network management software to monitor the OSPF running status.

Related Commands

Binding the MIB with the OSPF Process

Command	**enable mib-binding**
Parameter Description	N/A
Command Mode	OSPF routing process configuration mode
Usage Guide	The OSPFv2 MIB does not have the OSPFv2 process information. Therefore, you must perform operations on a single OSPFv2 process through SNMP. By default, the OSPFv2 MIB is bound with the OSPFv2 process with the smallest process ID, and all user operations take effect on this process. If you wish to perform operations on a specified OSPFv2 through SNMP, run this command to bind the MIB with the process.

Enabling the Trap Function

Command	**enable traps** [**error** [**IfAuthFailure | IfConfigError | IfRxBadPacket | VirtIfAuthFailure | VirtIfConfigError | VirtIfRxBadPacket**] * | **lsa** [**LsdbApproachOverflow | LsdbOverflow | MaxAgeLsa | OriginateLsa**] * | **retransmit** [**IfTxRetransmit | VirtIfTxRetransmit**] * | **state-change** [**IfStateChange | NbrRestartHelperStatusChange | NbrStateChange | NssaTranslatorStatusChange | RestartStatusChange | VirtIfStateChange | VirtNbrRestartHelperStatusChange | VirtNbrStateChange**] *]
Parameter	**error**: Configures all trap switches related to error. This parameter can also be used to configure the

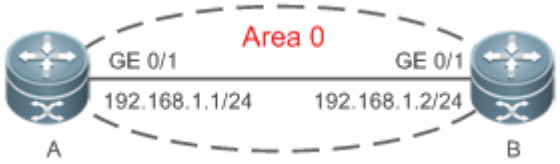
Description	following specific error trap switches: **IfAuthFailure**: Indicates that an interface authentication failure occurs. **IfConfigError:** Indicates that an interface parameter configuration error occurs. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **IfRxBadPacket:** Indicates that the interface receives a bad packet. **VirtIfAuthFailure:** Indicates that a virtual interface authentication failure occurs. **VirtIfConfigError:** Indicates that a virtual interface parameter configuration error occurs. **VirtIfRxBadPacket:** Indicates that the virtual interface receives a bad packet. **lsa**: Configures all trap switches related to LSA. This parameter can also be used to configure the following specific LSA trap switches: **LsdbApproachOverflow:** Indicates that the number of external LSAs has reached 90% of the upper limit. **LsdbOverflow:** Indicates that the number of external LSAs has reached the upper limit. **MaxAgeLsa:** Indicates that the LSA aging timer expires. **OriginateLsa:** Indicates that a new LSA is generated. **retransmit**: Configures all trap switches related to retransmit. This parameter can also be used to configure the following specific retransmit trap switches: **IfTxRetransmit:** Indicates that a packet is retransmitted on the interface. **VirtIfTxRetransmit:** Indicates that a packet is retransmitted on the virtual interface. **state-change**: Configures all trap switches related to state-change. This parameter can also be used to configure the following specific state-change trap switches: **IfStateChange:** Indicates that interface state changes. **NbrRestartHelperStatusChange:** Indicates that the state of the neighbor GR process changes. **NbrStateChange:** Indicates that the neighbor state changes. **NssaTranslatorStatusChange:** Indicates that the NSSA translation state changes. **RestartStatusChange:** Indicates that the GR state of the local device changes. **VirtIfStateChange:** Indicates that the virtual interface state changes. **VirtNbrRestartHelperStatusChange:** Indicates that the GR state of the virtual neighbor changes. **VirtNbrStateChange:** Indicates that the virtual neighbor state changes.
Command Mode	OSPF routing process configuration mode
Usage Guide	The function configured by this command is restricted by the **snmp-server** command. You can configure **snmp-server enable traps ospf** and then **enable traps** command before the corresponding OSPF traps can be correctly sent out. This command is not restricted by the MIB bound with the process. The trap function can be enabled concurrently for different processes.

Configuring the Logging Function

Command	**log-adj-changes**[**detail**]
Parameter Description	**detail**: Records all status change information.
Command Mode	OSPF routing process configuration mode
Usage Guide	N/A

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Scenario **Figure 1-24**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Bind the MIB with the OSPF process on Router A. ● Enable the trap function on Router A.

A	`A# configure terminal`
	`A(config)# snmp-server host 192.168.2.2 traps version 2c public`
	`A(config)# snmp-server community public rw`
	`A(config)# snmp-server enable traps`
	`A(config)# router ospf 10`
	`A(config-router)# enable mib-binding`
	`A(config-router)# enable traps`

Verification	Use the MIB tool to read and set the OSPF parameters and display the OSPF running status.

Common Errors

Configurations on the SNMP-Server are incorrect. For example, the MIB or trap function is not enabled.

1.4.17 Modifying Protocol Control Parameters

Configuration Effect

Modify protocol control parameters to change the protocol running status.

Notes

- The OSPF basic functions must be configured.
- The neighbor dead time cannot be shorter than the Hello interval.

Configuration Steps

Configuring the Hello Interval

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on routers at both end of a link.

Configuring the Dead Interval

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if you wish to accelerate OSPF convergence when a link fails.
- This configuration is performed on routers at both end of a link.

Configuring LSU Retransmission Interval

- (Optional) You are advised to adjust this configuration if a lot of routes exist in the user environment and network congestion is serious.

Configuring the LSA Generation Time

- (Optional) You are advised to retain the default configuration.

Configuring the LSA Group Refresh Time

- (Optional) You are advised to retain the default configuration. This configuration can be adjusted if a lot of routes exist in the user environment.
- This configuration is performed on an ASBR or ABR.

Configuring LSA Repeated Receiving Delay

- (Optional) You are advised to retain the default configuration.

Configuring the SPF Computation Delay

- (Optional) This configuration can be adjusted if network flapping frequently occurs.

Configuring the Inter-Area Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on all routers.

Configuring the External Route Computation Delay

- (Optional) You are advised to retain the default configuration.
- This configuration is performed on all routers.

Configuring Route Computation Suppression Time on an Interface

- (Optional) It is used with **max-metric**.
- Configure it on interfaces.

Verification

Run the **show ip ospf** and **show ip ospf neighbor** commands to display the protocol running parameters and status.

Related Commands

Configuring the Hello Interval

Command	**ip ospf hello-interval** *seconds*
Parameter Description	*seconds*: Indicates the interval at which OSPF sends the Hello packet. The unit is second. The value ranges from 1 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	The Hello interval is contained in the Hello packet. A shorter Hello interval indicates that OSPF can detect topological changes more quickly, but the network traffic increases. The Hello interval must be the same on all routers in the same network segment. If you want to manually modify the neighbor dead interval, ensure that the neighbor dead interval is longer than the Hello interval.

Configuring the Dead Interval

Command	**ip ospf dead-interval** *seconds*
Parameter Description	*seconds*: Indicates the time that the neighbor is declared lost. The unit is second. The value ranges from 0 to 2,147,483,647.
Command Mode	Interface configuration mode
Usage Guide	The OSPF dead interval is contained in the Hello packet. If OSPF does not receive a Hello packet from a neighbor within the dead interval, it declares that the neighbor is invalid and deletes this neighbor record form the neighbor list. By default, the dead interval is four times the Hello interval. If the Hello interval is modified, the dead interval is modified automatically. When using this command to manually modify the dead interval, pay attention to the following issues: 1. The dead interval cannot be shorter than the Hello interval. 2. The dead interval must be the same on all routers in the same network segment.

Configuring the LSU Transmission Delay

Command	**ip ospf transmit-delay** *seconds*
Parameter Description	*seconds*: Indicates the LSU transmission delay on the OSPF interface. The unit is second. The value ranges from 0 to 65,535.
Command Mode	Interface configuration mode
Usage Guide	Before an LSU packet is transmitted, the Age fields in all LSAs in this packet will increase based on the amount specified by the **ip ospf transmit-delay** command. Considering the transmit and line propagation delays on the interface, you need to set the LSU transmission delay to a greater value for a low-speed line or interface. The LSU transmission delay of a virtual link is defined by the **transmit-delay** parameter in the **area virtual-link** command. If the value of the Age field of an LSA reaches 3600, the packet will be retransmitted or a retransmission will be requested. If the LSA is not updated in time, the expired LSA will be deleted from the LSDB.

Configuring LSU Retransmission Interval

Command	**ip ospf retransmit-interval** *seconds*
Parameter Description	*seconds*: Indicates the LSU retransmission interval. The unit is second. The value ranges from 0 to 65,535. This interval must be longer than the round-trip transmission delay of data packets between two neighbors.

Command Mode	Interface configuration mode
Usage Guide	After a router finishes sending an LSU packet, this packet is still kept in the transmit buffer queue. If an acknowledgment from the neighbor is not received within the time defined by the **ip ospf retransmit-interval** command, the router retransmits the LSU packet. The retransmission delay can be set to a greater value on a serial line or virtual link to prevent unnecessary retransmission. The LSU retransmission delay of a virtual link is defined by the **retransmit-interval** parameter in the **area virtual-link** command.

Configuring the LSA Generation Time

Command	**timers throttle lsa all** *delay-time hold-time max-wait-time*
Parameter Description	*delay-time*: Indicates the minimum delay for LSA generation. The first LSA in the database is always generated instantly. The value ranges from 0 to 600,000. The unit is ms. *hold-time*: Indicates the minimum interval between the first LSA update and the second LSA update. The value ranges from 1 to 600,000. The unit is ms. *max-wait-time*: Indicates the maximum interval between two LSA updates when the LSA is updated continuously. This interval is also used to determine whether the LSA is updated continuously. The value ranges from 1 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	If a high convergence requirement is raised when a link changes, you can set **delay-time** to a smaller value. You can also appropriately increase values of the preceding parameters to reduce the CPU usage. When configuring this command, the value of **hold-time** cannot be smaller than the value of **delay-time,** and the value of **max-wait-time** cannot be smaller than the value of **hold-time**.

Configuring the LSA Group Refresh Time

Command	**timers pacing lsa-group** *seconds*
Parameter Description	*seconds*: Indicates the LSA group pacing interval. The value ranges from 10 to 1,800. The unit is second.
Command Mode	OSPF routing process configuration mode
Usage Guide	Every LSA has a time to live (LSA age). When the LSA age reaches 1800s, a refreshment is needed to prevent LSAs from being cleared because their ages reaching the maximum. If LSA update and aging computation are performed for every LSA, the device will consume a lot of CPU resources. In order to use CPU resources effectively, you can refresh LSAs by group on the device. The interval of group refreshment is called group pacing interval. The group refreshment operation is to organize the LSAs generated within a group pacing interval into a group and refresh the group as a whole. If the total number of LSAs does not change, a larger group pacing interval indicates that more LSAs need to be processed after timeout. To maintain the CPU stability, the number of LSAs processes upon each timeout cannot be too large. If the number of LSAs is large, you are advised to reduce the group pacing interval. For example, if there are 1000 LSAs in the database, you can reduce the pacing interval; if there are 40 to 100 LSAs, you can set the pacing interval to 10-20 minutes.

Configuring the LSA Group Refresh Interval

Command	**timers pacing lsa-transmit** *transmit-time transmit-count*
Parameter Description	*transmit-time*: Indicates the LSA group transmission interval. The value ranges from 10 to 1,000. The unit is ms. *transmit-count*: Indicates the number of LS-UPD packets in a group. The value ranges from 1 to 200.
Command Mode	OSPF routing process configuration mode
Usage Guide	If the number of LSAs is large and the device load is heavy in an environment, properly configuring **transimit-time** and **transimit-count** can limit the number of LS-UPD packets flooded on a network. If the CPU usage is not high and the network bandwidth load is not heavy, reducing the value of **transimit-time** and increasing the value of **transimit-count** can accelerate the environment convergence.

Configuring LSA Repeated Receiving Delay

Command	**timers lsa arrival** *arrival-time*
Parameter Description	*arrival-time*: Indicates the delay after which the same LSA is received. The value ranges from 0 to 600,000. The unit is ms.
Command Mode	OSPF routing process configuration mode
Usage Guide	No processing is performed if the same LSA is received within the specified time.

Configuring the Inter-Area Route Computation Delay

Command	**timers throttle route inter-area** *ia-delay*
Parameter Description	*ia-delay*: Indicates the inter-area route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	This delay cannot be modified if strict requirements are raised for the network convergence time.

Configuring the External Route Computation Delay

Command	**timers throttle route ase** *ase-delay*
Parameter Description	*ase-delay*: Indicates the external route computation delay. The unit is ms. The value ranges from 0 to 600,000.
Command Mode	OSPF routing process configuration mode
Usage Guide	This delay cannot be modified if strict requirements are raised for the network convergence time.

Configuring the SPF Computation Delay

Command	**timers spf** *spf-delay spf-holdtime*
Parameter Description	*spf-delay*: Defines the waiting time for the SPF computation, in seconds. The value ranges from 0 to 2,147,483,647. The OSPF routing process must wait for the specified time after receiving a topology change before performing SPF computation. *spf-holdtime*: Defines the time interval between two consecutive SPF computations, in seconds. The value ranges from 0 to 2,147,483,647. The SPF computation cannot be performed until the time interval between two consecutive computations has passed, even if the waiting time has elapsed.
Command	OSPF routing process configuration mode

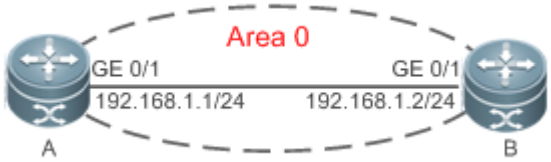
Mode	
Usage Guide	The smaller the spf-delay and spf-holdtime values, the shorter the time OSPF takes to adapt to topology changes, which means faster network convergence, but it also consumes more CPU time on the routing device. The **timers spf** configuration and the **timers throttle spf** configuration will override each other.

Command	**timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*
Parameter Description	*spf-delay*: Indicates the SPF computation delay. The unit is ms. The value ranges from 1 to 600,000. When detecting a topological change, the OSPF routing process triggers the SPF computation at least after **spf-delay** elapses. *spf-holdtime*: Indicates the minimum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *spf-max-waittime*: Indicates the maximum interval between two SPF computations. The unit is ms. The value ranges from 1 to 600,000. *number*: indicates the metric of the summarized route.
Command Mode	OSPF routing process configuration mode
Usage Guide	**spf-delay** indicates the minimum time between the occurrence of the topological change and the start of SPF computation. **spf-holdtime** indicates the minimum interval between the first SPF computation and the second SPF computation. After that, the interval between two SPF computations must be at least twice of the previous interval. When the interval reaches **spf-max-waittime**, the interval cannot increase again. If the interval between two SPF computations already exceeds the required minimum value, the interval is computed by starting from **spf-holdtime**. You can set **spf-dela**y and **spf-holdtime** to smaller values to accelerate topology convergence, and set **spf-max-waittime** to a larger value to reduce SPF computation. Flexible settings can be used based on stability of the network topology. Compared with the **timers spf** command, this command supports more flexible settings to accelerate the convergence speed of SPF computation and further reduce the system resources consumed by SPF computation when the topology continuously changes. Therefore, you are advised to use the **timers throttle spf** command for configuration. 1. The value of **spf-holdtime** cannot be smaller than the value of **spf-delay**; otherwise, **spf-holdtime** will be automatically set to the value of **spf-delay**. 2. The value of **spf-max-waittime** cannot be smaller than the value of **spf-holdtime**; otherwise, **spf-max-waittime** will be automatically set to the value of **spf-holdtime**. 3. The configurations of **timers throttle spf** and **timers spf** are mutually overwritten. 4. When both **timers throttle spf** and **timers spf** are not configured, the default values of **timers throttle spf** prevail.

Configuration Example

The following configuration examples assume that the OSPF basic functions have been configured. For details about the OSPF basic functions, see section 1.4.1 "Configuring OSPF Basic Functions."

Configuring the Hello Interval and Dead Interval

Scenario **Figure 1-25**	
Configuration Steps	● Configure the interface IP addresses on all routers. (Omitted) ● Configure the OSPF basic functions on all routers. (Omitted) ● Configure the Hello interval and dead interval on all routers.

A	`A# configure terminal`
	`A(config)# interface GigabitEthernet 0/1`
	`A(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15`
	`A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50`

B	`B# configure terminal`
	`B(config)# interface GigabitEthernet 0/1`
	`B(config-if-GigabitEthernet 0/1)# ip ospf hello-interval 15`
	`A(config-if-GigabitEthernet 0/1)# ip ospf dead-interval 50`

Verification	Check the interface parameters on Router A. Verify that the Hello interval is 10s and the dead interval is 50s.

A	`A# show ip ospf interface`
	`GigabitEthernet 0/1 is up, line protocol is up`
	`  Internet Address 192.168.1.1/24, Ifindex 2, Area 0.0.0.0, MTU 1500`
	`  Matching network config: 192.168.1.0/24`
	`  Process ID 1, Router ID 192.168.1.2, Network Type POINTOMULTIPOINT, Cost: 1`
	`  Transmit Delay is 1 sec, State Point-To-Point`
	`  Timer intervals configured, Hello 15, Dead 50, Wait 40, Retransmit 5`
	`    Hello due in 00:00:02`
	`  Neighbor Count is 1, Adjacent neighbor count is 0`
	`  Crypt Sequence Number is 4787`
	`  Hello received 465 sent 466, DD received 8 sent 8`
	`  LS-Req received 2 sent 2, LS-Upd received 8 sent 21`
	`  LS-Ack received 14 sent 7, Discarded 3`

Common Errors

- The configured neighbor dead time is shorter than the Hello interval.

1.5 Monitoring

Clearing

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

Description	Command
Clears and resets an OSPF process.	**clear ip ospf** [*process-id*] **process**

Displaying

Description	Command
Displays the OSPF process configurations.	**show ip ospf** [*process-id*]
Displays the OSPF internal routing table, including routes to ABRs and ASBRs.	**show ip ospf**[*process-id*] **border-routers**
Displays information about the OSPF LSDB.	**show ip ospf** [*process-id* [*area-id* | *ipv4-address*]] **database** [{ **asbr-summary** | **external** | **network** | **nssa-external** | **opaque-area** | **opaque-as** | **opaque-link** | **router** | **summary** }] [{ **adv-router** *ipv4-address* | **self-originate** } | *link-state-id* | **brief**] [**database-summary** | **max-age** | **detail**]
Displays OSPF-enabled interfaces.	**show ip ospf** [*process-id*] **interface** [*interface-type interface-number* | **brief**]
Displays the OSPF neighbor list.	**show ip ospf** [*process-id*] **neighbor** [**statistics** | [*interface-type interface-number* | *neighbor-id* | **detail**] *]
Displays the OSPF routing table.	**show ip ospf** [*process-id*] **route**[**count |** *ipv4-address mask*]
Displays the number of times SPT is computed in the OSPF area.	**show ip ospf** [*process-id*] **spf**
Displays the summarized route of OSPF redistributed routes.	**show ip ospf**[*process-id*] **summary-address**
Displays OSPF virtual links.	**show ip ospf** [*process-id*] **virtual-links** [*ipv4-address*]

Debugging

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

Description	Command
Debugs OSPF events.	**debug ip ospf events** [**abr**|**asbr**|**lsa**|**nssa**|**os**|**restart**| **router**|**slink**| **vlink**]
Debugs OSPF interfaces.	**debug ip ospf ifsm** [**events**|**status**|**timers**]
Debugs OSPF neighbors.	**debug ip ospf nfsm** [**events** | **status** | **timers**]
Debugs the OSPF NSM.	**debug ip ospf nsm** [**interface** | **redistribute** | **route**]
Debugs OSPF LSAs.	**debug ip ospf lsa** [**flooding** | **generate** | **install** | **maxage** | **refresh**]
Debugs OSPF packets.	**debug ip ospf packet** [**dd**|**detail**|**hello**|**ls-ack**|**ls-request**|**ls-update**|**recv**|**send**]
Debugs OSPF routes.	**debug ip ospf route** [**ase** | **ia** | **install** | **spf** | **time**]

1 Configuring Routing Policies

1.1 Overview

Routing policies are used to modify packet forwarding path or routing information and are typically implemented through filtering lists and route maps. They are flexibly and widely applied in various ways, including:

- Use a filtering list in a routing protocol to filter or modify routing information.
- Use a route map in a routing protocol to filter or modify routing information. The route map can reference a filtering list.
- Use a route map in Policy-based Routing (PBR) to control packet forwarding or modify packet fields.

1.2 Applications

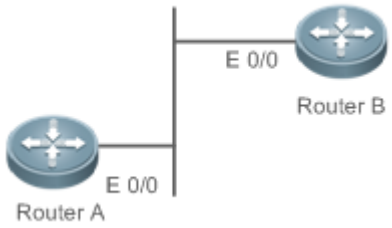
Application	Description
Route Filtering	Use a filtering list in a routing protocol to filter routing information sent or received by this protocol.
Route Redistribution	Use a route map in a routing protocol to filter or modify routing information and redistribute RIP routes to OSPF. Only RIP routes with four hops can be redistributed.
PBR	Use a route map in PBR to control packet forwarding or modify packet fields and specify optimal outbound interfaces for packets from different subnets.

1.2.1 Route Filtering

By default, a routing protocol advertises and learns all routing information. When a filtering list is used, the routing protocol advertises only required routes or receives only required routing information.

Scenario

Figure 1-1



As shown in Figure 1-1, Router A has routes to three networks: 10.0.0.0, 20.0.0.0, and 30.0.0.0.

Configure a filtering list on the routers to achieve the following purposes:

- Filter the sent routing information on Router A to filter routes that Router A does not need to send.
- Filter the received routing information on Router B to filter routes that Router B does not need to learn.

Deployment

- Filter the sent routing information 30.0.0.0 on Router A.
- Filter the received routing information 20.0.0.0 on Router B to ensure that Router B learns only routing information 10.0.0.0.

1.2.2 Route Redistribution

By default, route redistribution allows the device to redistribute all routing information in a routing protocol to another routing protocol. All routing attributes will also be inherited. You can use a route map to control redistribution of specific routing information between two routing protocols, including:

- Specify the route redistribution range and redistribute only routing information that meets certain rules.
- Set attributes of routes to be redistributed.

Scenario

Figure 1-2



As shown in Figure 1-2, configure route redistribution on the devices to achieve the following purposes:

- Redistribute only RIP routes with four hops to OSPF.
- In the OSPF routing domain, the initial metric of this route is 40, the route type is Type-1 external route and the route tag value is set to 40.

Deployment

- In the route map **rip_to_ospf**, match a route with four hops, and set the initial metric of this route to 40, the route type to Type-1 external route and the route tag value to 40.
- Configure route redistribution to enable the device to redistribute RIP routes to OSPF by referencing the route map **rip_to_ospf**.

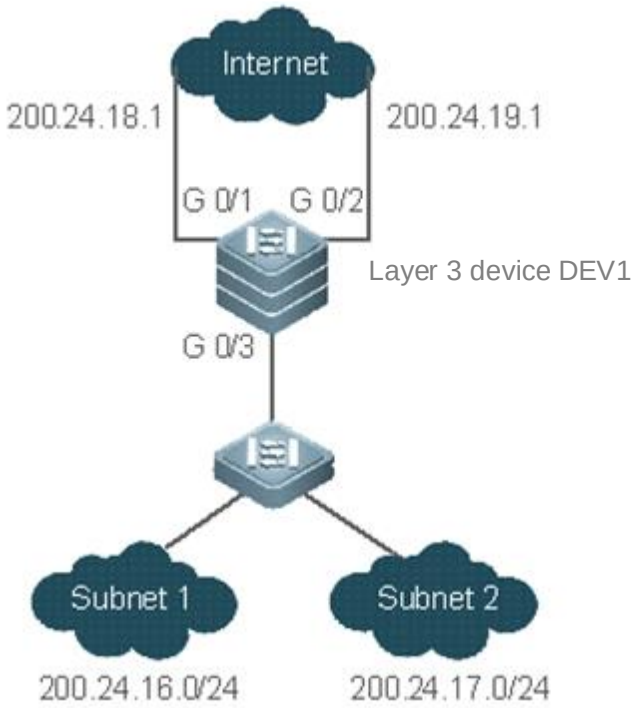
1.2.3 PBR

PBR is implemented by applying a route map including policies to interfaces and devices.

Similar to static routing, PBR is also manually configured. Recursive routes can also be automatically updated with network changes. Compared with static and dynamic routing, PBR is more flexible. Static and dynamic routing can be used to forward packets only based on destination addresses. PBR can forward packets based on the source and destination addresses, packet length, and inbound interface.

Scenario

Figure 1-3



Configure PBR on the Layer 3 device DEV1 to achieve the following purposes:

- Packets from subnet 1 (200.24.16.0/24) are sent from GE0/1 first.
- Packets from subnet 2 (200.24.17.0/24) are sent from GE0/2 first.

Deployment

- Configure two different access control lists (ACLs) to match packets from subnets 1 and 2 respectively.
- Configure the route map **RM_FOR_PBR**: policy 10 is used to ensure that packets from subnet 1 are sent from GE0/1 first; policy 20 is used to ensure that packets from subnet 2 are sent from GE0/2 first.
- Perform PBR for packets received from GE0/3 and reference the route map **RM_FOR_PBR**.

1.3 Features

Overview

Feature	Description
Filtering List	Defines a group of lists based on route attributes, which can be used by a routing protocol for route filtering.
Route Map	Takes actions when conditions are met.

1.3.1 Filtering List

Filtering lists are a group of lists defined based on route attributes for filtering routing policies. Independent filtering lists are invalid and can be used to filter routes only when being applied to routing protocols.

Working Principle

Based on different route attributes, filtering lists are classified into the following types.

ACL

ACLs comprise IPv4 and IPv6 ACLs. When defining ACLs, you can specify IPv4/IPv6 addresses and masks to match the destination network segment or next-hop addresses of routing information.

For description about ACLs, see *Configuring ACL*.

Address Prefix List

Similar to ACLs, address prefix lists (prefix-lists), including IPv4 and IPv6 prefix-lists, are used to match destination network segments of routing information during route filtering.

Related Configuration

Creating an ACL

By default, no ACL is configured and no policy is set.

In global configuration mode, run the **ip access-list** { **extended** | **standard** } { *id* | *name* } command to create an IPv4 ACL.

You can set multiple policies in an ACL, which are sorted by sequence number. Policies have two working modes: permit and deny.

Creating a Prefix-List

By default, no prefix-list is configured and no entry is set.

In global configuration mode, run the **ip prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*] command to create an IPv4 prefix-list and add a prefix entry to the list.

You can set multiple entries in the prefix-list, which are sorted by sequence number. Entries have two working modes: permit and deny.

Run the **ip prefix-list** *prefix-list-name* **description** *description-text* command to add the description to the prefix-list.

Run the **ip prefix-list sequence-number** command to enable the sorting function for the prefix-list.

1.3.2 Route Map

A route map uses the "match …, set…" statement, indicating that processing actions are taken if certain conditions are met.

Working Principle

Enforcing Policies

A route map may contain multiple policies, which are identified by sequence number. A smaller sequence number means a higher priority. Policies are executed based on their sequence numbers. Once the matching condition of a policy is met, the processing action for this policy needs to be taken and the route map exits. If no matching condition of any policy is met, no processing action will be taken.

Working Modes of Policies

Policies have two working modes:

- permit: When the matching condition of a policy is met, the processing action for this policy will be performed and the route map will exit.
- deny: When the matching condition of a policy is met, the processing action for this policy will not be performed and the route map will exit.

Matching Conditions of Policies

The matching condition of a policy may contain no match rule, one match rule, or more match rules.

- If the matching condition contains no match rule, packets are matched.
- If the matching condition contains one or more match rules, packets must match all rules.

Processing Action for a Policy

The processing action of a policy may contain no set rule, one set rule, or more set rules.

- If the processing action contains no set rule, no processing action will be performed and the route map will directly exit.
- If the processing action contains one or more set rules, all processing actions will be performed and then the route map will exit.

⚠ If set rules have different priorities, the set rule with the highest priority will take effect.

Related Configuration

Creating a Route Map (Policy)

By default, no route map is configured and no policy is set.

In global configuration mode, you can run the **route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*] command to create a route map and add a policy to the route map.

You can set multiple policies in a route map. Each policy uses different sequence numbers.

Setting Matching Conditions of a Policy

By default, no match rule is set (that is, the matching condition of a policy contains no match rule).

In route map mode, run the **match** command to set match rules. One **match** command is mapped to one match rule.

RGOS provides abundant **match** commands for setting flexible matching conditions.

Command	Description
match interface	Uses the outbound interface of a route as the matching condition.
match ip address	Uses the destination IPv4 address of a route as the matching condition.
match ip next-hop	Uses the next-hop IPv4 address of a route as the matching condition.
match ip route-source	Uses the source IPv4 address of a route as the matching condition.
match ipv6 address	Uses the destination IPv6 address of a route as the matching condition.
match ipv6 next-hop	Uses the next-hop IPv6 address of a route as the matching condition.
match ipv6 route-source	Uses the source IPv6 address of a route as the matching condition.

Command	Description
match mac-address	Uses the MAC address of a route as the matching condition.
match metric	Uses the metric of a route as the matching condition.
match route-type	Uses the type of a route as the matching condition.
match tag	Uses the tag value of a route as the matching condition.

Setting the Processing Actions of a Policy

By default, no set rule is configured (that is, the processing action of a policy contains no set rule).

In the route map mode, run the **set** command to configure set rules. One **set** command is mapped to one set rule.

RGOS provides abundant **set** commands for setting flexible processing actions.

Command	Description
set level	Sets the destination area type to which a route will be directed.
set metric	Changes the metric value of a route.
set metric-type	Sets the metric type of a route.
set next-hop	Sets the next-hop IP address of a route.
set tag	Sets the tag value of a route.

1.4 Configuration

Configuration	Description and Command	
Configuring a Route Map	(Optional) It is used to define a policy.	
	route-map	Creates a policy (route map).
	match	Sets matching conditions of the policy.
	set	Sets processing actions of the policy.
Configuring a Filtering List	(Optional) It is used to define a filtering list.	
	ip prefix-list	Creates a prefix-list.
	ip prefix-list description	Adds the description to a prefix-list.
	ip prefix-list sequence-number	Enables the sorting function for a prefix-list.
	ipv6 prefix-list	Creates an IPv6 prefix-list.
	ipv6 prefix-list description	Adds the description to an IPv6 prefix-list.
	ipv6 prefix-list sequence-number	Enables the sorting function for an IPv6 prefix-list.
Configuring the Exit Policy for Routing Protocols	**memory-lack exit-policy**	Specifies the exit policy for upper-layer routing protocols after the memory reaches the lower threshold.

1.4.1 Configuring a Route Map

Configuration Effect

- Define a set of routing policies to be used by routing protocols or PBR.

Notes

- If the **match** command uses an ACL to define matching conditions of packets, the ACL must have been configured.
- The following **match** commands in the left and right columns cannot be configured simultaneously.

Command	Conflicting Command
match ipv6 address	**match ipv6 prefix-list**
match ip next-hop	**match ip next-hop prefix-list**
match ipv6 next-hop	**match ipv6 next-hop prefix-list**
match ip route-source	**match ip route-source prefix-list**
match ipv6 route-source	**match ipv6 route-source prefix-list**

Configuration Step

Creating a Policy (Route Map)

- Mandatory.
- Perform this configuration on a device to which a policy needs to be applied.

Setting Matching Conditions of a Policy

- Optional.
- If no match rule is configured, packets are matched.
- If multiple match rules are configured, packets must match all the match rules.
- Perform this configuration on a device to which a policy needs to be applied.

Setting Processing Actions of a Policy

- Optional.
- If no set rule is configured, no processing action will be performed.
- If multiple set rules are configured, all set rules must be executed (if the set rules have different priorities, the set rule with the highest priority takes effect).
- Perform this configuration on a device to which a policy needs to be applied.

Verification

- Check the route map configuration.

Related Commands

Creating a Policy (Route Map)

Command	**route-map** *route-map-name* [{ **permit** | **deny** } *sequence*]
Parameter Description	*route-map-name*: Indicates the name of a route map. It has no more than 32 characters (limited to 200 characters in some versions). permit: Specifies the working mode of this policy as permit, which is the default mode. deny: Specifies the working mode of this policy as deny.

	sequence: Specifies the sequence number of this policy. A smaller value means a higher priority. The default value is 10.
Command Mode	Global configuration mode
Usage Guide	If this route map is unavailable, this command will create a route map and add a policy to the route map. If this route map is available, this command will add a policy to the route map.

Setting Matching Conditions of a Policy

Command	**match interface** *interface-type interface-number* [*…interface-type interface-number*]
Parameter Description	*interface-type interface-number*: Indicates the interface type and interface number.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the next-hop outbound interface of a route or a packet.

Command	**match ip address** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...*| *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }
Parameter Description	*access-list-number*: Indicates the number of an ACL. For a standard ACL, the value range is from 1 to 99 and 1300 to 1999. For an extended ACL, the value range is from 100 to 199 and 2000 to 2699. For an expert-level extended ACL, the value range is from 2700 to 2899. *access-list-name*: Indicates the name of an ACL. **prefix-list** *prefix-list-name*: Indicates the name of a prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the destination IPv4 address of a packet or route by using an ACL or a prefix-list.

Command	**match ip next-hop** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name* [*prefix-list-name...*] }
Parameter Description	*access-list-number*: Indicates the number of an ACL. For a standard ACL, the value range is from 1 to 99 and 1300 to 1999. For an extended ACL, the value range is from 100 to 199 and 2000 to 2699. *access-list-name*: Indicates the name of an ACL. **prefix-list** *prefix-list-name*: Indicates the name of a prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the next-hop IPv4 address of a route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured simultaneously.

Command	**match ip route-source** { *access-list-number* [*access-list-number...* | *access-list-name...*] | *access-list-name* [*access-list-number...* | *access-list-name*] | **prefix-list** *prefix-list-name*

	[*prefix-list-name...*] }
Parameter Description	*access-list-number*: Indicates the number of an ACL. For a standard ACL, the value range is from 1 to 99 and 1300 to 1999. For an extended ACL, the value range is from 100 to 199 and 2000 to 2699. *access-list-name*: Indicates the name of an ACL **prefix-list** *prefix-list-name*: Indicates the name of a prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the source IPv4 address of a route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured simultaneously.

Command	**match ipv6 address** { *access-list-name* | **prefix-list** *prefix-list-name* }
Parameter Description	*access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of an IPv6 prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the destination IPv6 address of a packet or route by using an ACL or a prefix-list. An ACL and a prefix list cannot be configured simultaneously.

Command	**match ipv6 next-hop** { *access-list-name* | **prefix-list** *prefix-list-name* }
Parameter Description	*access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of an IPv6 prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the next-hop IPv6 address of a route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured simultaneously.

Command	**match ipv6 route-source** { *access-list-name* | **prefix-list** *prefix-list-name* }
Parameter Description	*access-list-name*: Indicates the access list name. **prefix-list** *prefix-list-name*: Indicates the name of an IPv6 prefix-list to be matched.
Command Mode	Route map configuration mode
Usage Guide	This match rule matches the source IPv6 address of a route by using an ACL or a prefix-list. An ACL and a prefix-list cannot be configured simultaneously.

Command	**match metric** *metric*
Parameter Description	*metric*: Indicates the metric value of a route. The value range is from 0 to 4294967295.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the metric value of a route.

Command	**match route-type** { **internal | external** [**type-1 | type-2**] | **nssa-external** [**type-1** | **type-2**] }
Parameter	**Internal**: Indicates the internal route of OSPF.

Description	**external**: Indicates the external route of OSPF. **type-1 | type-2**: Indicates the Type-1 or Type-2 external route of OSPF. **nssa-external**: Indicates the OSPF NSSA external route.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the type of a route.

Command	**match tag** *tag* [*…tag*]
Parameter Description	*tag*: Indicates the tag value of a route.
Command Mode	Route map configuration mode
Usage Guide	This match rule is used to match the tag value of a route.

Setting the Processing Actions of a Policy

Command	**set level** {**stub-area** | **backbone** }
Parameter Description	**stub-area**: Indicates that the redistributed route is advertised to OSPF stub area. **backbone**: Indicates that the redistributed route is advertised to the OSPF backbone area.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to set the type of the destination area to which a route will be redirected.

Command	**set metric** [+ *metric-value* | **-** *metric-value* | *metric-value*]
Parameter Description	+: Indicates the value increased based on the metric value of the original route. -: Indicates the value decreased based on the metric value of the original route. *metric-value*: Sets the metric value of a redistributed route. A larger value means a lower priority.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to modify the metric value of a route.

Command	**set metric-type** *type*
Parameter Description	*type*: Sets the type of a redistributed route.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to set the metric type.

Command	**set next-hop** *ip-address*
Parameter Description	*ip-address*: Indicates the next-hop IP address.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to set the next-hop IP address.

Command	**set tag** *tag*
Parameter Description	*tag*: Sets the tag of a redistributed route.
Command Mode	Route map configuration mode
Usage Guide	This set rule is used to set the tag value of a route.

Displaying the Route Map Configuration

Command	**show route-map** [*name*]
Parameter Description	***name***: Specifies a route map.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Run the **show route-map** command to display the route map configuration. If an ACL is used when a route map is configured, you can run the **show access-list** command to display the ACL configuration.

Configuration Example

Using a Route Map in Route Redistribution to Filter and Modify Routing Information

Scenario Figure 1-4	As shown in Figure 1-4, a device is connected to both the OSPF routing domain and RIP routing domain. 
	● Redistribute only RIP routes with four hops to OSPF. In the OSPF routing domain, if the route type is Type-1 external route, set the tag value of the route to 40. ● Redistribute only OSPF routes with the tag value 10 to RIP. In the RIP routing domain, set the initial metric value of this route to 10.
Configuration Steps	● Configure the route map **redrip**: match a route with four hops, set the initial metric value of the route to 40, set the route type to Type-1 external route, and set the tag value of the route to 40. ● Configure the route map **redospf**: match a route with the tag value 10 and set the initial metric value of the route to 10. ● Configure redistribution of the RIP route to OSPF and apply the route map **redrip**. ● Configure redistribution of the OSPF route to RIP and apply the route map **redospf**.

	`Hostname(config)# route-map redrip permit 10`
	`Hostname(config-route-map)# match metric 4`
	`Hostname(config-route-map)# set metric-type type-1`
	`Hostname(config-route-map)# set tag 40`
	`Hostname(config-route-map)# exit`
	`Hostname(config)# route-map redospf permit 10`
	`Hostname(config-route-map)# match tag 10`
	`Hostname(config-route-map)# set metric 10`
	`Hostname(config-route-map)# exit`

	Hostname(config)# router ospf 1 Hostname(config-router)# redistribute rip subnets route-map redrip Hostname(config-router)# exit Hostname(config)# router rip Hostname(config-router)# redistribute ospf 1 route-map redospf Hostname(config-router)# exit
Verification	● Check the route map configuration to verify policy rules. ● Check the OSPF routing information library to verify that the rules matching the policy rules are redistributed.

	Hostname# show route-map
	route-map redrip, permit, sequence 10
	  Match clauses:
	  metric 4
	  Set clauses:
	  metric 40
	  metric-type type-1
	  tag 40
	route-map redospf, permit, sequence 10
	  Match clauses:
	  tag 10
	  Set clauses:
	  metric 10

	Hostname# show ip ospf database external
	
	  OSPF Router with ID (192.100.1.9) (Process ID 1)
	
	  AS External Link States
	
	  LS age: 5
	  Options: 0x2 (-|-|-|-|-|-|E|-)
	  LS Type: AS-external-LSA
	  Link State ID: 192.168.199.0 (External Network Number)
	  Advertising Router: 192.100.1.9
	  LS Seq Number: 80000001
	  Checksum: 0x554d
	  Length: 36
	  Network Mask: /24
	  Metric Type: 1
	  TOS: 0
	  Metric: 4
	  Forward Address: 0.0.0.0
	  External Route Tag: 40

1.4.2 Configuring a Filtering List

Configuration Effect

- Define a set of route filtering rules to be used by routing protocols.

Notes

- A configured filtering list can take effect only when being associated with a routing protocol.

Configuration Step

Configuring a Prefix-List

- To filter address prefixes, you should perform this configuration.
- Unless otherwise required, perform this configuration on devices for which filtering based on a prefix-list needs to be performed.

Verification

- Check whether the filtering list is correctly configured.
- Check the routing table to verify that routes can be correctly filtered.

Related Commands

Creating a Prefix-List

Command	**ip prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]
Parameter Description	***prefix-list-name***: Indicates the prefix-list name. *seq-number*: Assigns a sequence number to an prefix-list entry. The value range is from 1 to 2147483647. If this command does not contain the sequence number, the system will assign a default sequence number to the prefix-list entry. The default sequence number of the first entry is 5. Subsequently, the default sequence number of each entry not assigned with a value is the first multiple of 5 greater than the previous sequence number. **deny**: Denies access when certain conditions are matched. **permit**: Permits access when certain conditions are matched. ***ip-prefix***: Configures the IP address and mask. The value has 0 to 32 digits. ***minimum-prefix-length***: Specifies the minimum range, namely, start length of a range. ***maximum-prefix-length***: Specifies the maximum range, namely, end length of a range.
Command Mode	Global configuration mode
Usage Guide	N/A

Adding the Description to a Prefix-List

Command	**ip prefix-list** *prefix-list-name* **description** *description-text*
Parameter Description	***prefix-list-name***: Indicates the prefix-list name. *description-text*: Indicates the description of the prefix-list.
Command	Global configuration mode

Mode	
Usage Guide	N/A

Enabling the Sorting Function for a Prefix-List

Command	**ip prefix-list sequence-number**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Creating an IPv6 Prefix-List

Command	**ipv6 prefix-list** *prefix-list-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-prefix* [**ge** *minimum-prefix-length*] [**le** *maximum-prefix-length*]
Parameter Description	***prefix-list-name***: Indicates the prefix-list name. *seq-number*: Assigns a sequence number to an prefix-list entry. The value range is from 1 to 2147483647. If this command does not contain the sequence number, the system will assign a default sequence number to the prefix-list entry. The default sequence number of the first entry is 5. Subsequently, the default sequence number of each entry not assigned with a value is the first multiple of 5 greater than the previous sequence number. **deny**: Denies access when certain conditions are matched. **permit**: Permits access when certain conditions are matched. ***ipv6-prefix***: Configures the IP address and mask. The value has 0 to 128 digits. ***minimum-prefix-length***: Specifies the minimum range, namely, start length of a range. ***maximum-prefix-length***: Specifies the maximum range, namely, end length of a range.
Command Mode	Global configuration mode
Usage Guide	N/A

Adding Description to an IPv6 Prefix List

Command	**ipv6 prefix-list** *prefix-list-name* **description** *description-text*
Parameter Description	***prefix-list-name***: Indicates the prefix-list name. *description-text*: Indicates the description of the prefix-list.
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling the Sorting Function for an IPv6 Prefix-List

Command	**ipv6 prefix-list sequence-number**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Common Errors

- A filtering list is configured but is incorrectly applied in a routing protocol, which causes that the filtering list to take ineffective.

1.4.3 Configuring the Exit Policy for Routing Protocols

Configuration Effect

- When the memory reaches the lower threshold, to ensure running of other protocols in the system, one routing protocol will be disabled to release memory resources.

Related Commands

Configuring the Exit Policy for Routing Protocols

Command	**memory-lack exit-policy** { **ospf** | **rip** }
Parameter Description	**ospf**: Specifies the OSPF protocol as the first to exit when memory is insufficient. **rip**: Specifies the RIP protocol as the first to exit when memory is insufficient.
Command Mode	Global configuration mode
Usage Guide	You must learn main network services supported by corresponding routing protocols. In case of insufficient memory, the least important protocol should be disabled to ensure running of main services in extreme situations. For routing protocols that are disabled, specifying them as the first to exit will not help the system obtain sufficient memory resources. Specifying this policy only partially protects important network services in case of insufficient memory. If the memory is further consumed, all routing protocols will exit and stop running.

1.5 Monitoring

Displaying

Command	Description
show route-map [*route-map-name*]	Displays the route map configuration.
show ip prefix-list [*prefix-name*]	Displays the IPv4 prefix-list configuration.
show ipv6 prefix-list [*prefix-name*]	Displays the IPv6 prefix-list configuration.
show ip protocols { **ospf | rip** }	Displays information about the status of running IPv4 routing protocols.

1 Configuring PBR

1.1 Overview

Policy-based Routing (PBR) is implemented by applying a route map including policies to interfaces and devices.

Similar to static routing, PBR is also manually configured and cannot automatically adapt to network changes. In addition, PBR is effective only for packets sent from local interfaces and devices. Compared with static and dynamic routing, PBR is more flexible. Static and dynamic routing can forward packets only based on destination addresses. PBR can forward packets based on destination addresses and inbound interfaces.

1.2 Applications

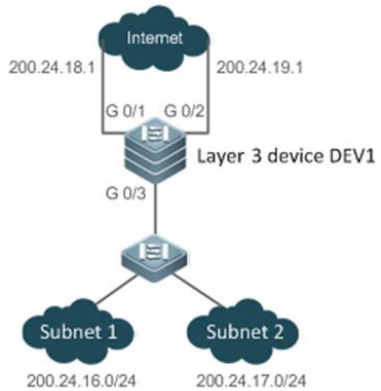
Application	Description
Selecting an ISP by Using PBR	Specify preferential outbound interfaces for packets from different subnets.

1.2.1 Selecting an ISP by Using PBR

An existing user network often uses resources of multiple internet server providers (ISPs). PBR is necessary because different bandwidths may be requested from different ISPs or the network resources for key users need to be protected. By controlling forwarding of specific data packets, you can optimize ISP resource usage and accomodate flexible and diversified application requirements.

Scenario

Figure 3-1



A LAN has two outbound interfaces connected to the Internet. PBR is configured on the Layer 3 device DEV1 to enable the two outbound interfaces to implement load balancing and mutual backup.

The specific requirements are as follows:

- Data streams from subnet 1 are sent from GE 0/1.
- Data streams from subnet 2 are sent from GE 0/2.

- If the link of GE 0/1 is disconnected, data streams on GE 0/1 are switched to GE 0/2. The same applies in reverse.

Deployment

- Configure two different Access Control Lists (ACLs) on DEV1:

ACL1: Source addresses belong to subnet 1.

ACL2: Source addresses belong to subnet 2.

- Configure two policies in the route map on DEV1:

Policy 1: Sets the next hops for packets matching ACL1 to GE0/1 and GE0/2. Based on the configuration sequence, GE0/1 takes effect first and GE0/2 works in backup mode.

Policy 2: Sets the next hops for packets matching ACL2 to GE0/2 and GE0/1. Based on the configuration sequence, GE0/2 takes effect first and GE0/1 works in backup mode.

- Configure PBR on GE0/3 by using a route map. Then, packets received on this interface are forwarded based on policies.

1.3 Features

Feature	Description
Configuring a Policy	Configures policies in a route map before configuring PBR.
Configuring PBR	Applies a route map including policies to interfaces and devices to implement PBR.

1.3.1 Configuring a Policy

A policy uses the "match …, set…" statement, indicating that processing actions are taken if certain conditions are met.

For details about policies, see *Configuring Routing Policies*.

Executing Policies

In global configuration mode, run the **route-map** *route-map-name* [**permit** | **deny**] [*sequence-number*] command to create a policy in a route map.

A route map may contain multiple policies, which are identified by sequence number. A smaller sequence number means a higher priority. Policies are executed based on their sequence numbers. Once the matching condition of a policy is met, the processing action for this policy needs to be taken and the route map exits. If no matching condition of any policy is met, no processing action will be taken.

Policies have two working modes:

- permit: When the matching condition of a policy is met, perform the processing action for this policy and exit the route map.
- deny: When the matching condition of a policy is met, do not perform the processing action for this policy and exit the route map.

Matching Conditions of Policies

The matching condition of a policy may contain no match rule, one match rule, or more match rules.

- If the matching condition contains no match rule, packets are matched.
- If the matching condition contains one or more match rules, packets must match all rules.

In route map configuration mode, run the **match** command to configure match rules. One **match** command is mapped to one match rule.

PBR supports the following **match** commands.

PBR	Command	Description
IPv4 PBR	**match ip address**	The source IPv4 address (and the destination IPv4 address) is used as the matching condition. Multiple **match ip address** commands can be configured in a policy.
IPv6 PBR	**match ipv6 address**	The source IPv6 address (and the destination IPv6 address) is used as the matching condition. Only one **match ipv6 policy** command can be configured in a policy.

IPv4 PBR defines the source IP address (and destination IP address) ranges of packets by using the standard or extended IP ACLs. IPv6 PBR defines the source IPv6 address (and destination IPv6 address) ranges of packets by using the extended IPv6 ACLs.

Packet forwarding based on policies of IPv4 PBR interfaces supports expert and MAC ACLs. Packet forwarding based on local policies does not support expert and MAC ACLs.

When PBR references a nonexistent ACL, the route sub-map will not be matched and the next route sub-map will be matched instead. If no route sub-map is matched, a common route will be selected for forwarding. If only ACLs are configured but no ACE is configured, the PBR forwarding behavior is the same as that in a scenario where an ACL does not exist.

Processing Action for a Policy

The processing action of a policy may contain no set rule, one set rule, or more set rules.

- If the processing action contains no set rule, no processing action will be performed and the route map will directly exit.
- If the processing action contains one or more set rules, all processing actions will be performed and then the route map will exit.

If set rules have different priorities, the set rule with the highest priority will take effect.

In route map configuration mode, run the **set** command to configure set rules. One **set** command is mapped to one set rule.

PBR supports the following **set** commands.

PBR	Command	Description
IPv4 PBR	**set ip next-hop**	Configures the next hop of IPv4 packet forwarding. The next hop must be directly connected; otherwise, this command is invalid. A packet matching the match rules will be forwarded to the next hop

PBR	Command	Description
		specified by **set ip next-hop first**, regardless of whether the route selected for the packet in the routing table is consistent with the next hop specified by PBR. On a switch, the outbound interfaces for next hops supported by PBR include the SVI, routed interface, and Layer 3 aggregate interface.
	set ip default next-hop	Configures the default next hop of IPv4 packet forwarding. A packet matching the match rules will be forwarded to the default next hop specified by this command if a route fails to be selected or the default route is selected for this packet in the routing table.
IPv6 PBR	**set ipv6 next-hop**	Configures the next hop of IPv6 packet forwarding. An IPv6 packet matching the match rules will be forwarded to the next hop specified by **set ipv6 next-hop** first, regardless of whether the route selected for the IPv6 packet in the routing table is consistent with the next hop specified by PBR. The next hop must be directly connected; otherwise, this command is invalid.
	set ipv6 default next-hop	Configures the default next hop of IPv6 packet forwarding. An IPv6 packet matching the match rules will be forwarded to the default next hop specified by this command if a route fails to be selected or the default route is selected for this packet in the routing table. The next hop must be directly connected; otherwise, this command is invalid.

The following commands and routes are in descending order of priority: **set ip next-hop**, common route, **set ip default next-hop**, and default route. The preceding **set** commands can be configured simultaneously, but only the command with the highest priority takes effect.

The following commands and routes are in descending order of priority: **set ipv6 next-hop**, common route, **set ipv6 default next-hop**, and default route. The preceding **set** commands can be configured at the same time but only the command with the highest priority takes effect.

The **set ipv6 default next-hop** command is invalid for IPv6 addresses with the mask length longer than 64.

1.3.2 Configuring PBR

PBR

Apply a route map including policies to interfaces or devices to implement PBR.

- Apply a route map to an interface so that packets received by the interface are routed based on the policy.
  PBR is often used to control user packets received by a device. This command is effective only for forwarded packets but not for packets initiated locally.

- Apply a route map to a device so that packets initiated locally are routed based on the policy.
  PBR is often used to control protocol packets exchanged between devices (such as ping packets sent locally).
  This command is effective only for locally initiated packets, but not for forwarded packets.

By default, PBR is unavailable on a device and packets are forwarded based on a routing table.

Redundant Backup or Load Balancing

You can set multiple next hops in a policy. Either redundant backup or load balancing can be implemented among multiple next hops. Redundant backup is implemented by default.

Redundant backup or load balancing is only effective for next hops configured in the **set ip next-hop**, **set ip next-hop recursive**, **set ip default next-hop**, **set ipv6 next-hop**, and **set ipv6 default next-hop** commands, and for multiple next hops in the same set rule.

- Redundant backup

  Based on the configuration sequence, the first accessible next hop takes effect. When the currently effective next hop (R1) is faulty, traffic automatically switches to the next accessible next hop (R2). When R1 becomes accessible again, traffic automatically switches back to R1.

  A newly added next hop is arranged at the end of the sequence. Assume that the original sequence of multiple next hops is R1 > R2 > R3. After R1 is deleted and added again, the sequence changes to R2 > R3 > R1.
  If no next hop is accessible, packets will be discarded.

- Load balancing
  When multiple accessible next hops take effect simultaneously, the Weighted Cost Multiple Path (WCMP) and Equal Cost Multiple Path (ECMP) are supported. After an accessible next hop becomes unavailable, traffic will be load balanced among the other accessible next hops.

Correlation with BFD

Correlation between PBR and BFD is effective only for next hops configured by the **set ip next-hop** or **set ipv6 next-hop** command.

Correlation between PBR and BFD helps enhance the capability to detect network changes. When BFD detects that the current next hop is inaccessible, BFD will immediately notify PBR to switch the traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

For details on how to configure correlation between PBR and BFD, see *Configuring BFD*.

Correlation with Track

Correlation between PBR and track is effective only for next hops configured by the **set ip next-hop** command.

The **set ip next-hop** command carries **verify-availability** and **track** *track-obj-number* parameters, which can be used to configure correlation between PBR and a track session and monitor reachability of next hops.

Correlation between PBR and track helps enhance the capability to detect network changes. When track detects that the current next hop is inaccessible, track will immediately notify PBR to switch traffic to another accessible next hop (to implement redundant backup) or all the other accessible next hops (to implement load balancing).

Only IPv4 PBR supports correlation with track.

For details on how to configure correlation between PBR and track, see *Configuring RNS*.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions of PBR	(Mandatory) It is used to apply PBR to forward packets.	
	ip policy route-map	Applies PBR to IPv4 packets received by an interface.
	ipv6 policy route-map	Applies PBR to IPv6 packets received by an interface.
	ip local policy route-map	Applies PBR to IPv4 packets initiated locally.
	ipv6 local policy route-map	Applies PBR to r IPv6 packets initiated locally.
Configuring Redundant Backup or Load Balancing	(Optional) It is used to set whether PBR implements redundant backup or load balancing among multiple next hops.	
	ip policy { **redundance** | **load-balance** }	Sets whether IPv4 PBR implements redundant backup or load balancing among multiple next hops. The default setting is redundant backup.
	ipv6 policy { **redundance** | **load-balance** }	Sets whether IPv6 PBR implements redundant backup or load balancing among multiple next hops. The default setting is redundant backup.

1.4.1 Configuring Basic Functions of PBR

Configuration Effect

Perform personalized routing management for user data streams by configuring flexible policies.

Perform personalized management for protocol interaction and network topologies by configuring flexible policies.

Notes

- A route map must be used when PBR is configured; therefore, you must configure a route map on a device.
- If an ACL is used when the route map is configured, you must first configure the ACL on the device.

Configuration Step

Applying PBR to IPv4 Packets Received by an Interface

- To perform personalized routing management for IPv4 user data streams passing a device, perform this configuration.
- Perform this configuration on the inbound interface for user data streams.
- Run the **ip policy route-map** command to apply a route map to an interface. Then, PBR is executed for IPv4 packets received on this interface.

Command	**ip policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is not configured on a device and packets are forwarded based on a routing table.
Command Mode	Interface configuration mode
Usage Guide	Only one **ip policy route-map** command can be configured for an interface. If multiple **ip policy route-map** commands are configured for an interface, only the latest configuration takes effect. If the route map used in PBR does not exist, PBR does not take effect.

Applying PBR to IPv6 Packets Received by an Interface

- To perform personalized routing management for IPv6 user data streams passing a device, perform this configuration.
- Perform this configuration on the inbound interface for user data streams.
- Run the **ipv6 policy route-map** command to apply a route map to an interface. Then, PBR is executed for IPv6 packets received on this interface.

Command	**ipv6 policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is not configured on a device and packets are forwarded based on a routing table.
Command Mode	Interface configuration mode
Usage Guide	Only one **ipv6 policy route-map** command can be configured for an interface. If multiple **ipv6 policy route-map** commands are configured for an interface, only the latest configuration takes effect. If the route map used in PBR does not exist, PBR does not take effect.

Applying PBR to IPv4 Packets Initiated Locally

- To perform personalized management for IPv4 protocol interaction and IPv4 network topologies, perform this configuration.
- Run the **ip local policy route-map** command to apply a route map to a device. Then PBR is executed for IPv4 packets initiated locally.

Command	**ip local policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is not configured on a device and packets are forwarded based on a routing table.
Command Mode	Global configuration mode
Usage Guide	Only one **ip local policy route-map** command can be configured for a device. If the route map used in PBR does not exist, PBR does not take effect.

Applying PBR to IPv6 Packets Initiated Locally

- To perform personalized management for IPv6 protocol interaction and IPv6 network topologies, perform this configuration.

- Run the **ipv6 local policy route-map** command to apply a route map to a device. Then, PBR is executed for IPv6 packets initiated locally.

Command	**ipv6 local policy route-map** *route-map-name*
Parameter Description	*route-map-name*: Indicates the name of a route map.
Defaults	By default, PBR is not configured on a device and packets are forwarded based on a routing table.
Command Mode	Global configuration mode
Usage Guide	Only one **ipv6 local policy route-map** command can be configured for a device. If the route map used in PBR does not exist, PBR does not take effect.

Verification

- Check the PBR configuration.
- Check the configuration of the route map used by PBR.
- If an ACL is used when the route map is configured, you should check the ACL configuration.

Displaying the IPv4 PBR Configuration

Command	**show ip policy** [*route-map-name*]
Parameter Description	*route-map-name*: Indicates the name of a route map.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Check the interfaces configured with IPv4 PBR according to the output information and the name of the used route map.
	`Hostname# show ip policy`
	`Banlance mode: redundance`
	`Interface Route map`
	`local RM_for_PBR_1`
	`GigabitEthernet 0/1 RM_for_PBR_2`
	Local indicates that PBR is applied to IPv4 packets initiated locally.

Displaying the IPv6 PBR Configuration

Command	**show ipv6 policy** [*route-map-name*]
Parameter Description	*route-map-name*: Indicates the name of a route map.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Check the interfaces configured with IPv6 PBR according to the output information and the name of the used route map.
	`Hostname#show ipv6 policy`
	`Banlance mode: redundance`
	`Interface Route map`
	`local RM_for_PBR_1`

	`VLAN 1 RM_for_PBR_2` **Local** indicates that PBR is applied to IPv6 packets initiated locally.

Displaying the Route Map Configuration

Command	**show route-map** [*route-map-name*]
Parameter Description	*route-map-name*: Indicates the name of a route map.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Multiple route maps may be available on a device. Focus on the route map used in PBR and check its policy settings.
	`Hostname# show route-map`
	`route-map RM_FOR_PBR, permit, sequence 10`
	`  Match clauses:`
	`    ip address acl1`
	`  Set clauses:`
	`ip next-hop 200.24.18.1`
	`route-map RM_FOR_PBR, permit, sequence 20`
	`  Match clauses:`
	`    ip address acl2`
	`  Set clauses:`
	`ip next-hop 200.24.19.1`

Displaying the ACL Configuration

Command	**show access-lists** [*acl-id* | *acl-name*]
Parameter Description	*acl-id*: Indicates the number of an ACL. *acl-name*: Indicates the name of an ACL.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Multiple ACLs may be available on a device. Focus on the ACL used by a route map and check its configuration.
	`Hostname# show access-lists 1`
	`ip access-list standard 1`
	`  10 permit 200.24.16.0 0.0.0.255`
	`ip access-list standard 2`
	`  10 permit 200.24.17.0 0.0.0.255`

Displaying Routing Information About IPv4 PBR

Command	**show ip pbr route** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates that PBR is applied to packets initiated locally.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Specify a local interface or device and check routing information about IPv4 PBR.

```
Hostname# show ip pbr route
PBR IPv4 Route Summay : 1
Interface        : GigabitEthernet 0/1
  Sequence       : 10
  VRF ID         : 0
  Route Flags    :
   Route Type    : PBR
   Direct        : Permit
   Priority      : High
   Precedence    : None
  Precedence     : 0
  Mode           : redundance
  Nexthop Count  : 1
   Nexthop[0]    : 192.168.8.100
   Weight[0]     : 1
   Ifindex[0]    : 2
```

Displaying Routing Information About IPv6 PBR

Command	**show ipv6 pbr route** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates that PBR is applied to packets initiated locally.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	Specify a local interface or device and check routing information about IPv6 PBR.

```
Hostname# show ipv6 pbr route
PBR IPv6 Route Summary : 1
Interface        : GigabitEthernet 0/1
  Sequence       : 10
  ACL[0]         : 2900
  ACL_CLS[0]     : 5
  VRF ID         : 0
  Route Flags    :
   Route Type    : PBR
   Direct        : Permit
   Priority      : High
   Precedence    : None
  Precedence     : 0
  Mode           : redundance
  Nexthop Count  : 1
   Nexthop[0]    : 10::2
   Weight[0]     : 1
   Ifindex[0]    : 2
```

Displaying the Route Map Used by IPv4 PBR

Command	**show ip pbr route-map** *rmap-name*
Parameter Description	*rmap-name*: Indicates the name of a route map.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Specify a route map and check the route map used by IPv4 PBR.
	`Hostname# show ip pbr route-map rm`
	`PBR VRF: GLOBAL, ID: 0`
	` Forward Mode: redundance`
	` Forwarding: On`
	
	`Route-map rm`
	`  Route-map index: Sequence 10, permit`
	`    Match rule:`
	`      ACL ID :   2900, CLS: 1, Name: acl1`
	`    Set rule:`
	`      IPv4 nexthop: 192.168.8.100, (VRF name: , ID: 0), Weight: 0`
	`        PBR state info ifx: 2, Connected: True, Track state: Up`

Displaying the Route Map Used by IPv6 PBR

Command	**show ipv6 pbr route-map** *rmap-name*
Parameter Description	*rmap-name*: Indicates the name of a route map.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Specify a route map and check the route map used by IPv6 PBR.
	`Hostname# show ipv6 pbr route-map rm6`
	`PBR VRF: GLOBAL, ID: 0`
	` Forward Mode: redundance`
	` Forwarding: On`
	
	`Route-map rm6`
	`  Route-map index: Sequence 10, permit`
	`    Match rule:`
	`      ACL ID :   2901, CLS: 5, Name: acl6`
	`    Set rule:`
	`      IPv6 nexthop: 10::2, (VRF name: , ID: 0), Weight: 0`
	`        PBR state info ifx: 2, Connected: True, Track state: Up`

Displaying Statistics About Packets Forwarded by IPv4 PBR

Command	**show ip pbr statistics** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates that PBR is applied to packets initiated locally.
Command	Privileged EXEC mode, global configuration mode, or interface configuration mode

Mode	

Usage Guide	`Hostname# show ip pbr statistics`
	`IPv4 Policy-based route statistic`
	`gigabitEthernet 0/1`
	`  statistics : 10`

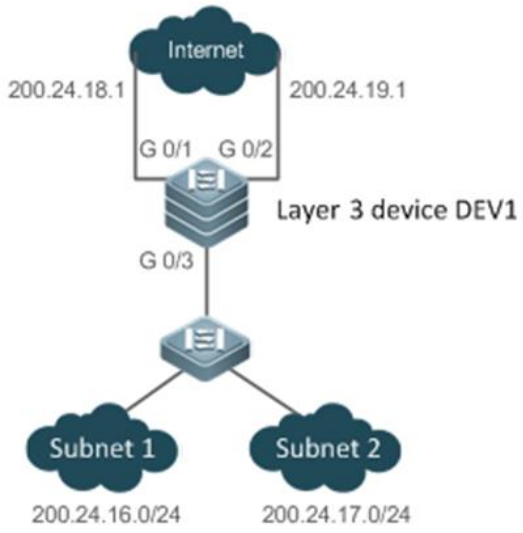
Displaying Statistics About Packets Forwarded by IPv6 PBR

Command	**show ipv6 pbr statistics** [**interface** *if-name* | **local**]
Parameter Description	*if-name*: Indicates an interface name. **local**: Indicates that PBR is applied to packets initiated locally.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	`Hostname# show ipv6 pbr statistics`
	`IPv6 Policy-based route statistic`
	`gigabitEthernet 0/1`
	`  statistics : 20`

Configuration Example

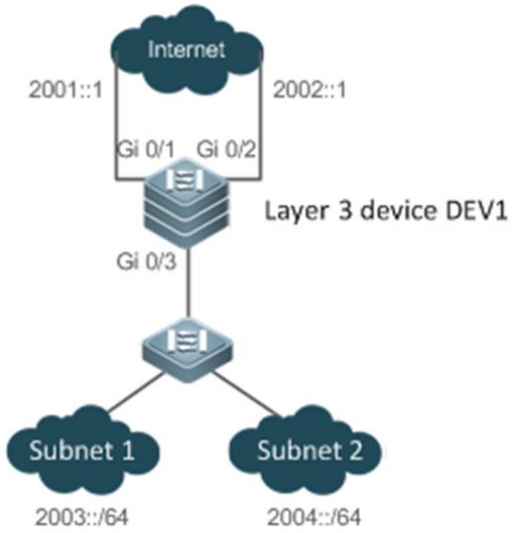
Configuring IPv4 PBR and Selecting an Egress Link Based on Source Addresses of Packets

Scenario **Figure 3-2**	
	● The Layer 3 device DEV1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 200.24.16.0/24, whereas the network segment where subnet 2 resides is 200.24.17.0/24. ● DEV1 is connected to the Internet through GE0/1 and GE0/2, and their next hops are 200.24.18.1 and 200.24.19.1.
	This LAN has two outbound interfaces connected to the Internet. The requirements are as follows: ● Data streams from subnet 1 for accessing the Internet should pass GE 0/1. ● Data streams from subnet 2 for accessing the Internet should pass GE 0/2. ● If the link of GE 0/1 link is disconnected, data streams on GE 0/1 are switched to GE 0/2. The same applies in reverse.
Configuration	● Configure two ACLs to match packets from subnets 1 and 2 respectively. ● Set a policy and configure next hops for packets from subnet 1 to GE0/1 and GE0/2. (Pay

Steps	attention to the configuration sequence.) ● Set a policy and configure next hops for packets from subnet 2 to GE0/2 and GE0/1. (Pay attention to the configuration sequence.) ● Apply the policy to GE 0/3. ● Configure redundant backup among multiple next hops. (Redundant backup is used by default.) During redundant backup, based on the configuration sequence, the first next hop takes effect first.
	DEV1(config)# access-list 1 permit 200.24.16.0 0.0.0.255 DEV1(config)# access-list 2 permit 200.24.17.0 0.0.0.255 DEV1(config)# route-map RM_FOR_PBR 10 DEV1(config-route-map)# match ip address 1 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# exit DEV1(config)# route-map RM_FOR_PBR 20 DEV1(config-route-map)# match ip address 2 DEV1(config-route-map)# set ip next-hop 200.24.19.1 DEV1(config-route-map)# set ip next-hop 200.24.18.1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy redundance
Verification	● Check the IPv4 PBR configuration. ● Check the route map configuration. ● Check the ACL configuration.
	DEV1# show ip policy Interface Route map GigabitEthernet 0/3 RM_FOR_PBR
	DEV1# show route-map route-map RM_FOR_PBR, permit, sequence 10 Match clauses: ip address 1 Set clauses: ip next-hop 200.24.18.1 200.24.19.1 route-map RM_FOR_PBR, permit, sequence 20 Match clauses: ip address 2 Set clauses: ip next-hop 200.24.19.1 200.24.18.1
	DEV1# show access-lists ip access-list standard 1 10 permit 200.24.16.0 0.0.0.255

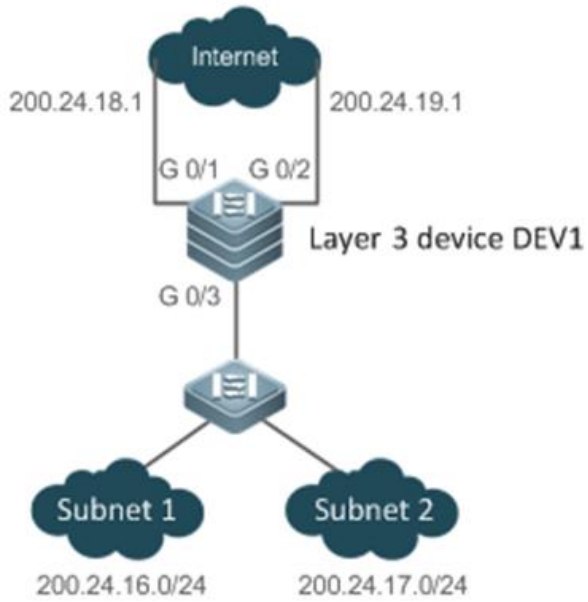
	ip access-list standard 2 10 permit 200.24.17.0 0.0.0.255

Configuring IPv6 PBR and Selecting an Egress Link Based on Source Addresses of Packets

Scenario **Figure 3-3**	
	● DEV1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 2003::/64, whereas the network segment where subnet 2 resides is 2004::/64. ● DEV1 is connected to the Internet through GE0/1 and GE0/2, and their next hops are 2001::1/64 and 2002::1/64.
	This LAN has two outbound interfaces connected to the Internet. The requirements are as follows: ● Data streams from subnet 1 for accessing the Internet should pass GE 0/1. ● Data streams from subnet 2 for accessing the Internet should pass GE 0/2. ● If the link of GE 0/1 link is disconnected, data streams on GE 0/1 are switched to GE 0/2. The same applies in reverse.
Configuration Steps	● Configure two ACLs to match packets from subnets 1 and 2 respectively. ● Set a policy and configure next hops for packets from subnet 1 to GE0/1 and GE0/2. (Pay attention to the configuration sequence.) ● Set a policy and configure next hops for packets from subnet 2 to GE0/2 and GE0/1. (Pay attention to the configuration sequence.) ● Apply the policy to GE 0/3. ● Configure redundant backup among multiple next hops. During redundant backup, based on the configuration sequence, the first next hop takes effect first.
	DEV1(config)# ipv6 access-list net1 DEV1(config-ipv6-acl)# permit ipv6 2003::/64 any DEV1(config-ipv6-acl)# exit DEV1(config)# ipv6 access-list net2 DEV1(config-ipv6-acl)# permit ipv6 2004::/64 any DEV1(config-ipv6-acl)# exit DEV1(config)# route-map RM_FOR_PBR 30 DEV1(config-route-map)# match ipv6 address net1

	DEV1(config-route-map)# set ipv6 next-hop 2001::1 DEV1(config-route-map)# set ipv6 next-hop 2002::1 DEV1(config-route-map)# exit DEV1(config)# route-map RM_FOR_PBR 40 DEV1(config-route-map)# match ipv6 address net2 DEV1(config-route-map)# set ipv6 next-hop 2002::1 DEV1(config-route-map)# set ipv6 next-hop 2001::1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ipv6 policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ipv6 policy redundance
Verification	● Check the IPv6 PBR configuration. ● Check the route map configuration. ● Check the ACL configuration.
	DEV1# show ipv6 policy Interface Route map GigabitEthernet 0/3 RM_FOR_PBR
	DEV1# show route-map route-map RM_FOR_PBR, permit, sequence 11 Match clauses: ipv6 address net1 Set clauses: ipv6 next-hop 2001::1 2002::1 route-map RM_FOR_PBR, permit, sequence 21 Match clauses: ipv6 address net2 Set clauses: ipv6 next-hop 2002::1 2001::1
	DEV1# show access-lists ipv6 access-list net1 10 permit ipv6 2003::/64 any (0 packets matched) ipv6 access-list net2 10 permit ipv6 2004::/64 any (0 packets matched)

Configuring Correlation Between IPv4 PBR and Track

Scenario **Figure 3-4**	
	● The Layer 3 device DEV1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 200.24.16.0/24, whereas the network segment where subnet 2 resides is 200.24.17.0/24. ● DEV1 is connected to the Internet through GE0/1 and GE0/2 and their next hops are 200.24.18.1 and 200.24.19.1.
	● DEV1 can fast detect a faulty egress link and switch to a backup link.
Configuration Steps	When configuring IPv4 PBR and selecting an egress link based on source addresses of the packets, add or modify the following configurations: ● Set two track objects to track reachability of the next hops of the two outbound interfaces. ● When configuring a policy, configure correlation between the next hops and track objects.
DEV1	DEV1(config)# ip access-list extended 101 DEV1(config-ip-acl)# permit ip 200.24.16.0 0.0.0.255 any DEV1(config-ip-acl)# exit DEV1(config)# ip access-list extended 102 DEV1(config-ip-acl)# permit ip 200.24.17.0 0.0.0.255 any DEV1(config-ip-acl)# exit DEV1(config)#ip rns 1 DEV1(config-ip-rns)#icmp-echo 200.24.18.1 DEV1(config)#ip rns schedule 1 start-time now life forever DEV1(config)#track 1 rns 1 DEV1(config)#ip rns 2 DEV1(config-ip-rns)#icmp-echo 200.24.19.1 DEV1(config)#ip rns schedule 2 start-time now life forever DEV1(config)#track 2 rns 2 DEV1(config)# route-map RM_FOR_PBR 10 DEV1(config-route-map)# match ip address 101 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1

	track 2 DEV1(config-route-map)# exit DEV1(config)# route-map RM_FOR_PBR 20 DEV1(config-route-map)# match ip address 102 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.19.1 track 2 DEV1(config-route-map)# set ip next-hop verify-availability 200.24.18.1 track 1 DEV1(config-route-map)# exit DEV1(config)# interface GigabitEthernet 0/3 DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_FOR_PBR DEV1(config-if-GigabitEthernet 0/3)# exit DEV1(config)# ip policy redundance
Verification	● Check whether the track objects are Up.

DEV1	DEV1#show track
	Track 1
	  Reliable Network Service 1
	  The state is Up
	  1 change, current state last: 120 secs
	  Delay up 30 secs, down 50 secs
	Track 2
	  Reliable Network Service 2
	  The state is Up
	  1 change, current state last: 130 secs
	  Delay up 30 secs, down 50 secs

Common Errors

- A route map is used when PBR is configured but the route map does not exist.
- An ACL is used when a route map is configured but the ACL does not exist.

1.4.2 Configuring Redundant Backup or Load Balancing

Configuration Effect

- Using multiple next hops in backup mode can enhance network reliability.
- Implementing load balancing among multiple next hops can increase the network bandwidth.

Notes

- Basic functions of PBR must be configured.
- Redundant backup and load balancing are effective only for the next hops configured by the following **set** commands.

Command	Description
set ip next-hop	Configures the next hop of IPv4 packets. This command carries the *weight* parameter, which is used to set the weight of WCMP. The default value is 1.

set ip default next-hop	Configures the default next hop of IPv4 packets. This command carries the *weight* parameter, which is used to set the weight of WCMP. The default value is 1.
set ipv6 next-hop	Configures the next hop of IPv6 packets. This command carries the *weight* parameter, which is used to set the weight of WCMP. The default value is 1.
set ipv6 default next-hop	Configures the default next hop of IPv6 packets. This command carries the *weight* parameter, which is used to set the weight of WCMP. The default value is 1.

Up to eight next hops can be set for WCMP, whereas up to 32 next hops can be set for ECMP.

Configuration Step

Configuring Whether IPv4 PBR Implements Redundant Backup or Load Balancing Among Multiple Next Hops

- If load balancing needs to be implemented among multiple next hops, perform this configuration.
- If load balancing is configured, perform this configuration to restore redundant backup.
- This configuration is effective for all PBR-based routes configured on a device.

Command	**ip policy** { **redundance** | **load-balance** }
Parameter Description	redundance: Indicates redundant backup. load-balance: Indicates load balancing.
Defaults	Redundant backup is configured by default.
Command Mode	Global configuration mode
Usage Guide	If redundant backup is selected, the first next hop takes effect based on the configuration sequence. If load balancing is selected, all next hops take effect simultaneously and share traffic by weight.

Configuring Whether IPv6 PBR Implements Redundant Backup or Load Balancing Among Multiple Next Hops

- If load balancing needs to be implemented among multiple next hops, perform this configuration.
- If load balancing is configured, perform this configuration to restore redundant backup.
- This configuration is effective for all PBR-based routes configured on a device.

Command	**ipv6 policy** { **redundance** | **load-balance** }
Parameter Description	redundance: Indicates redundant backup. load-balance: Indicates load balancing.
Defaults	Redundant backup is configured by default.
Command Mode	Global configuration mode
Usage Guide	If redundant backup is selected, the first next hop takes effect based on the configuration sequence. If load balancing is selected, all next hops take effect simultaneously and share traffic by weight.

Verification

- Check whether redundant backup or load balancing is implemented among multiple next hops.

Displaying Whether IPv4 PBR Implements Redundant Backup or Load Balancing Among Multiple Next Hops

Command	**show ip policy** [*route-map-name*]
Parameter Description	***route-map-name***: Specifies a route map.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	See the following example and focus on the red field.
	`Hostname# show ip policy`
	`Banlance mode: redundance`
	`Interface Route map`
	`local test`
	`GigabitEthernet 0/3 test`

Checking whether IPv6 PBR implements redundant backup or load balancing among multiple next hops

Command	**show ipv6 policy** [*route-map-name*]
Parameter Description	***route-map-name***: Specifies a route map.
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	See the following example and focus on the red field.
	`Hostname#show ipv6 policy`
	`Banlance mode: redundance`
	`Interface Route map`
	`VLAN 1 RM_for_Vlan_1`
	`VLAN 2 RM_for_Vlan_2`

Configuration Example

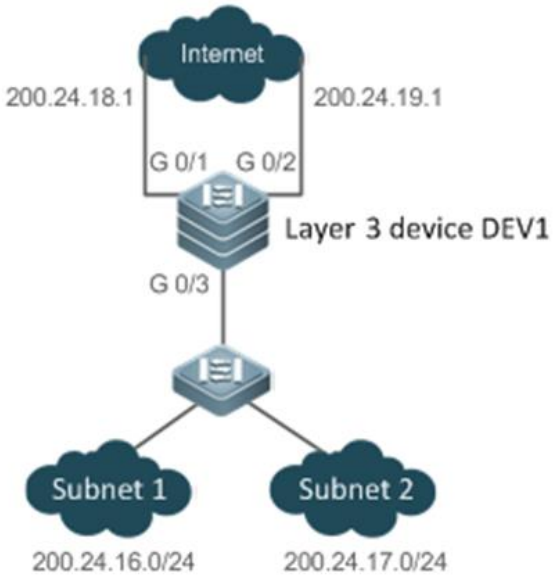
Configuring IPv4 PBR to implement redundant backup among multiple next hops

See Configuring IPv4 PBR and Selecting an Egress Link Based on Source Addresses of Packets.

Configuring IPv6 PBR to implement redundant backup among multiple next hops

See Configuring IPv6 PBR and Selecting an Egress Link Based on Source Addresses of Packets.

Configuring IPv4 PBR to Implement Load Balancing Among Multiple Next Hops

Scenario **Figure 3-5**	
	● The Layer 3 device DEV1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 200.24.16.0/24, whereas the network segment where subnet 2 resides is 200.24.17.0/24. ● DEV1 is connected to the Internet through GE0/1 and GE0/2, and their next hops are 200.24.18.1 and 200.24.19.1.
	This LAN has two outbound interfaces connected to the Internet. The requirements are as follows: ● Traffic is equally shared by GE0/1 and GE0/2.
Configuration Steps	● Configure basic functions of PBR. Specify multiple next hops. ● Set the load balancing mode.

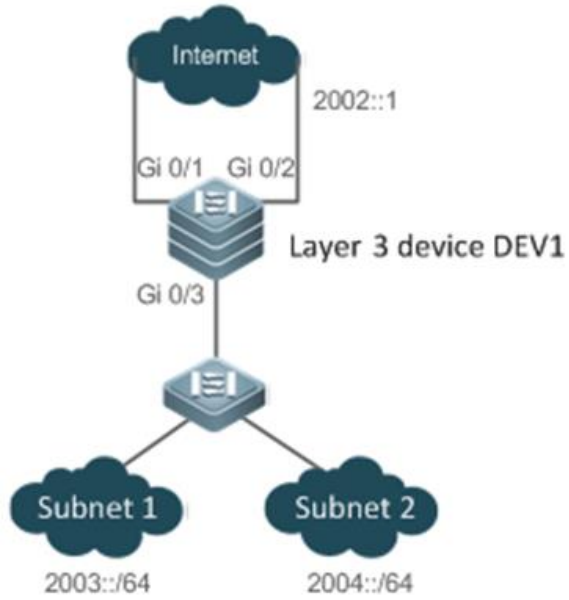
	`DEV1(config)# route-map RM_LOAD_PBR 10`
	`DEV1(config-route-map)# set ip next-hop 200.24.18.1`
	`DEV1(config-route-map)# set ip next-hop 200.24.19.1`
	`DEV1(config-route-map)# exit`
	`DEV1(config)# interface GigabitEthernet 0/3`
	`DEV1(config-if-GigabitEthernet 0/3)# ip policy route-map RM_LOAD_PBR`
	`DEV1(config-if-GigabitEthernet 0/3)# exit`
	`DEV1(config)# ip policy load-balance`

Verification	● Check the IPv4 PBR configuration. ● Check the route map configuration.

	`DEV1# show ip policy`
	`Balance mode: load-balance`
	`Interface Route map`
	`GigabitEthernet 0/3 RM_LOAD_PBR`

	`DEV1# show route-map`
	`route-map PBR-VRF-Selection, permit, sequence 10`
	`Match clauses:`
	`Set clauses:`
	`ip next-hop 200.24.18.1 8`
	`ip next-hop 200.24.19.1 8`

Configuring IPv6 PBR to Implement Load Balancing Among Multiple Next Hops

Scenario **Figure 3-6**	
	● DEV1 is connected to subnet 1 and subnet 2 through GE0/3. The network segment where subnet 1 resides is 2003::/64, whereas the network segment where subnet 2 resides is 2004::/64. ● DEV1 is connected to the Internet through GE0/1 and GE0/2, and their next hops are 2001::1/64 and 2002::1/64.
	This LAN has two outbound interfaces connected to the Internet. The requirements are as follows: ● Traffic is equally shared by GE0/1 and GE0/2.
Configuration Steps	● Configure basic functions of PBR. Specify multiple next hops. ● Set the load balancing mode.

	`DEV1(config)# route-map RM_LOAD_PBR 20`
	`DEV1(config-route-map)# set ipv6 next-hop 2001::1`
	`DEV1(config-route-map)# set ipv6 next-hop 2002::1`
	`DEV1(config-route-map)# exit`
	`DEV1(config)# interface GigabitEthernet 0/3`
	`DEV1(config-if-GigabitEthernet 0/3)# ipv6 policy route-map RM_LOAD_PBR`
	`DEV1(config-if-GigabitEthernet 0/3)# exit`
	`DEV1(config)# ipv6 policy load-balance`

Verification	● Check the IPv6 PBR configuration. ● Check the route map configuration.

	`DEV1# show ipv6 policy`
	`Balance mode: load-balance`
	`Interface Route map`
	`GigabitEthernet 0/3 RM_LOAD_PBR`
	`DEV1# show route-map`
	`route-map PBR-VRF-Selection, permit, sequence 10`
	`Match clauses:`
	`Set clauses:`

	ipv6 next-hop 2001::1 ipv6 next-hop 2002::1

1.5 Monitoring

Clearing

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

Command	Description
clear ip pbr statistics [**interface** *if-name* | **local**]	Clears statistics about packets forwarded by IPv4 PBR.
clear ipv6 pbr statistics [**interface** *if-name* | **local**]	Clear statistics about packets forwarded by IPv6 PBR.

Displaying

Command	Description
show ip policy	Displays the IPv4 PBR configuration.
show ipv6 policy	Displays the IPv6 PBR configuration.
show route-map [*name*]	Displays the route map configuration.
show access-list	Displays the ACL configuration.
show ip pbr bfd	Displays correlation between IPv4 PBR and BFD.
show ipv6 pbr bfd	Displays correlation between IPv6 PBR and BFD.
show ip pbr route [**interface** *if-name* | **local**]	Displays routing information about IPv4 PBR.
show ipv6 pbr route [**interface** *if-name* | **local**]	Displays routing information about IPv6 PBR.
show ip pbr route-map *rmap-name*	Displays a route map used by IPv4 PBR.
show ipv6 pbr route-map *rmap-name*	Displays a route map used by IPv6 PBR.
show ip pbr statistics [**interface** *if-name* | **local**]	Displays statistics about IPv4 PBR.
show ipv6 pbr statistics [**interface** *if-name* | **local**]	Displays statistics about IPv6 PBR.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug pbr error	Debugs PBR errors.
debug pbr events	Debugs PBR events.
debug pbr ms	Debugs multiple service cards supported by PBR.
debug pbr msg	Debugs PBR message communication.
debug pbr nsm	Debugs interaction between PBR and NSM.
debug pbr packet	Debugs packet forwarding of PBR.
debug pbr restart	Debugs PBR GR.

1 Configuring Keys

1.1 Overview

Keys are used in algorithms for conversion from cleartext to cipher text or from cipher text to cleartext.

Cleartext and cipher text authentication are supported for packet authentication in a routing protocol, during which keys need to be used.

Keys are used only for RIP packet authentication.

1.2 Applications

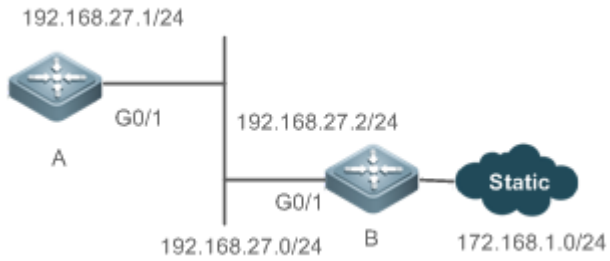
Application	Description
RIP Authentication	RIP uses keys for packet authentication.

1.2.1 RIP Authentication

Scenario

Network devices run RIP and use the MD5 authentication mode to improve protocol security.

Figure 1-1



Deployment

- Configure a keychain on A. Configure RIP to enable packet authentication and use the keychain.
- Configure a keychain on B. Configure RIP to enable packet authentication and use the keychain.

1.3 Features

Overview

Feature	Description
Keychain	Provides authentication in a routing protocol.

1.3.1 Keychain

Working Principle

A keychain may contain multiple different keys. Each key contains the following attributes:

- Key ID: Identifies a key. In the keychain, keys and IDs are mapped in one-to-one manner.
- Authentication string: Indicates a set of key characters used for verifying consistency of authentication strings in a routing protocol.
- Lifetime: Specifies the lifetime of the key for sending or receiving packets. Different authentication keys can be used in different periods.

Related Configuration

Creating a Keychain and a Key

In global configuration mode, run the **key chain** *key-chain-name* command to define a keychain and enter the keychain configuration mode.

In keychain configuration mode, run the **key** *key-id* command to define a key and enter the keychain key configuration mode.

Configuring an Authentication String

In keychain key configuration mode, run the **key-string** [**0** | **7**] *text* command to specify an authentication string.

- A cleartext authentication string is configured by default. The value 0 indicates that a cleartext authentication key is configured.
- The value 7 indicates that a cipher text authentication string is configured.
- The encryption authentication service is disabled by default. You can run the **service password-encryption** command to enable the encryption service to forcibly convert cleartext authentication into cipher text.

Configuring Lifetime

In the keychain key configuration mode, you can configure the lifetime of a keychain in receiving and sending directions.

- **accept-lifetime** *start-time* { **infinite |** *end-time* **| duration** *seconds* }: Configures the lifetime of a keychain in the receiving direction.
- **send-lifetime** *start-time* { **infinite |** *end-time* **| duration** *seconds* }: Configures the lifetime of a keychain in the sending direction.

1.4 Configuration

Configuration	Description and Command	
Configuring a Keychain	(Mandatory) It is used to create a key.	
	key chain	Creates a keychain.
	key	Configures a key ID.
	key-string	Configures a key string.
	accept-lifetime	Configures the lifetime in the receiving direction.

Configuration	Description and Command	
	send-lifetime	Configures the lifetime in the sending direction.

1.4.1 Configuring a Keychain

Configuration Effect

- Define a keychain to be used by a routing protocol.

Notes

- A keychain can take effect only when being associated with a routing protocol.

Configuration Step

Creating a Key Chain

- This configuration is mandatory if a keychain needs to be used.
- Unless otherwise required, perform this configuration on all routers for which routing protocol authentication needs to be performed.

Configuring a Key ID

- This configuration is mandatory if a keychain needs to be used.
- Unless otherwise required, perform this configuration on all routers for which routing protocol authentication needs to be performed.

Configuring a Key String

- This configuration is mandatory if a keychain needs to be used.
- Unless otherwise required, perform this configuration on all routers for which routing protocol authentication needs to be performed.

Configure the Lifetime in the Receiving Direction

- Optional.
- If the lifetime in the sending direction is not configured, the keychain will be always effective.

Configure the Lifetime in the Sending Direction

- Optional.
- If the lifetime in the sending direction is not configured, the keychain will be always effective.

Verification

- Use keys in a routing protocol and observe the neighbor relationship established by the routing protocol. If the keys are inconsistent, the neighbor relationship fails to be established.

Related Commands

Configuring a Key Chain

Command	**key chain** *key-chain-name*
Parameter Description	*key-chain-name*: Indicates the name of a keychain.
Command Mode	Global configuration mode
Usage Guide	To make a keychain take effect, you must configure at least one key.

Configuring a Key ID

Command	**key** *key-id*
Parameter Description	*key-id*: Indicates the authentication key ID in a keychain. The value range is from 0 to 2147483647.
Command Mode	Keychain configuration mode.
Usage Guide	-

Configuring a Key Authentication String

Command	**key-string** [**0** | **7**] *text*
Parameter Description	**0**: Specifies that the key is displayed in cleartext. **7**: Specifies that the key is displayed in cipher text. *text*: Specifies the authentication character string.
Command Mode	Keychain key configuration mode.
Usage Guide	-

Configuring the Lifetime in the Sending Direction

Command	**send-lifetime** *start-time* {**infinite** | *end-time* | **duration** *seconds*}
Parameter Description	***start-time***: Indicates the start time of the lifetime. **infinite**: Indicates that the key is always effective. ***end-time***: Indicates the end time of the lifetime, which must be later than the start time. **duration *seconds***: Specifies the duration from the start time to the end time. The value range is from 1 to 2147483646.
Command Mode	Keychain key configuration mode.
Usage Guide	Run this command to define the lifetime of the key in the sending direction.

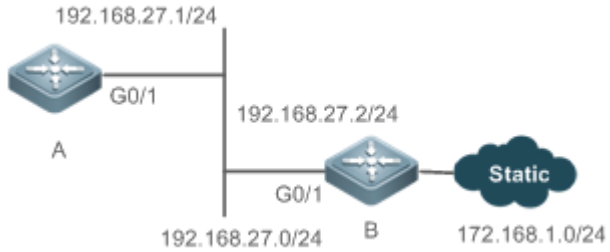
Configuring the Lifetime in the Receiving Direction

Command	**accept-lifetime** *start-time* **{infinite |** *end-time* **| duration** *seconds***}**
Parameter Description	***start-time***: Indicates the start time of the lifetime. **infinite**: Indicates that the key is always effective. ***end-time***: Indicates the end time of the lifetime, which must be later than the start time. **duration *seconds***: Specifies the duration from the start time to the end time. The value range is from 1 to 2147483646.
Command Mode	Keychain key configuration mode.

Usage Guide	Run this command to define the lifetime of the key in the receiving direction.

Configuration Example

Configuring a Keychain and Using the Keychain in RIP Packet Authentication

Scenario Figure 1-2	
Configuration Steps	● Configure a key on all routers. ● Configure RIP on all routers. ● Enable RIP authentication on all routers.
A	A>enable A#configure terminal A(config)#key chain ripchain A(config-keychain)#key 1 A(config-keychain-key)#key-string Hello A(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2013 duration 43200 A(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2013 duration 43200 A(config-keychain-key)#exit A(config-keychain)#key 2 A(config-keychain-key)#key-string World A(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 2013 infinite A(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2013 infinite A(config-keychain-key)#exit A(config)#interface gigabitEthernet 0/1 A(config-if)#ip address 192.168.27.1 255.255.255.0 A(config-if)#ip rip authentication key-chain ripchain A(config-if)#ip rip authentication mode md5 A(config-if)#exit A(config)#router rip A(config-router)#version 2 A(config-router)#network 192.168.27.0
B	B>enable B#configure terminal B(config)#key chain ripchain B(config-keychain)#key 1 B(config-keychain-key)#key-string Hello B(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2013 duration 43200 B(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2013 duration 43200 B(config-keychain-key)#exit

	B(config-keychain)#key 2 B(config-keychain-key)#key-string World B(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 2013 infinite B(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2013 infinite B(config-keychain-key)#exit B(config)#interface gigabitEthernet 0/1 B(config-if)#ip address 192.168.27.2 255.255.255.0 B(config-if)#ip rip authentication key-chain ripchain B(config-if)#ip rip authentication mode md5 B(config-if)#exit B(config)#router rip B(config-router)#version 2 B(config-router)#network 192.168.27.0 B(config-router)#redistribute static
Verification	● Run the **show ip route rip** command to check whether router A can receive an RIP route from router B.
A	A(config)#show ip route rip R 172.168.0.0/16 [120/1] via 192.168.27.2, 00:05:16, GigabitEthernet 0/1

Common Errors

- A key is not correctly associated with a routing protocol, which causes an authentication failure.
- The keys configured on multiple routers are inconsistent, which causes an authentication failure.

1.5 Monitoring

Displaying

Command	Description
show key chain [*key-chain-name*]	Displays the configurations of a keychain.

Configuring Multicast

1. Configuring IPv4 Multicast Routing Configuration
2. Configuring IGMP Snooping

1 Configuring IPv4 Multicast Routing Configuration

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 Monitoring

Displaying

Description	Command
Displays the IPv4 multicast non-stop forwarding configuration.	**show msf nsf**
Displays the IPv4 multi-layer multicast forwarding table.	**show msf msc**

Debugging

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

Description	Command
Debugs the processing of IPv4 multi-layer multicast packet forwarding.	**debug msf forwarding**
Debugs the operation on multi-layer multicast forwarding entries on an IPv4 network.	**debug msf 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 events**

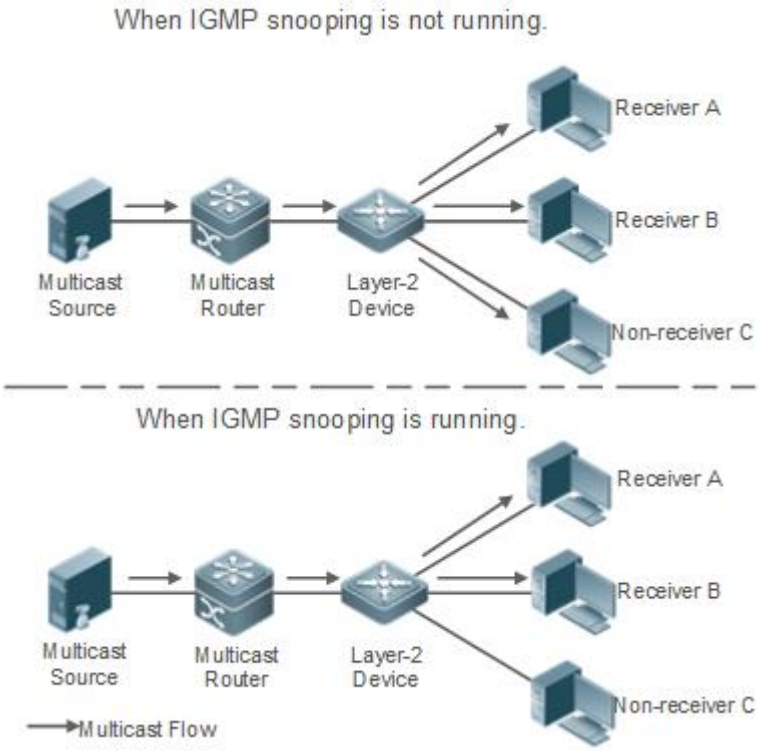
1 Configuring IGMP Snooping

1.1 Overview

Internet Group Management Protocol (IGMP) snooping is a mechanism of listening to IP multicast. It is used to manage and control the forwarding of IP multicast traffic within VLANs, realizing Layer-2 multicasting.

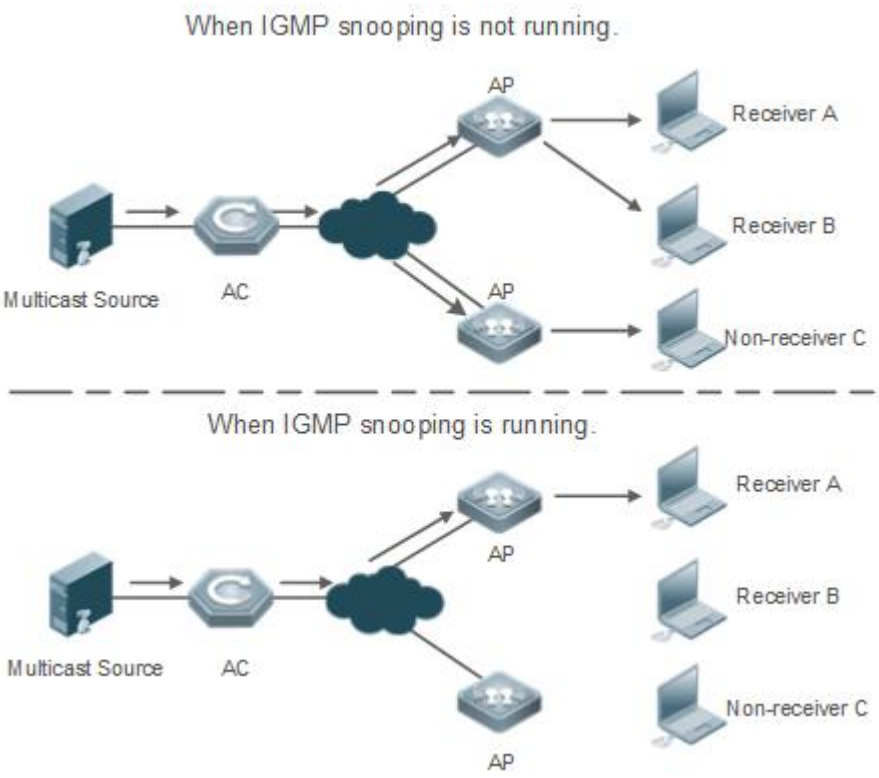
As shown in the following figure, when a Layer-2 device is not running IGMP snooping, IP multicast packets are broadcasted within the VLAN; when the Layer-2 device is running IGMP snooping, IP multicast packets are transmitted only to profile members.

Figure 13-1 Networking Topology of IP Multicast Forwarding within the VLAN Before and After IGMP Snooping Is Run on the Layer-2 Device



As shown in the following figure, when IGMP Snooping does not run on the AC and AP in wireless multicast environment, multicast packets are broadcasted within the VLAN of the AC and are broadcasted by the AP to all wireless ports. When IGMP Snooping runs on both the AC and AP, multicast packets of a known multicast profile are not broadcasted but forwarded to specific receivers.

Figure 13-2 Forwarding of IP Multicast Streams in a VLAN Before and After IGMP Snooping Is Enabled on the AC and AP



Protocols and Standards

- RFC4541: Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

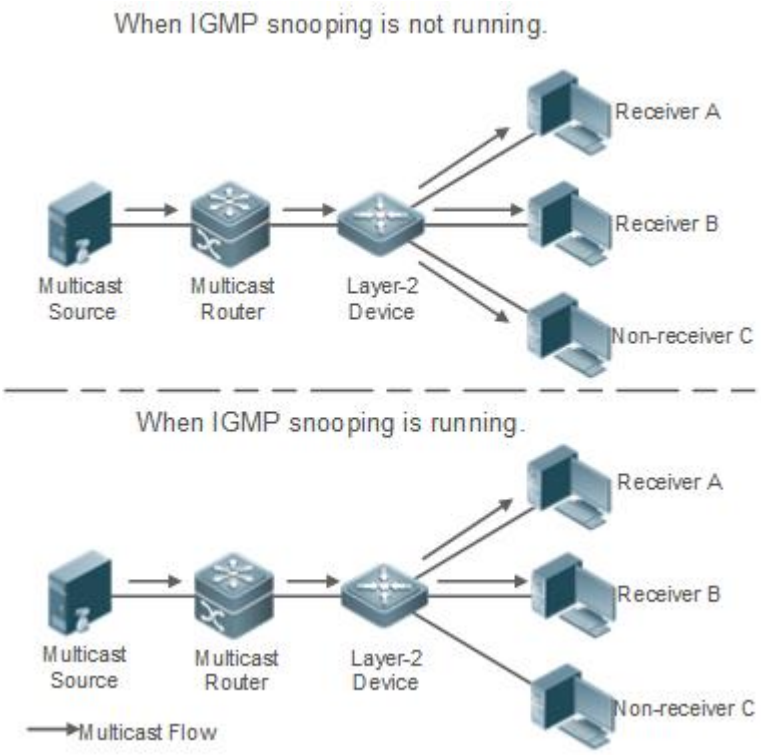
1.2 Applications

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 13-3 Networking Topology of Implementing Layer-2 Multicast Control (Multicast VLAN)



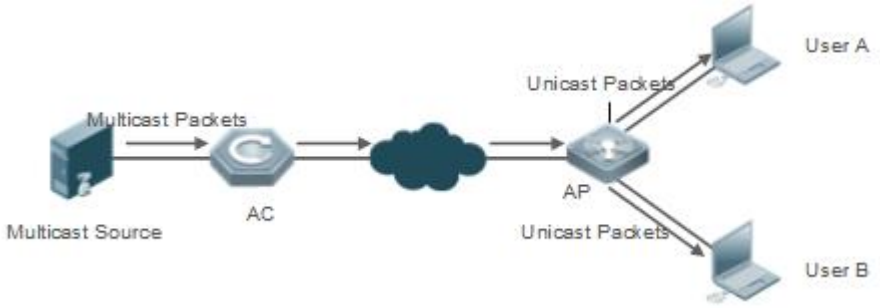
Deployment

- 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 13-4 Multicast-to-Unicast Conversion



Deployment

- Configure the multicast-to-unicast conversion function.

The function is available only in wireless multicast scenarios.

1.3 Features

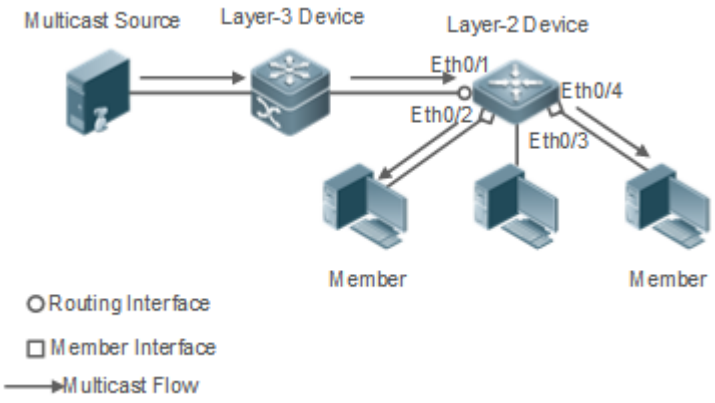
Basic Concepts

Multicast Router Ports and Member Ports

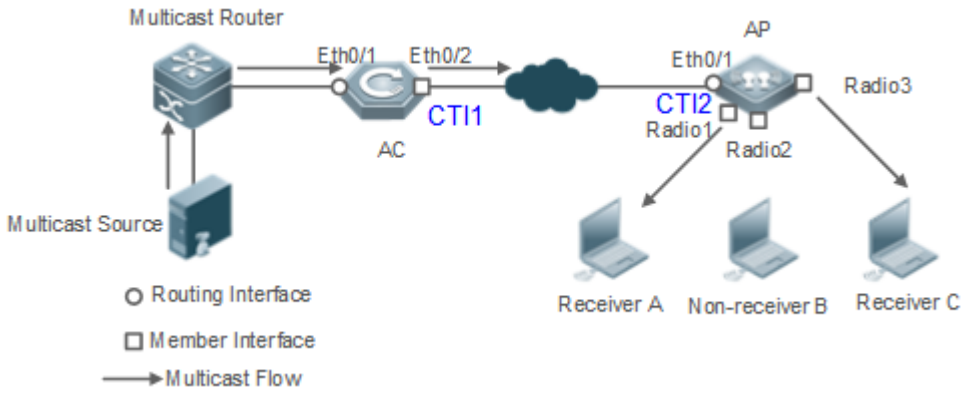
IGMP snooping is VLAN-based. The ports involved refer to the member ports within the VLAN.

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. As shown in the following figure, when IGMP snooping is run on a Layer-2 device, multicast traffic enters the multicast router port and exits from the member ports.

Figure 13-5 Networking Topology of Two IGMP Snooping Ports



- Multicast router port: The location of the multicast source is directed by the port on the Layer-2 multicast device which is connected to the multicast router (Layer-3 multicast device): By listening to IGMP packets, the Layer-2 multicast device can automatically detect the multicast router port and maintain the port dynamically. It also allows users to configure a static router port.
- Member port: The port is on a Layer-2 multicast device and is connected to member hosts. It directs the profile members. It is also called the Listener Port. By listening to IGMP packets, the Layer-2 multicast device can automatically detect the member port and maintain the port dynamically. It also allows users to configure a static member port.
- Figure 13-6 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.

Enabling Dynamic Router Port Learning

Dynamic router port learning is enabled by default.

Run the **no ip igmp snooping mrouter learn pim-dvmrp** command to disable dynamic router port learning.

Run the **no ip igmp snooping vlan** *vid* **mrouter learn pim-dvmrp** command to disable dynamic router port learning for designated VLANs.

Configuring the Aging Time of a Dynamic Member Port

The default aging time is 260s.

When a dynamic member port receives a Report packet, the aging timer of the port is enabled or reset, and the aging time is the maximum response time of the dynamic member port.

Run **ip igmp snooping host-aging-time** to configure the aging time of the dynamic member port.

Configuring the Maximum Response Time of a Query Packet

The maximum response time of a query packet is not configured by default and the maximum response time carries by the query packet is used.

Run **ip igmp snooping query-max-response-time** to configure the maximum response time of a query packet.

1.3.2 IGMP Snooping Working Modes

A device running in the 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** *num* **querier** command to enable the querier function for specific VLANs.

Specifying the IGMP Version for a Querier

By default, a querier runs IGMPv2.

Run the **ip igmp snooping querier version** command to configure the global querier version.

Run the **ip igmp snooping vlan querier version** command to specify the querier version for specific VLANs.

Configuring the Source IP Address of a Querier

By default, the source IP address of a querier is 0.

Run the ip igmp snooping querier address command to enable global source IP addresses of queriers.

Run the ip igmp snooping vlan querier address command to specify the source IP addresses of the queriers on specific VLANs.

Configuring the Query Interval of a Querier

By default, the query interval of a querier is 60s.

Run the **ip igmp snooping querier query-interval** command to enable the global query interval of queriers.

Run **ip igmp snooping vlan** *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 timer expiry** command to configure the maximum response time of the query packets sent by global queriers.

Run the **ip igmp snooping vlan queriertimer expiry** command to specify the maximum response time of the query packets sent by the queriers on specific VLANs.

Configuring the Aging Time of a Querier

By default, the aging time of a querier is 125s.

Run the **ip igmp snooping querier max-response-time** command to configure the aging time of global queriers.

Run the **ip igmp snooping vlan** *vid* **querier max-response-time** 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 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 **ip multicast wlan** command to enable the global multicast function. After global multicast is enabled, when an AC receives multicast packets, it conducts CAPWAP encapsulation on the multicast packets and sends the packets to the AP associated with the AC in CAPWAP unicast mode.

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.

In ap-config mode on an AC, run the **igmp snooping mcast-to-unicast enable** command to enable multicast-to-unicast conversion.

In ap-config mode on an AC, run the **no igmp snooping mcast-to-unicast enable** command to disable multicast-to-unicast conversion, or on a fat AP.

Configuring the Multicast Range for Multicast-to-Unicast Conversion

By default, multicast-to-unicast conversion is available to all multicast profiles.

Use AC as an example. In ap-config mode, run the **igmp snooping mcast-to-unicast group-range** command to configure the profile address range for multicast-to-unicast conversion.

In ap-config mode, 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.

Use AC as an example. In ap-config mode, 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.

In ap-config mode, 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.

Use AC as an example. In ap-config mode, run the **igmp snooping ignore-query-timer** command to ignore the port aging timer resetting for query packets.

In ap-config mode, 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	⚠ 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 *vlan-id* **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.
	igmp snooping host-aging-time *time*	Configures the aging time of a dynamic member port.
	ip igmp snooping fast-leave enable	Enables the immediate-leave function for a dynamic member port.
	igmp snooping query-max-response-time *time*	Configures the maximum response time of an IGMP query packet.
	ip igmp snooping query-max-response-time *time*	Configures the maximum response time of an IGMP query packet.

	ip igmp snooping suppression enable	Enables IGMP Report packet suppression.
Configuring 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 *num*	Configures the query interval of queriers globally.
	ip igmp snooping vlan *vid* **querier query-interval** *num*	Configures the query interval for a querier of a VLAN.
	ip igmp snooping querier max-response-time *num*	Configures the maximum response time for query packets globally.
	ip igmp snooping vlan *vid* **querier max-response-time** *num*	Configures the maximum response time of query packets for a VLAN.
	ip igmp snooping querier timer expiry *num*	Configures the aging timer for queriers globally.
	ip igmp snooping vlan *vid* **querier timer expiry** *num*	Configures the aging timer for a querier of a VLAN.
Configuring Multicast-to-Unicast Conversion	**igmp snooping mcast-to-unicast enable**	Enables multicast-to-unicast conversion.
	ip igmp snooping mcast-to-unicast enable	Enables multicast-to-unicast conversion.
	igmp snooping mcast-to-unicast group-range *ip-addr ip-addr*	Configures an AP's maximum multicast range for multicast-to-unicast 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.
	igmp snooping mcast-to-unicast max-group *group-num*	Configures an AP's maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion.
	ip igmp snooping mcast-to-unicast max-group *group-num*	Configures an AP's maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion.
Optimizing the Wireless Multicast Environment	**igmp snooping ignore-query-timer**	Configures the function of ignoring port aging timer resetting for query packets.

	ip igmp snooping ignore-query-timer	Configures the function of ignoring port aging timer resetting for query packets.

1.4.1 Configuring Basic IGMP Snooping Functions

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 Description	N/A
Command Mode	Global configuration mode
Usage Guide	After this command is executed, IGMP snooping will be run on all VLANs. By default, IGMP snooping is disabled.

↘ Disabling IGMP Snooping for a VLAN

Command	**no ip igmp snooping vlan** *num*
Parameter Description	N/A
Command	Global configuration mode

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

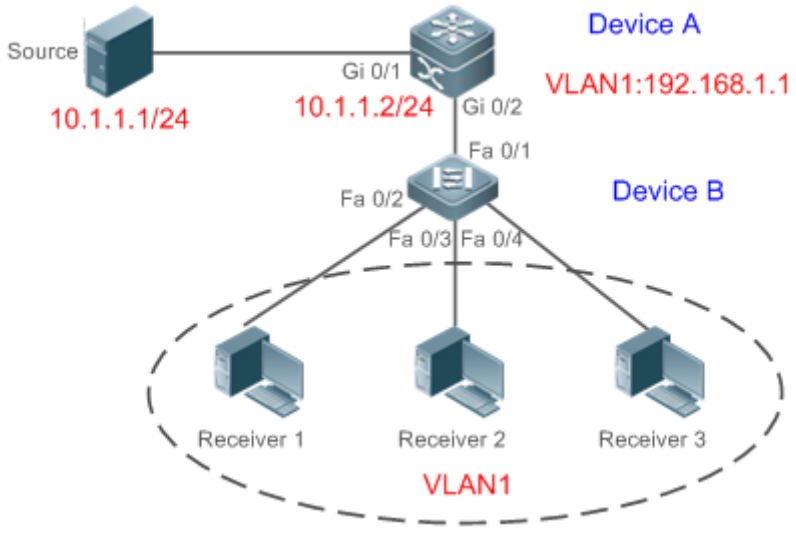
Command	**show ip igmp snooping gda-table**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode
Usage Guide	This command is used to verify that the ports include only those connecting member hosts.

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 1-7**	
	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 Fa0/2. ● Check whether the IGMP snooping working mode is IVGL.
B	B# show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*,224.1.1.1, 1): VLAN(1) 2 OPORTS: FastEthernet 0/1(M) FastEthernet 0/2(D) B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Disable IGMP Global Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds) vlan 1 ------------- IGMP Snooping state: Enable

	Multicast router learning mode: pim-dvmrp IGMP Fast-Leave: Disabled IGMP VLAN querier: Disable IGMP VLAN Mode: STATIC

Common Errors

- The working mode of IGMP snooping is improper.

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.
- The aging time can be adjusted according to the IGMP query packet sending interval of the connected multicast routing device, which is generally set as the IGMP query packet sending interval *2 + IGMP last query response time of the multicast routing device.

Configuring the Maximum Response Time of a Query Packet

- Optional.
- You can configure the aging time based on network load.

Verification

- Run the **show ip igmp snooping mrouter** command to check whether the configured static router port has an "S" in the displayed configuration information.
- Run the **show ip igmp snooping gda** command to check whether the configured static member port is marked with an S.
- Run the **show ip igmp snooping** command to check whether Report packets suppression, immediate leave, router port learning, router port aging time, member port aging time, and the maximum response time of the Query packet take effect.

Related Commands

Configuring a Static Router Port

Command	**ip igmp snooping vlan** *vid* **mrouter interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	In IVGL mode, the configurations for the static router ports within all the VLANs can take effect.

Configuring a Static Member Port

Command	**ip igmp snooping vlan** *vid* **static** *group-address* **interface** *interface-type interface-number*
Parameter Description	*vid*: Indicates a VLAN. The value ranges from 1 to 4,094. *group-address*: Indicates a profile address. *interface-type interface-number*: Indicates an interface name.
Command Mode	Global configuration mode
Usage Guide	By default, no static member port is configured.

Enabling Report Packet Suppression

Command	**ip igmp snooping suppression enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	When Report packets suppression is enabled, only the first Report packet from a specified VLAN or profile is forwarded to the router port within a Query interval, and the following Report packets will not be forwarded to the router port, thereby reducing the quantity of packets on the network. Only the IGMPv1 and IGMPv2 Report packets can be suppressed, 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	*seconds*: Indicates the maximum response time.

Description	
Command Mode	Global configuration mode
Usage Guide	When an IGMP general Query packet is received, the multicast device will reset the aging time of all the dynamic member ports, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. When an IGMP profile-specific Query packet is received, the multicast device will reset the aging time of all the dynamic member ports of the specific profile, which is query-max-response-time. If the timer expires, the multicast device deems that no user host for receiving the multicast packet exists under the port, and will delete the port from the entry of IGMP snooping member port. This configuration takes effect after the next Query packet is received, and the timer in use will not be refreshed. The timer of an IGMPv3 profile-specific Query packet is not refreshed.

Displaying Router Ports

Command	**show ip igmp snooping mroute**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	If the router port is successfully configured, an "S" will be displayed in the port information.
	`Hostname(config)#show ip igmp snooping mrouter`
	`Multicast Switching Mroute Port`
	`  D: DYNAMIC`
	`  S: STATIC`
	`(*, *, 1):`
	`  VLAN(1)  1 MROUTES:`
	`    GigabitEthernet 0/1(S)`

Displaying the Information of Dynamic Router Port Learning

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Run the **show ip igmp snooping** command to display the aging time and learning status of the dynamic router port.
	`Dynamic Mroute Aging Time : 300(Seconds)`
	`Multicast router learning mode: pim-dvmrp`

Displaying the Information of a Member Port

Command	**show ip igmp snooping gda-table**
Parameter Description	N/A

Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	If the member port is successfully configured, an "S" will be displayed in the port information.
	`Hostname(config)#show ip igmp snooping gda-table`
	`Multicast Switching Cache Table`
	`D: DYNAMIC`
	`S: STATIC`
	`M: MROUTE`
	`(*, 224.1.1.1, 1):`
	`VLAN(1) 1 OPORTS:`
	`GigabitEthernet 0/1(S`

Displaying Other Parameters

Command	**show ip igmp snooping**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or interface configuration mode

Usage Guide	Run the **show ip igmp snooping** command to display the aging time of the router port, aging time of the dynamic member port, response time of the query packet, and Report packets suppression, and immediate leave.
	`IGMP Fast-Leave: Enable`
	`IGMP Report suppress: Enable`
	`Query Max Response Time: 20(Seconds)`
	`Dynamic Mroute Aging Time : 300(Seconds)`
	`Dynamic Host Aging Time : 260(Seconds)`

Configuration Example

Configuring a Static Router Port and Static Member Port

Configuration Steps	● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.

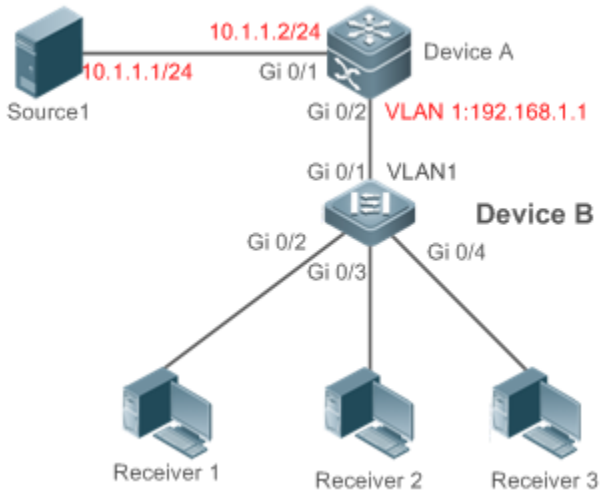
	`Hostname# configure terminal`
	`Hostname(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet 0/0`
	`Hostname(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface gigabitethernet 0/0`
	`Hostname(config)# end`

Verification	Run the **show ip igmp snooping mrouter** and **show ip igmp snooping gda-table** commands to check whether the configuration takes effect.

	`Hostname#show ip igmp snooping mrouter`
	`Multicast Switching Mroute Port`
	`D: DYNAMIC`
	`S: STATIC`

Configuration Steps	● Configure basic IGMP snooping functions. ● Configure a static router port and static member port.
	Hostname# configure terminal Hostname(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet 0/0 Hostname(config)# ip igmp snooping vlan 1 static 224.1.1.1 interface gigabitethernet 0/0 Hostname(config)# end
Verification	Run the **show ip igmp snooping mrouter** and **show ip igmp snooping gda-table** commands to check whether the configuration takes effect.
	(*, *, 1): VLAN(1) 1 MROUTES: GigabitEthernet 0/0(S) Hostname#show ip igmp snooping gda-table Multicast Switching Cache Table D: DYNAMIC S: STATIC M: MROUTE (*, 224.1.1.1, 1): VLAN(1) 1 OPORTS: GigabitEthernet 0/0(SM)

Enabling Report Packet Suppression

Scenario **Figure 1-8**	
	A is the multicast router and is connected directly to multicast Source 1. B is a Layer-2 device and is connected directly to the user host and multicast Source 2. Receiver 1, Receiver 2, and Receiver 3 are connected to VLAN 1.
Configuration Steps	● Configure the IP address and VLAN. (Omitted) ● Enable multicast routing on A and enable the multicast routing protocol on Layer-3 interface (Gi0/1 and VLAN 1). ● Enable IGMP snooping on B and select IVGL mode.

	● Enable Report packets suppression on B.
A	A# configure terminal A(config)# ip multicast-routing A(config)# interface gigabitethernet 0/1 A(config-if-GigabitEthernet 0/1)# ip pim sparse-mode A(config-if-GigabitEthernet 0/1)# exit A(config)# interface vlan 1 A(config-if-VLAN 1)# ip pim sparse-mode A(config-if-VLAN 1)# exit
B	B# configure terminal B(config)#ip igmp snooping ivgl B(config)# ip igmp snooping suppression enable
Verification	Check whether Receiver 1 and Receiver 2 are added to profile 239.1.1.1, and only the IGMP Report packets of profile 239.1.1.1 are forwarded from interface Gi0/1 of B.
B	B# show ip igmp snooping IGMP Snooping running mode: IVGL IGMP Snooping L2-entry-limit: 65536 Source port check: Disable Source ip check: Disable IGMP Fast-Leave: Disable IGMP Report suppress: Enable IGMP Globle Querier: Disable IGMP Preview: Disable IGMP Tunnel: Disable IGMP Snooping version: 2 IGMP Preview group aging time : 60(Seconds) Dynamic Mroute Aging Time : 300(Seconds) Dynamic Host Aging Time : 260(Seconds)

↘ Configuring Other Parameters

Configuration Steps	● Configure basic IGMP snooping functions. ● Enable Immediate-leave function. ● Disable router port learning. ● Configure the aging time of a router port. ● Configuring the aging time of a member port. ● Configure the response time of a Query packet.
	Hostname# configure terminal Hostname(config)# ip igmp snooping fast-leave enable Hostname(config)#ip igmp snooping dyn-mr-aging-time 200 Hostname(config)#ip igmp snooping host-aging-time 100 Hostname(config)#ip igmp snooping query-max-response-time 60 Hostname(config)# end
Verification	Run the **show ip igmp snooping** command to check whether the configuration is successful.
	Hostname#show ip igmp snooping

```
IGMP Snooping running mode: IVGL
IGMP Snooping L2-entry-limit: 65536
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Enable
IGMP Report suppress: Enable
IGMP Globle Querier: Disable
IGMP Preview: Disable
IGMP Tunnel: Disable
IGMP Snooping version: 2 Query Max Response Time: 60(Seconds)
IGMP Preview group aging time : 60(Seconds)
Dynamic Mroute Aging Time : 200(Seconds)
Dynamic Host Aging Time : 100(Seconds)
```

Common Errors

- Basic IGMP snooping functions are not configured or the configuration is not successful.

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** *ip-address*
Parameter Description	**vlan** *vid*: Specifies a VLAN. This configuration applies to all VLANs by default. *ip-address*: 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** | **2** }
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#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
```

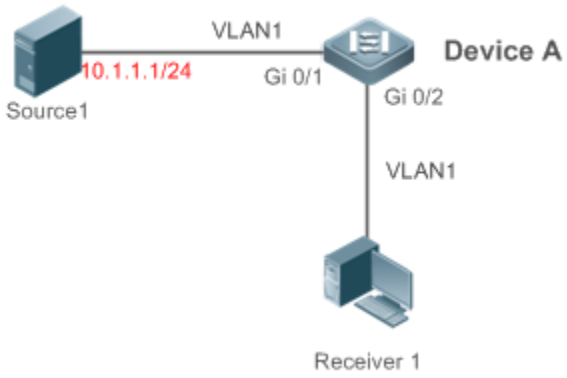
```
-----------------------------------------------------
admin state                 : Disable
admin version               : 2
source IP address           : 1.1.1.1
query-interval (sec)        : 60
max-response-time (sec)     : 10
querier-timeout (sec)       : 125
operational state           : Disable
operational version         : 2
```

Configuration Example

↘ Enabling the IGMP Querier Function

Scenario

Figure 13-9



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 ivgl
A(config)#ip igmp snooping querier
A(config)#ip igmp snooping querier address 10.1.1.1
A(config)#ip igmp snooping vlan 1 querier
```

Verification

Run the **show ip igmp snooping querier** command to check whether the querier of VLAN 1 takes effect.

A

```
A(config)#show ip igmp snooping querier
Vlan     IP Address          IGMP Version          Port
-----------------------------------------------------------
1        10.1.1.1              2                 switch

A(config)#show ip igmp snooping querier vlan 1

Vlan 1:   IGMP switch querier status
```

```
-------------------------------------------------------
elected querier is 10.1.1.1        (this switch querier)
-------------------------------------------------------
admin state                  : Enable
admin version                : 2
source IP address            : 10.1.1.1
query-interval (sec)         : 60
max-response-time (sec)      : 10
querier-timeout (sec)        : 125
operational state            : Querier
operational version          : 2
```

Common Errors

- The source IP address is not configured for the querier and the querier does not take effect.

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 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	**igmp snooping mcast-to-unicast enable**
Parameter Description	N/A
Command Mode	ap-config mode
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	**igmp snooping mcast-to-unicast group-range** *ip-address ip-address*
Parameter Description	*ip-address:* 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	**igmp snooping mcast-to-unicast max-group** *number*
Parameter Description	number: Indicates the maximum number of multicast profiles that are allowed to use multicast-to-unicast conversion. The value ranges from 1 to 64. The default value is 64.
Command Mode	ap-config mode on the AC or 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

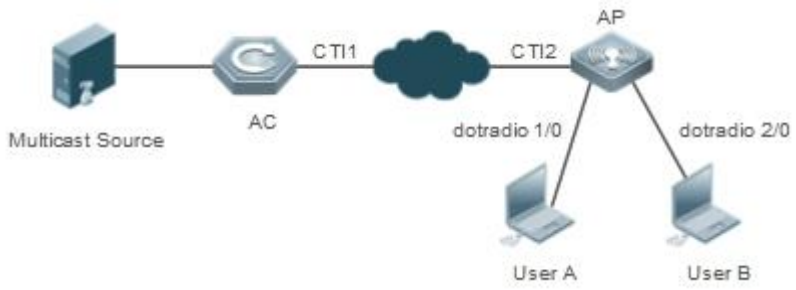
Command	show ip igmp snooping
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode

Usage Guide	If multicast-to-unicast conversion is configured successfully, the following information is displayed:
	`Hostname# 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 1-10	
	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 AC. ● Enable global multicast on the AC. ● Enable IGMP Snooping in global configuration mode.

	● Enable multicast-to-unicast conversion in ap-config mode. ● Configure the maximum multicast range for multicast-to-unicast conversion in ap-config mode. ● Configure the maximum number of multicast profiles that are allowed to support multicast-to-unicast conversion in ap-config mode.
A	A(config)# ip igmp snooping A(config)# ip multicast wlan A(config)# ip igmp snooping A(config)# ap-confing all A(config-ap)# igmp snooping mcast-to-unicast enable A(config-ap)# igmp snooping mcast-to-unicast group-range 233.1.1.1 233.255.255.255 A(config-ap)# 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# 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 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 or ap-config 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**
Displays the global switch of wireless multicast.	**show ip multicast wlan**

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**

Configuring AP Management

1. Configuring CAPWAP
2. Configuring Basic Configuration Management Service
3. Configuring APMG
4. Configuring ETH-MNG
5. Configuring AMMG
6. Configuring LED
7. Configuring iBeacon

1 Configuring CAPWAP

1.1 Overview

Control And Provisioning of Wireless Access Points (CAPWAP) is a protocol proposed to address the issue of large-scale access point (AP) deployment on the wireless local area network (WLAN).

On a fit AP network, the access controller (AC) manages all APs in a unified manner through CAPWAP. The AC delivers control polices to specified APs, eliminating the need to configure APs separately. CAPWAP is used to set up the control tunnel and the data tunnel between an AP and an AC. The control tunnel is used by ACs to configure APs, or by APs to send event notifications to ACs. The data tunnel is used to exchange data packets between APs and ACs.

Protocols and Standards

- RFC5415: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11
- RFC5417: Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option

1.2 Applications

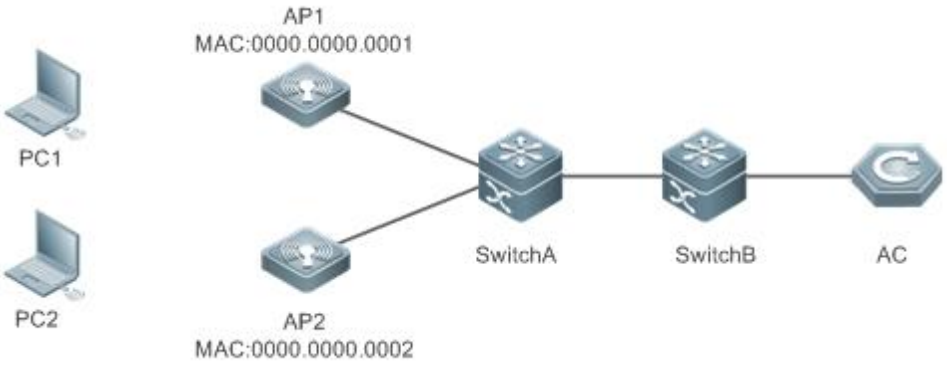
Application	Description
Dynamic CAPWAP Tunnel Setup	An AP accesses an AC through switches. The DCHP server is deployed on the switch connected to APs. The AP obtains the AC address dynamically through DHCP to set up a CAPWAP tunnel with the AC.
Static CAPWAP Tunnel Setup	An AP accesses an AC through switches. The static IP address of the AC is configured on the AP. The AP sets up a CAPWAP tunnel with the AC based on the configured static IP address of the AC.
AP Upgrade	After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in batches through CAPWAP.
Smart Upgrade	Smart upgrade is mainly applied in scenarios where high-reliability network is needed, such as warehouses and production networks that usually require uninterrupted services.

1.2.1 Dynamic CAPWAP Tunnel Setup

Scenario

APs access the AC through switches. The DCHP server is deployed on the switch connected to APs. The DHCP server is configured with a DHCP address pool and Option 138 that defines the IP address of the AC. The AP obtains the AC address and sets up a CAPWAP tunnel with the AC. As shown in Figure 1-1, the AC, switches (Switch A and Switch B), and APs (AP1 and AP2) are connected with each other through the trunk ports. PC1 is connected to AP1, and PC2 is connected to AP2.

Figure 1-1



Remarks	Switch: Indicates a switch. AC: Indicates a wireless access controller.

Deployment

- APs do not need to be configured one by one on a fit AP network. When an AP is powered on, the IP address must be obtained first. Therefore, a DHCP server must be deployed on the network. If the DHCP server is not deployed, the DHCP function of the AC is used to implement functions of the DHCP server.
- The AC communicates with the AP through the Layer 3 switch and the DHCP server must be configured with Option 138 that defines the IP address of the AC. After obtaining the IP address of the AC, the AP sets up a CAPWAP communication tunnel with the AC.
- On the AC, configure a loopback interface address, or run the **capwap ctrl-ip** *ip-address* command to configure the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interconnection between the AC and the IP address obtained by the AP.

1.2.2 Static CAPWAP Tunnel Setup

Scenario

The AP sets up a CAPWAP tunnels with the AC based on the configured static IP address of the AC. An AP accesses an AC through switches. The topology is the same as that shown in Figure 1-1.

Deployment

- Configure the static IP addresses of ACs. The AP will send a Discover Request messages to these static IP addresses to check whether ACs are valid. Upon receiving a Discover Response message, the AP selects an AC and sets up a CAPWAP tunnel with the AC.
- On the AC, configure a loopback interface address as the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interconnection between the AC and the IP address obtained by the AP.

1.2.3 AP Upgrade

Scenario

The AP obtains the AC address based on the configured static IP address of the AC or from the DHCP server, and sets up a CAPWAP tunnel with the AC. The AP accesses the AC through switches. The topology is the same as that shown in Figure 1-1.

Deployment

- On the AC, configure an IP interface address as the source address for setting up a CAPWAP tunnel.
- Configure a route to implement interconnection between the AC and the IP address obtained by the AP.
- On the AC, activate the AP software that is stored locally.

1.2.4 Smart Upgrade

Scenario

Smart upgrade is mainly applied in scenarios where high-reliability network is needed, such as warehouses and production networks that usually require uninterrupted services.

Deployment

- Activate the .bin file to be upgraded on the AC.
- Configure the upgrade mode in AP group configuration mode on the AC.
- Configure scheduled upgrade time and upgrade mode in AP group configuration mode on the AC.

1.3 Features

Basic Concepts

↘ STA, AP, and AC

STA: It is a wireless workstation that is equipped with the wireless network interface card (NIC), such as a laptop computer or a mobile phone.

AP: It is a wireless access point that provides radio signals so that the STA can access the wireless network.

AC: It is a wireless access controller that provides wireless connection and related service functions.

↘ Control Tunnel and Data Tunnel

Control tunnel: It is used by ACs to configure APs, or by APs to send event notifications to ACs.

Data tunnel: It is used to exchange data packets between APs and ACs.

↘ AC Discovery

An AP can send a Discover Request message by means of broadcast, multicast, DHCP, DNS, or static configuration to discover ACs. Upon receiving a Discover Response message, the AP selects the optimal AC and sets up a CAPWAP tunnel with the AC.

↘ Datagram Transport Layer Security (DTLS)

The CAPWAP control tunnel uses the DTLS protocol for key negotiation and encryption.

Options

The option field sent by the DHCP server can carry the IPv4 or IPv6 address of an AC. The AP obtains the AC address from the option field sent by the DHCP server.

The AP can obtain the IP address of an AC using Option 138 or Option 43, or obtain the IPv6 address of an AC using Option 52. When configuring the DHCP server of the AP, configure the related options that defines the IP address of the AC. Otherwise, the AP cannot discover the AC through DHCP discovery.

Option 138 and Option 52 are standard formats defined in RFC5417. Option 43 is defined by vendors. Currently, Option 43 in the following formats can be parsed:

Format 1: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is Option 43 hex f10401010101.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   option-code   | option-length | Sub-opt Type   |   Sub-opt Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|          Server   Address                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: Indicates the option code. In this example, the option code is 43 in decimal format.

option-length: Indicates the length of the option data, excluding option-code and option-length.

Sub-opt Type: Indicates the sub-option type. In this example, the sub-option type is 0xF1, that is, 241 in decimal format.

Sub-opt Len: Indicates the length of the sub-option, which is equal to (number of addresses x 4).

Server Address: Indicates the server address.

Format 2: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is option 43 hex 8007000001010101.

```
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   option-code   | option-length | Sub-opt Type   |   Sub-opt Len   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|            PXE Server Type            | PXE Server Num|                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
         PXE Server   Address                          |       …          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

option-code: Indicates the option code. In this example, the option code is 43 in decimal format.

option-length: Indicates the length of the option data, excluding option-code and option-length.

Sub-opt Type: Indicates the sub-option type. In this example, the sub-option type is 0x80, that is, 128 in decimal format.

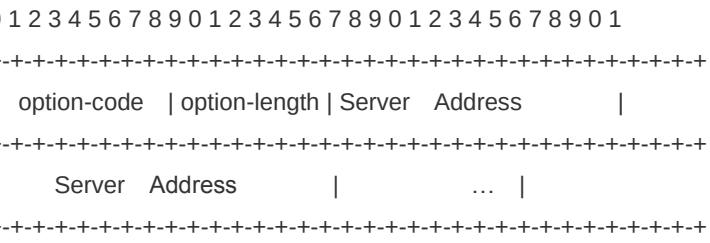
Sub-opt Len: Indicates the length of the sub-option, which is equal to (number of addresses x 4 +3).

Server Type: Indicates the server type. The value is 0x0000.

Server Num: Indicates the number of server addresses.

Server Address: Indicates the server address.

Format 3: Assume that the IP address of a specified AC is 1.1.1.1. The corresponding configuration is option 43 hex 01010101.



option-code: Indicates the option code. In this example, the option code is 43 in decimal format.

option-length: Indicates the length of the option data, excluding option-code and option-length.

Server Address: Indicates the server address.

Overview

Feature	Description
AC Discovery	The AP discovers potential ACs.
CAPWAP Tunnel Setup	The AP selects the optimal AC and sets up a CAPWAP tunnel with the AC.
AP Upgrade	After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in batches.
Data Data Forwarding over the Tunnel	After a CAPWAP tunnel is set up between an AC and each AP, data packets can be exchanged over the data tunnel.
Self-balancing Based on VAC	When a switch fails to balance load, self-balancing based on virtual AC (VAC) can be enabled to allow APs and STAs to evenly access the member ACs on the VAC network.

1.3.1 AC Discovery

An AP discovers potential ACs by sending a Discovery Request message.

Working Principle

As soon as an AP is connected to the network, the AP starts to discover ACs. The AP sends a Discovery Request message by means of broadcast, multicast, or unicast. If the AP unicasts a Discovery Request message, the AP obtains the IP address list of the AC through the DHCP server, DNS, or static IP configuration.

1.3.2 CAPWAP Tunnel Setup

The AP selects the optimal AC and sets up a CAPWAP tunnel with the AC.

Working Principle

The AP sends a Discovery Request message to ACs. ACs that receive the Discovery Request message reply a Discovery Response message to the AP respectively. The AP selects the optimal AC and sets up a DTLS connection with this AC.

After the DTLS connection is successfully set up, the AP sends a Join Request message. The AC replies a Join Response message to confirm that the AP is connected and starts to provide services for this AP.

1.3.3 AP Upgrade

After a CAPWAP tunnel is set up between an AC and each AP, the AC upgrades APs in batches.

Working Principle

After an AP joins an AC, if the AP firmware version expires, the firmware needs to be upgraded. The AP downloads the latest firmware version from the AC, restarts after upgrade, and reinitiates an AC discovery process. If the AP firmware is the latest version, the AP downloads configuration parameters from the AC and starts running. Figure 1-2 shows the flowchart of the working principle.

Figure 1-2

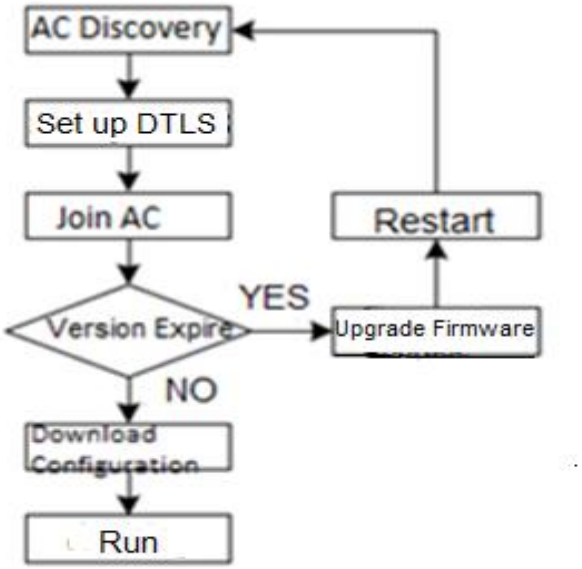
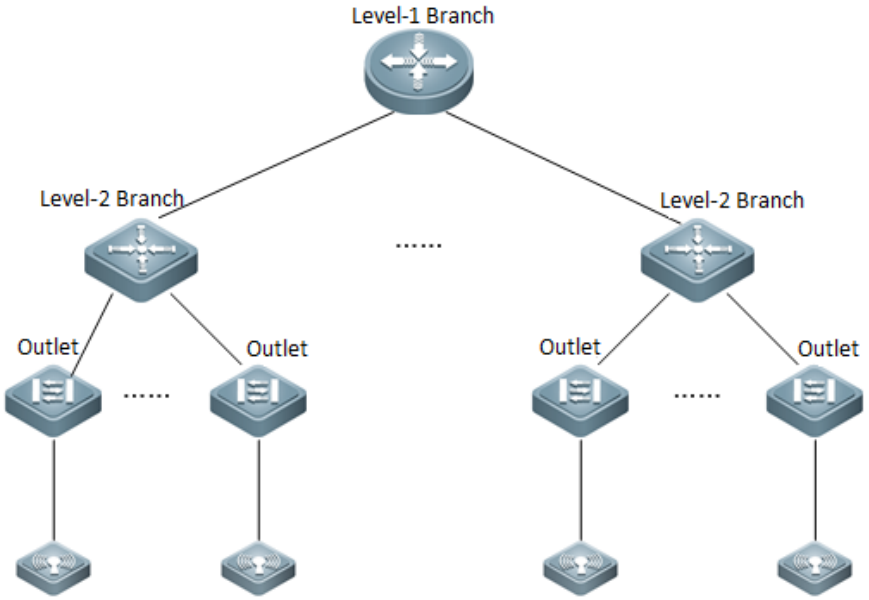


Figure 1-3 shows the typical scenario where the bandwidth is limited for upgrade.

Figure 1-3



The following explains the configuration method for upgrading APs in a bank. Assume that the bank consists of one level-1 branch and multiple level-2 branches, and each branch has hundreds of outlets. One AP is deployed in one outlet, and the AC is deployed in the level-1 branch. The bandwidth between the level-1 bank and the level-2 bank is 20 Mbps, and the bandwidth between the level-2 bank and the outlet is 2 Mbps. To avoid affecting normal services of the bank, the bandwidth occupied by the AP upgrade process cannot exceed 50% of the total available bandwidth. Assume that there are eight level-2 branches, eight upgrade groups are configured on the AC, and APs of outlets under each level-2 branches are added to the corresponding upgrade group. For each AP, the maximum available bandwidth is 1 Mbps. Therefore, a bandwidth of 128 kbps (1 Mbps = 1024 kbps) should be configured for each AP. Under each level-2 branch, up to 10 APs can be upgraded concurrently (bandwidth: 10 x 1 Mbps = 10 Mbps). In addition, you are advised to configure the maximum number of APs that can be concurrently upgraded by an AC as the number of upgrade groups multiplied by the number of APs that can be upgraded concurrently in an upgrade group, that is, 80.

1.3.4 Smart Upgrade

Smart upgrade is a solution to improve reliability during service upgrade. Users can set the upgrade time and mode as required, maximizing upgrade reliability.

Working Principle

The smart upgrade solution allows users to set a scheduled upgrade time and upgrade mode, improving reliability and reducing costs during upgrade. (1) Scheduled upgrade time: Users can schedule an off-peak time for upgrade to avoid automatic upgrades during service peak hours, reducing upgrade costs. (2) Upgrade mode: Forced upgrade and smart upgrade are provided. Forced upgrade mode is adopted to quickly upgrade APs. In smart upgrade mode, an optimal AP is selected from the AP group for upgrade. After the upgrade is completed, another optimal AP is further selected to continue upgrade, thereby avoiding service crash caused by simultaneous upgrades of multiple APs in the area.

1.3.5 Data Forwarding over the Tunnel

After a CAPWAP tunnel is set up between an AC and each AP, data packets can be exchanged over the data tunnel.

Working Principle

A control tunnel and a data tunnel between APs and ACs are set up through CAPWAP. The control tunnel is used by ACs to configure APs, or by APs to send event notifications to ACs. The control tunnel must be encrypted. The data tunnel is used to exchange the 802.11 or 802.3 frames between APs and ACs. When running on the IPv4 protocol stack, the CAPWAP uses the UDP for data transmission. When running on the IPv6 protocol stack, the CAPWAP uses the UDP over the control tunnel, and UDP or UDP-lite over the data tunnel for data transmission.

1.3.6 Self-balancing Based on VAC

Working Principle

To evenly distribute APs and STAs in a VAC scenario, configure load balancing policies on the switch directly connected to the AC for load balancing. However, when the switch fails to balance load, frequent AP migration may occur, which affects network use. In this case, self-balancing based on VAC can be enabled, so that APs and STAs can evenly access the member ACs on the VAC network.

1.4 Configuration

Configuration	Description and Command	
Configuring the AC Location	⚠ (Optional) It is used to configure the location of an AC.	
	location	Configures the location of an AC so that the physical location of the AC can be displayed.
Configuring the Version Number	⚠ (Optional) It is used to configure the version number.	
	set-version	Configures the version number,
Configuring the AP Location	⚠ (Optional) It is used to configure the location of an AP.	
	location	Configures the location of an AP so that the physical location of the AP can be displayed.
Configuring AP Time Synchronization	⚠ (Optional) It is used to enable the AP to synchronize the time with the AC.	
	timestamp	Enables the AP to synchronize the time with the AC.
Configuring an AP to Access an AC	⚠ (Optional) It is used to configure an AP to set up a CAPWAP tunnel with an AC.	
	ac-control disable	Configures an AP to access an AC.
	ac-domain-name	Configures the DNS domain name of the AP, which is used to obtain the address of the AC.
	acip ipv4	Configures the static IP address of the AC accessed by the AP.

	acip ipv6	Configures the static IPv6 address of the AC accessed by the AP.
	ip address	Configures the static IP address, subnet mask, and gateway.
	ipv6 address	Configures the static IPv6 address and gateway.
	ipv6 enable	Enables the CAPWAP IPv6 function on the AP.
Configuring an AP to Execute a Command	(Optional) It is used to configure an AP to set up a CAPWAP tunnel with an AC.	
	exec-cmd	Configures an AP or the entire AP group to execute the **ap-config** command.
Configuring AP Upgrade	(Optional) It is used to configure AP upgrade.	
	ap-serial	Creates the name of an AP product series and specifies the AP product models that belong to this series.
	ap-image	In AP configuration mode, configures the specified AP upgrade version. In AC configuration mode, configures the specified AP software version that should be used by a specified AP product series for the upgrade, or sets the adaptive upgrade mode.
	active-bin-file	Activates the AP software version file.
	capwap upgrade max-concurrent	Configures the maximum number of APs that can be concurrently upgraded by the AC.
	capwap upgrade group	In AC configuration mode, creates a bandwidth control upgrade group.
	ap-upgrade band-width	In AP configuration mode, configures the bandwidth for centralized AP upgrade.
	ap-upgrade group	In AP configuration mode, adds APs to the bandwidth control upgrade group.
Configuring Smart Upgrade	**ap-image upgrade-mode**	In AP group configuration mode, configures the upgrade mode as smart upgrade or forced upgrade.
	ap-image upgrade-appoint	In AP group configuration mode, configures scheduled upgrade time. You can start upgrade immediately, stop upgrade immediately, perform upgrade at scheduled time and periods, and execute a specified quantity of upgrade cycles in the scheduled time period.
Configuring a Micro AP	(Optional) It is used to configure a micro AP.	
	slot	Configures the name of a micro AP in a specified slot by running the **slot** command.

Configuring the CAPWAP Control Address Address	(Optional) It is used to configure the control IP address of the CAPWAP tunnel. When this address is not configured, the address of the loopback interface is used as the control IP address by default.	
	capwap ctrl-ip	Configures the control IP address of the CAPWAP tunnel.
Configuring CAPWAP Fragmentation	(Optional) It is used to configure CAPWAP fragmentation.	
	capwap mtu	Configures the path maximum transmission unit (MTU) transmitted over the data tunnel of a specified AP. This function can be enabled through the **capwap fragment enable** command.
	capwap ctrl-mtu	Configures the path MTU transmitted over a control tunnel of a specified AP. It is enabled by the software by default and cannot be disabled.
	capwap fragment enable	Enables CAPWAP data tunnel fragmentation for a specified AP.
Configuring CAPWAP Encryption	(Optional) It is used to configure CAPWAP encryption.	
	capwap data-tunnel encryption	Configures data tunnel encryption for a specified AP.
	capwap dtls enable	Enables encryption on the CAPWAP control tunnel.
Configuring CAPWAP Access Control	(Optional) It is used to control the maximum number of APs that can concurrently go online.	
	capwap max-concurrent	Configures the maximum number of APs that can concurrently go online.
Configuring the Heartbeat Keepalive Interval of the CAPWAP Tunnel	(Optional) It is used to configure the heartbeat keepalive interval of the CAPWAP tunnel.	
	echo-interval	Configures the heartbeat keepalive interval of the CAPWAP tunnel.
Configuring the Maximum Number of CAPWAP Packet Retransmission Attempts	(Optional) It is used to configure the maximum number of CAPWAP packet retransmission attempts.	
	capwap max-retransmit	Configures the maximum number of CAPWAP packet retransmission attempts.
Configuring the AC Discovery Mode	(Optional) It is used to configure the AC discovery mode.	
	capwap discovery-type ac-referral	Configures an AC to allow an AP to discover the AC by using discovery packets of the referral type.
	capwap discovery-type all	Configures an AC to allow an AP to discover the AC by using any type of discovery packets.
	capwap discovery-type dhcp	Configures an AC to allow an AP to discover the AC by using discovery packets of the DHCP type.

	capwap discovery-type dns	Configures an AC to allow an AP to discover the AC by using discovery packets of the DNS type.
	capwap discovery-type static-config	Configures an AC to allow an AP to discover the AC by using discovery packets containing a statically configured AC address.
	capwap discovery-type unknown	Configures an AC to allow an AP to discover the AC by using other types of discovery packets.
Enabling Self-Balancing Based on VAC	⚠ (Optional) It is used to enable self-balancing based on VAC.	
	virtual-ac self-balance enable	Enables self-balancing based on VAC.
Configuring the Command Set File Delivered by the AC to the AP	**auto-cfg**	Configures the command set file delivered by the AC to the AP.

1.4.1 Configuring the AC Location

Configuration Effect

- Configure the locations of ACs to conveniently check the locations of ACs on the WLAN.

Notes

- The location is a string of 1 to 255 characters and cannot contain any space.

Configuration Steps

- (Optional) Configure the locations of ACs to conveniently check the locations of ACs when a large number of ACs exist on the network.
- Enter the AC configuration mode and run the **location** command to configure the AC location on the AC.
- Use the **no** form of this command to restore the default setting.

Command	**location** *location-string*
Parameter Description	*location-string*: Indicates the location of an AC. The location is a string of 1 to 255 characters and cannot contain any space.
Defaults	Hostname_COM
Command Mode	AC configuration mode
Usage Guide	The AC location is **Hostname_COM** by default. You can configure the location for each AC as required to conveniently check the AC location on the WLAN.

Verification

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

Configuration Example

↘ **Configuring the AC Location as computer-layer2**

Configuration	● Enter the AC configuration mode.

Steps	● Configure the AC location.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)# locationcomputer-layer2`
	● Use the **no** form of this command to restore the default setting.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)#no location`
Verification	Run the **show ac-config** command to display the current location of the AC.
AC	`Hostname#show ac-config` `ac location :Ac_COM`

Common Errors

- N/A

1.4.2 Configuring the Version Number

Configuration Effect

- Customize the firmware version.

Notes

- The customized version number contains a maximum of 63 characters.

Configuration Steps

- Optional.
- Run this command to configure the customized firmware version number.
- Use the **no** form of this command to restore the default setting.

Command	**set-version** *string*
Parameter Description	*string*: Indicates the customized version number.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	This command is used to configure the firmware version number of the AC and deliver the firmware version number to APs.

Verification

- Run the **show version** command to display the version number.

Configuration Example

Configuring the Customized Firmware Version Number as RGOS 10.4(2B17)-SP2

Configuration Steps	Enter the AC configuration mode. Configure the customized version number.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)# set-version RGOS 10.4(2B17)-SP2`
Verification	Run the **show version** command to display the version number.
AC	`Hostname#show version` `System software version : RGOS 10.4(2B17)-SP2`

Common Errors

- N/A

1.4.3 Configuring the AP Location

Configuration Effect

- Configure the location of an AP.

Notes

- The AP location is a string of 1 to 255 characters and cannot contain any space.

Configuration Steps

Configuring the AP Location

- Optional.
- Run the **location** command to configure the AP location.
- Enter the AP configuration mode and configure the AP location on the AC to conveniently check the physical location of the AP.

Command	**location** *location-string*
Parameter Description	*location-string*: Indicates the location of an AP. The location is a string of 1 to 255 characters and cannot contain any space
Defaults	Null
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** command to display the AP location.

Configuration Example

Configuring the Location of AP0001 as AP-company

Configuration Steps	● Enter the AP configuration mode on the AC. ● Configure the location of AP0001 as **AP-company**.
AC	`Hostname(config)# ap-config AP0001` `Hostname(config-ap)# location AP-company`
Verification	● Run the **show ap-config running** command to display the location of AP0001.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP0001`
	`location AP-company`
	`!`

Common Errors

- N/A

1.4.4 Configuring AP Time Synchronization

Configuration Effect

- Configure a specified AP or all APs in an AP group to synchronize the time with the AC.

Notes

- N/A

Configuration Steps

Configuring a Specified AP or All APs in an AP Group to Synchronize the Time with the AC

- Optional.
- To synchronize the time on the AP with that on the AC, enter the AP or AP group configuration mode on the AC and run the **timestamp** command.

Command	**timestamp**
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Check whether the time on the AC is the same as that on the AP.

Configuration Example

Configuring AP0001 to Synchronize the Time with the AC

Configuration Steps	● Enter the AP configuration mode on the AC. ● Configure AP0001 to synchronize the time with the AC.
AC	`Hostname(config)# ap-config AP0001` `Hostname(config-ap)# timestamp`
Verification	● Run the **show clock** command to display the time on the AP0001 and the AC.
AC	`Hostname#showclock` `16:41:05 UTC Thu, Oct 17, 2013`

Common Errors

- N/A

1.4.5 Configuring an AP to Access an AC

Configuration Effect

- Configure the static IP addresses of ACs. The AP will send a Discover Request messages to these static IP addresses to check whether ACs are valid. Upon receiving a Discover Response message, the AP select an AC and set up a CAPWAP tunnel with the AC.

Notes

- A fit AP is generally not configured. It can discover ACs by means of broadcast, unicast, DHCP, or DNS, or can join ACs based on the statically configured AC addresses.
- If the AP address is configured as the static address, the DHCP/DHCPv6 function will be disabled. In this case, the AC address cannot be obtained from the DHCP/DHCPv6 option. Therefore, before this command is configured, you need to configure the address of the connected AC in AP configuration mode so that the AP can discover and join the AC when the AP and the AC are not on the same subnet.
- If the current address of the AP is different from the address specified in the AC command, the AP static address will be updated and the CAPWAP tunnel will be re-established. If IPv6 is not enabled on the AP, the CAPWAP tunnel will not be re-established.
- If both IPv4 and IPv6 addresses of the AP are specified and IPv6 is enabled on the AP, the AP will discover the IPv4 and IPv6 ACs simultaneously.

Configuration Steps

Configuring the Static AC Address

- Optional.
- The AC address can be obtained through DHCP or DNS. Alternatively, the static AC address can be configured in AP configuration mode on the AC.
- When the AC address is obtained in static mode, run the **acip ipv4** or **acip ipv6** command to configure the static AC address.

Command	**acip ipv4***ip-address*[*ip-address*…]
Parameter Description	*ip-address*: Indicates the static IP address. Up to six static addresses can be configured.
Defaults	No static AC IP address is configured.
Command Mode	AP configuration mode on the AC
Usage Guide	N/A

Command	**acip ipv6** *ipv6-address*[*ipv6-address*…]
Parameter Description	*ipv6-address*: Indicates the static IP address. Up to six static addresses can be configured.
Defaults	N/A
Command Mode	AP configuration mode on the AC
Usage Guide	N/A

Configuring the Domain Name for the AP to Discover the AC

- (Optional) Run the **ac-domain-name** command to configure the domain name on the AC so that the AP can discover the AC based on the domain name.
- When the AC address is obtained in dynamic mode, configure the domain name on the AC. The IP address of the AC can be obtained based on the domain name.
- If the domain name is not configured, the AP cannot obtain the IP address of the AC through DNS.

Command	**ac-domain-name** *ac-domain-name*
Parameter Description	*ac-domain-name*: Indicates the domain name of the AC.
Defaults	ac. Hostname.com.cn
Command Mode	AP configuration mode or AP group configuration mode on the AC
Usage Guide	N/A

Configuring the Static IP Address of the AP

- Optional.
- On the AP, configure the static IPv4 or IPv6 address of the AP so that the AP can use the fixed IPv4 or IPv6 address to access the AC.

Command	**ip address** *ip-address network-mask gateway*
Parameter Description	*ip-address*: Indicates the IP address of the AP. *network-mask*: Indicates the subnet mask of the AP. *gateway*: Indicates the gateway of the AP.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	An AP can obtain an IP address through the static configuration or DHCP. If the static IP address is not

	configured on the AP, the AP obtains the address through DHCP and joins the AC. In this case, you can run this command to configure the static IP address of the AP so that the address can remain unchanged after the AP is restarted.

Configuring the Static IPv6 Address of a Specific AP

- Optional.

Command	**ipv6 address** *ipv6-address-with-mask gateway*
Parameter Description	*ipv6-address-with-mask*: Indicates the IPv6 address of the AP. The format is X:X:X:X::X/24. *gateway*: Indicates the IPv6 gateway of the AP.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	When IPv6 is enabled, the AP can obtain an IPv6 address through the static configuration or DHCPv6. If the static IPv6 address is not configured on the AP, the AP obtains the address through DHCPv6 and joins the AC. In this case, you can run this command to configure the static IPv6 address of the AP so that the address can remain unchanged after the AP is restarted.

Configuring the AP to Support IPv6 Access

- Optional.
- Run this command to control whether an AP sets up a CAPWAP IPv6 tunnel.
- If a CAPWAP IPv6 tunnel needs to be set up, run the **ipv6 enable** command in AP configuration mode on the AC to support establishment of an IPv6 tunnel.

Command	**ipv6 enable**
Parameter Description	N/A
Defaults	IPv6 is disabled on the AP.
Command Mode	AP configuration mode
Usage Guide	If the configuration causes a change in the IPv6 support status of the AP, the AP re-establishes the CAPWAP tunnel. When IPv6 is enabled on the AP and the AP is configured with both static IPv4 and IPv6 addresses, the AP attempts to discover the IPv4 and IPv6 ACs simultaneously during re-establishment of the CAPWAP tunnel. Among discovered ACs, the AP does not necessarily select and join an IPv6 AC. To ensure that the AP selects and joins an IPv6 AC, delete the static IPv4 address of the AP and retain only the static IPv6 address of the AP before IPv6 is enabled on the AP.

Configuring the Fit AP to Access an AC

- Optional.
- Enable an AC.

Command	**no ac-control disable**
Parameter Description	N/A
Defaults	Enabled.

Command Mode	AC configuration mode
Usage Guide	The device can serve only as a switch, a gateway, or an AC on the network. When the device serves only as a switch or gateway, the fit AP is expected to access the actual AC but not the device. This command can be used to control the access of the AP. When the AC function is disabled, the device disables the CAPWAP ports (such as ports 5246 and 5247) and stops listening to the corresponding ports.

Verification

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

Configuration Example

Configuring the AP to Obtain the IP Address of the AC Based on the Static IPv4 Address

Configuration Steps	• Enter the AP configuration mode on the AC. • Set the static IP address of the AC accessed by the AP to 192.168.1.1. • Set the static IP address of the AP to 1.1.1.1, subnet mask to 255.255.255.0, and gateway to 1.1.1.2.

AC	`Hostname(config)# ap-config AP0001`
	`Hostname(config-ap)# acip ipv4 192.168.1.1`
	`Hostname(config-ap)# ip address 1.1.1.1 255.255.255.0 1.1.1.2`

Verification	• Display the AP configuration.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP0001`
	`acip ipv4 192.168.1.1`
	`ip address 1.1.1.1 255.255.255.0 1.1.1.2`
	`!`

Enabling the AP to Obtain the IP Address of the AC Based on the Domain Name

Configuration Steps	• Enter the AP configuration mode on the AC. • Set the domain name of the AC to **Hostname-ac**.
AC	`Hostname(config)# ap-config AP0001` `Hostname(config-ap)# ac-domain-name Hostname-ac`
Verification	• Display the AP configuration.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP0001`

Configuration Steps	● Enter the AP configuration mode on the AC. ● Set the domain name of the AC to **Hostname-ac**.
AC	`Hostname(config)# ap-config AP0001` `Hostname(config-ap)# ac-domain-name Hostname-ac`
Verification	● Display the AP configuration.
	`ac-domain-name Hostname.ac` `!`

Enabling IPv6 on the AP

Configuration Steps	● Enter the AP configuration mode on the AC. ● Enable IPv6 on the AP.
AC	`Hostname(config)# ap-config AP0001` `Hostname(config-ap)# ipv6 enable`
Verification	● Display the AP configuration.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP0001`
	`ipv6 enable`
	`!`

Configuring the Fit AP to Access the All-in-One AC

Configuration Steps	● Enter the AC configuration mode. ● Configure the fit AP to access the all-in-one AC.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)#no ac-control disable`
Verification	● Display the AP configuration.

AC	`Hostname#show ap-config running`
	`!`
	`ac-controller`
	` no ac-control disable`

Common Errors

- N/A

1.4.6 Configuring an AP to Execute a Command

Configuration Effect

- (Optional) On the AC, configure an AP to execute a command.
- (Optional) On the AC, configure all APs in an AP group to execute a command.

Notes

- N/A

Configuration Steps

Configuring an AP to Execute a Command

- (Optional) Enter the AP configuration mode.
- On the AC, configure the AP to execute a command.

Command	**exec-cmd mode** *exec-mode* **cmd** *exec-cmd* [**slot** { *id* | **all** } | **once**]
Parameter Description	*exec-mode*: Indicates the mode in which a command is executed on the AP. *exec-cmd*: Indicates the command to be executed on the AP. *id* : Indicates the slot ID of the micro AP connected to the i-Share+ AP. **all**: Indicates all micro APs connected to the i-Share+ AP. **once**: Indicates that the command is executed only once and is not saved.
Defaults	N/A
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	Some commands are supported currently only on the AP and they are unavailable on the AC. To configure the commands for APs on the AC, run the **exec-cmd** command. To cancel or change the configuration of the **exec-cmd** command, run the **no exec-cmd** command to remove the configuration and then run the **exec-cmd** command to cancel or change the required configuration. If **ap-config all** and **ap-config** are configured simultaneously, for online APs, the later configuration will take effect; for offline APs, **ap-config** has a higher priority than **ap-config all**. The AC can deliver the corresponding command to a micro AP by expanding the **exec-cmd** command. After delivery, run the command on the micro AP. Note: If a dedicated command is used on an AC to deliver configurations to an AP, do not use this command to deliver the configurations. Otherwise, conflicts occur.

Verification

- Log in to the AP to check whether the configuration takes effect. On the AC, run the **show run** or **show ap-config run** command to check whether the configuration takes effect.

Configuring APs in an AP Group to Execute a Command

- (Optional) Enter the AP group configuration mode.

- Configure all APs in an AP group to execute a command.

Command	**exec-cmd** *exec-cmd*
Parameter Description	*exec-cmd*: Indicates the command to be executed on all APs in an AP group.
Defaults	N/A
Command Mode	AP group configuration mode.
Usage Guide	Some configuration commands are available only in AP configuration mode and they are unavailable in AP group configuration mode. To configure such a command for all APs in an AP group, run the **exec-cmd** command in the AP group. Note that the configuration is not saved in AP group configuration mode, that is, the command is executed only once on all APs in the current AP group. If the configuration already exists in AP configuration mode, the original configuration will be overridden when the command is executed in AP group configuration mode.

Verification

- Run the **show ap-config run** command to check whether the configuration of the APs in an AP group takes effect.

Configuration Example

↘ Disabling the Eweb Function for an AP on the AC and Configuring Bluetooth iBeacon for all APs in an AP Group

Configuration Steps	• On the AC, disable the Eweb function for APs. • On the AC, enable the Eweb function for APs. • Enable Bluetooth iBeacon for all APs in an AP group. • Disable the Eweb function for all APs in the AP group.
AC	Hostname(config)#ap-config AP1 Hostname(config-ap)# exec-cmd mode configure cmd "no enable service web-server all" Hostname(config-ap)# no exec-cmd mode configure cmd "no enable service web-server all" Hostname(config-ap)# exec-cmd mode configure cmd "enable service web-server all" Hostname(config)#ap-group default Hostname(config-group)#exec-cmd ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff Hostname(config-group)#exec-cmd exec-cmd mode configure cmd "no enable service web-server all"
Verification	• On the AC, check whether the configuration takes effect.

AC	Hostname#show ap-config running ap-config AP1 exec-cmd mode configure cmd "no enable service web-server all" ibeacon uuid ffffffffffffffffffffffffffffffff major ffff minor ffff

Common Errors

- The configuration of the **exec-cmd** command is changed, the **no exec-cmd** command is not executed to delete original configuration, or the **exec-cmd** command is not re-executed to cancel the configuration.

1.4.7 Configuring AP Upgrade

Configuration Effect

- Upgrade the AP software version through configuration on the AC.

Notes

- Perform configuration to activate the AP software version file. This command loads the **.bin** file to the memory only when the AP needs to be upgraded. When no AP needs to be upgraded, the **.bin** file will be automatically removed from the memory.
- During the adaptive upgrade, the transitional version between RGOS 10 and RGOS 11 cannot be used to upgrade an AP equipped with the RGOS 10 system.
- When the bandwidth is limited, use the bandwidth control function for the upgrade.

Configuration Steps

Creating the AP Series

- (Optional) Run the **ap-serial** command to configure an AP product series on the AC.
- To upgrade the AP software version through the AC, you need to first configure the AP hardware version and product models for a specified product series on the AC.
- An AP software version is applicable to a series of APs. You can configure the AP hardware version and product models for a specified product series, and use the software version to upgrade specified AP models.

Command	**ap-serial** *serial-name ap-pid1* [*ap-pid2 ... ap-pidn*] [**hw-ver** *hardware-version*]
Parameter Description	*serial-name*: Indicates the name of the AP series to be created. *ap-pid1* [*ap-pid2 ... ap-pidn*]: Lists the product models to be added to the AP series. *hardware-version*: Specifies the AP hardware version.
Defaults	No AP series is configured.
Command Mode	AC configuration mode
Usage Guide	N/A

Activating the AP Software Version File

- (Optional) Run the **active-bin-file** command to activate an AP software version on the AC.

- To upgrade the AP software version through the AC, you need to activate the AP software version on the AC first.
- Only an activated AP software version can be used for the upgrade.

Command	**active-bin-file** *filename*[**rgos10**]
Parameter Description	*filename*:Specifies the name of a software version. The name may contain a path prefix (**flash:**,**tmp:**, or**usb0:**), followed by a real file name. The maximum length of a file name is 64 bytes. **rgos10:** Indicates that a transitional version between 10.X and 11.X is activated. It is applicable only to the AP software version.
Defaults	The AP software version is not activated.
Command Mode	AC configuration mode
Usage Guide	1. To download a software version from the AC to upgrade an AP, you need to activate the version file first. The RGOS 10 system differs a lot from the RGOS 11 system. Therefore, when using a transitional version between RGOS 10 and RGOS 11 for the upgrade, you need to add the RGOS 10 keyword. 2. The **.bin** file is loaded to the memory only when an AP needs to be upgraded. When no AP needs to be upgraded, the **.bin** file will be automatically removed from the memory. 3. Before configuring this command, ensure that the software version file already exists in the AC system files.

Upgrading the Version of Specified APs

- (Optional) Run the **ap-image** command to use a specified file to upgrade a specified AP series on the AC. This command takes effect on all APs connected to the AC.
- To upgrade the AP software version through the AC, you need to first specify the upgrade file used by the AP.
- To upgrade a specified AP series, you need to first activate the AP software version, specify the AP series, and specify a file for upgrading the specified AP series.

Command	**ap-image** *filename*
Parameter Description	*filename*: Specifies the software version name.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring Adaptive Upgrade

- (Optional) Run the **ap-image auto-upgrade** command so that the AC can automatically identify applicable AP products based on the AP upgrade file and upgrade all applicable APs.
- The command automatically matches the AP models to which the software version is applicable and upgrades these APs.

Command	**ap-image**{ **auto-upgrade** | *filename serial-name*}
Parameter Description	**auto-upgrade:** Indicates that the product model is automatically matched for the upgrade. *filename*: Specifies the software version name. This file name must be the same as that specified by the **active-bin-file** command. *serial-name*: Indicates the name of the AP series to be upgraded.

Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	You can use the **auto-upgrade** option to automatically match the software version and upgrade APs without configuring the mapping between the AP models and software version. You can also use a specified file to upgrade a specified AP series. When both the automatic upgrade mode and the specified series upgrade mode exist, the specified series upgrade mode is used preferentially. To enable the AC to upgrade the version of a specified AP series, you need to create the AP series, configure the software version corresponding to the specified APs, and activate the software version. The three steps are mandatory.

Configuring AP Upgrade Function in Hierarchical AC Scenarios

- Optional.
- Enable the AP upgrade function on the center AC or a branch AC in hierarchical AC scenarios.

Command	**capwap upgrade center enable**
Parameter Description	N/A
Defaults	The AP upgrade function is enabled on the center AC (disabled on branch ACs).
Command Mode	AC configuration mode
Usage Guide	1. This command applies only to hierarchical AC scenarios. 2. When the AP upgrade function on an AC is disabled, upgrade configurations (activated **.bin** file, automatic upgrade, sequential upgrade, and single AP upgrade) on the AC are automatically cleared. 3. After a branch AC is connected to the center AC, the configurations on the center AC are automatically synchronized to the branch AC. 4. When a branch AC is in the connection state, the configurations on the branch AC cannot be modified. The configurations can only be modified on the center AC and automatically synchronized to the branch AC. 5. When the branch AC is in the standalone state, the configurations on the branch AC can be modified.

Configuring the Maximum Number of APs That Can Be Concurrently Upgraded by the AC

- Optional.
- Limit the maximum number of APs that can be concurrently upgraded by the AC.

Command	**capwap upgrade max-concurrent** *num*
Parameter Description	*num*: Indicates the maximum number of APs that can be concurrently upgraded by the AC. The default value is 15. The value ranges from 1 to 200.
Defaults	15
Command Mode	AC configuration mode
Usage Guide	N/A

Creating an Upgrade Group

- Optional.

- Create an upgrade group. The AC can evenly distribute the centralized upgrade quota to the upgrade group through balanced scheduling to limit the bandwidth and avoid wasting the bandwidth.

Command	**capwap upgrade group** *group-name* [**max-concurrent** *num*]
Parameter Description	*group-name*: Indicates the name of an upgrade group. The upgrade group name cannot be set to **default**. *num*: Indicates maximum number of APs that can be concurrently upgraded in the group. The default value is 5. The value ranges from 0 to 200.
Defaults	No upgrade group is configured and the AP upgrade is not limited by the bandwidth. When an upgrade group is configured, the maximum number of APs that can be concurrently upgraded in the group is 5.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding APs to an Upgrade Group

- Optional.
- Add APs to an upgrade group. Limit the number of APs that are upgraded in a centralized manner in this group through scheduling and configuration to control the bandwidth by upgrade group.

Command	**ap-upgrade group** *group-name*
Parameter Description	*group-name*: Indicates the name of the upgrade group. Before adding APs to an upgrade group, you need to run the **capwap upgrade group** command to create an upgrade group.
Defaults	APs are not added to any upgrade group.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the Bandwidth Used for AP Upgrade

- Optional.
- Configure the bandwidth used for AP upgrade.

Command	**ap-upgrade band-width** *num*
Parameter Description	*num*: Indicates the bandwidth used for AP upgrade. The unit is 1 kbps. The value ranges from 8 to 10,240.
Defaults	The bandwidth is not limited.
Command Mode	AP configuration mode
Usage Guide	The **capwap upgrade group** *group-name* [**max-concurrent***num*], **ap-upgrade group** *group-name*, and **ap-upgrade band-width** *num* commands are used to limit the bandwidth for AP upgrade.

Verification

- Check whether the AP version is successfully upgraded.
- Check the upgrade status of the bandwidth-limit upgrade group and APs in the group.

Configuration Example

Configuring AP Upgrade

Configuration Steps	● Enter the AC configuration mode on the AC. ● Create an AP series on the AC. ● Activate the specified AP software version used for the upgrade on the AC. ● Configure the AP upgrade version file on the AC.

AC	`Hostname(config-ac)# ap-serial serial1 AP220-E AP220-SE AP620-H hw-ver 1.0`
	`Hostname(config-ac)# active-bin-file ap.bin`
	`Hostname(config-ac)# ap-image ap.bin serial1`
	`Hostname(config-ac)# exit`

Verification	● Display the list of files activated on the AC.

AC	`Hostname#show ac-config active-file`
	`Cnt File Name Version Used Cnt Ready`
	`------ ---------- ---------- ---------- --------`
	`1 ap.bin RGOS 10.4(1t7)(1T7), Release(88888) 1 1`

Configuring the Bandwidth Used for AP Upgrade

Configuration Steps	● Enter the AC configuration mode on the AC. ● Create an AP upgrade group on the AC. ● Exit from the AC configuration mode. ● Enter the AP configuration mode. ● Configure the specified AP upgrade group on the AC. ● Activate the bandwidth used for AP upgrade on the AC.

AC	`Hostname(config-ac)# capwap upgrade group UPGRADE-GROUP1 max-concurrent 10`
	`Hostname(config-ac)# exit`
	`Hostname(config)#ap-config 8832.0000.1111`
	`Hostname(config-ap)# ap-upgrade group UPGRADE-GROUP1`
	`Hostname(config-ap)# ap-upgrade band-width 128`
	`Hostname(config-ap)# exit`

Verification	● Display the upgrade group and APs in the group on the AC. ● Display the APs and their bandwidths in an upgrade group on the AC.

AC	Hostname#show ac-config upgrade-group Cnt Group-Name Max-Concurrent Token cnt Upgrading cnt ------ ---------- ---------- ---------- 1 UPGRADE-GROUP1 10 2 1 Hostname#show ac-config upgrade-groupUPGRADE-GROUP1 Group have 2 ap, online 1 offline 1 Cnt Ap-Name Ap-Mac Online Upgrade Band-width ------- ---------- ---------- ------- ---------- ---------- 1 ap220e 8832.0000.1111 true true 128 2 ap330 - false false 128 Hostname#show ap-config wtp-info 8832.0000.1111 Hostname#show ap-config wtp-info ap220e Upgrade-banfwidth : 128 Upgrade group : UPGRADE-GROUP1

Configuring AP Upgrade Function in Hierarchical AC Scenarios

Configuration Steps	1. Enable the AP upgrade function on the center AC (and disable it on branch ACs).
	`Hostname(config-ac)# capwap upgrade center enable`
	2. Enable the AP upgrade function on a branch AC (and disable it on the center AC).
	`Hostname(config-ac)# no capwap upgrade center enable`
	3. Cancel the configuration.
	`Hostname(config-ac)# default capwap upgrade center enable`

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

Common Errors

- AP upgrade is configured, but the software version file used for the upgrade does not exist in the AC system files.

1.4.8 Configuring Smart Upgrade

Configuration Effect

- Upgrade is performed based on the upgrade time and upgrade mode that are specified by the user.

Notes

- In an AP group, if upgrade time is scheduled but no upgrade mode is configured, no upgrade is performed at scheduled time.
- After smart upgrade is configured, if an AP fails the upgrade, the remaining APs no longer perform the upgrade, even in the next scheduled cycle.
- Before the upgrade, you need to activate the **.bin** file. The automatic upgrade function is enabled during the **.bin** file activation. If an AP to be upgraded is in the group for scheduled upgrade, the AP will not be automatically upgraded, whereas an AP not in the group for scheduled upgrade is automatically upgraded.

Configuration Steps

Configuring an Upgrade Mode

- Configure the upgrade mode of an AP group as smart upgrade or forced upgrade.

Command	**ap-image upgrade-mode { force | smart }**
Parameter Description	**force**: Indicates forced upgrade. **smart**: Indicates smart upgrade.
Defaults	No upgrade mode is configured.
Command Mode	AP group configuration mode
Usage Guide	N/A

Configuring a Scheduled Time for Upgrade

- Configure a scheduled time for the upgrade.

Command	**ap-image upgrade-appoint {start | stop |** *period* **[date-start** *date***] {once | cycle}}**
Parameter Description	**start**: Starts the upgrade immediately. **Stop**: Stops the upgrade immediately. *period*: Schedules the time period for the upgrade, in the format of *HH:MM HH:MM*. **date-start**: Schedules the start date of the upgrade. The default value is the day when the upgrade is performed. *date*: Indicates the date when the upgrade starts, in the format of *yyyy-mm-dd.* **once**: Indicates that the upgrade is only performed at the scheduled time on the scheduled date. **cycle**: Indicates that the upgrade takes effect at the scheduled time on the scheduled date and every day thereafter.
Defaults	No scheduled time is configured for the upgrade.
Command Mode	AP group configuration mode
Usage Guide	• The **once** parameter takes effect only at the scheduled time on the scheduled date. If the current time is later than the start time of the scheduled time range, the configuration fails and the error message "Appoint time is before current time" is displayed. In addition, if the configuration restoration time is later than the start time of the scheduled time range when the device restarts, the configuration cannot be restored. • The **upgrade-appoint** command takes effect only after the **upgrade-mode** command is configured. Therefore, automatic upgrade cannot be implemented when only the **upgrade-appoint** command is configured. In an AP group, if a scheduled time is configured for upgrade but no

	upgrade mode is configured, the upgrade cannot performed at the scheduled time. ● Before the upgrade, activate the bin file. If you activate the bin file after the automatic upgrade function is enabled, and the AP to be upgraded is in the AP group configured for scheduled upgrade, the AP cannot be upgraded automatically. If the AP to be upgraded is not in the AP group configured for scheduled upgrade, the AP will be upgraded automatically. ● After the smart upgrade mode is configured, if an AP fails to be upgraded for more than three times, the AP will not be upgraded again, and the upgrade will be performed on other APs to be upgraded. ● The automatic upgrade function is enabled on an AP by default. To use the smart upgrade and scheduled upgrade functions, you need to configure the upgrade mode and activate the version upgrade file. ● After the **ap-image upgrade-appoint start** command is configured, the AP will perform the upgrade immediately, regardless of the scheduled time. After the **ap-image upgrade-appoint stop** command is configured, the upgrade will be stopped regardless of the scheduled time. However, the upgrade of an AP that is already in the upgrade process cannot be stopped. ● The **start** and **stop** parameters are parameters of an action command. The parameters take effect only once and are not saved.

Verification

- Run the **show upgrade-appoint summary** command to display the scheduled upgrade configuration of groups.
- Run the **show upgrade-appoint ap-group** *apg-name* command to display the scheduled upgrade configuration of a single group.

Configuration Example

Configuring an Upgrade Mode

Configuration Steps	● On an AP group of an AC, separately configure the forced upgrade mode and smart upgrade mode, and delete the upgrade modes.
AC	Forced upgrade mode: Hostname(config-group)#ap-image upgrade-mode force Smart upgrade mode: Hostname(config-group)#ap-image upgrade-mode smart Delete the upgrade mode: Hostname(config-group)#no ap-image upgrade-mode smart
Verification	● On the AC, display the upgrade mode configured for the current AP group.
AC	Hostname(config-group)#show this Building configuration... ! ap-image upgrade-mode force !

	end

Configuring a Scheduled Time

Configuration Steps	● Separately configure a scheduled time for the upgrade, configure the upgrade to start immediately, configure the upgrade to stop immediately, configure a single upgrade cycle in the scheduled time period, and configure multiple upgrade cycles in the scheduled time period.
AC	Configure the upgrade to start immediately. Hostname(config-group)#ap-image upgrade-appoint start Configure the upgrade to stop immediately. Hostname(config-group)#ap-image upgrade-appoint stop Set the time period for the upgrade to 12:00-13:00, the date to the current day, and the number of times to execute the upgrade in the scheduled time period to 1. Hostname(config-group)#ap-image upgrade-appoint 12:00 13:00 once Set the time period for the upgrade to 12:00-13:00, the date to 2021-09-10, and the number of times to execute the upgrade in the scheduled time period to multiple times. Hostname(config-group)#ap-image upgrade-appoint 12:00 13:00 start-date 2021-09-10 cycle
Verification	● Display the scheduled upgrade configuration of all groups on the AC. ● Display the scheduled upgrade configuration and AP status of a single group. ● Run the **show this** command to display the scheduled upgrade configuration of the current group.
AC	Hostname#show upgrade-appoint summary APG MODE TIME DATE PERIOD ---------- ----- ----- ---------- ---------- test force cycle 2021-09-10 12:00 13:00 Hostname#show upgrade-appoint ap-group test The upgrade mode: force The appoint date: 2021-09-10 12:00 13:00 Achieve appoint time: no AP-PID AP-MAC VERSION NEED ---------- ---------- ---------- ----- AP840-I 0074.9cbd.af08 AP_RGOS 11.9(0)B0, Release(08200100) NO AP710-A 8005.886b.599e AP_RGOS 11.1(9)B1P25 NO Hostname(config-group)#show this Building configuration... ! ap-image upgrade-mode force

	ap-image upgrade-appoint 12:00 13:00 start-date 2021-09-10 cycle !

1.4.9 Configuring a Micro AP

Configuration Effect

- An i-Share+ master AP can be connected to multiple micro APs. To facilitate micro AP management, perform some operations such as configuring the names of micro APs and displaying the installation status.

Notes

- N/A

Configuration Steps

Configuring the Name of a Micro AP

- (Optional) Run the **slot** command to name a micro AP in a specified slot.
- This configuration takes effect only for i-Share APs. The corresponding radio frequency (RF) card can be named to determine the position of this card.

Command	**slot** *slot-id* {*slot-name* [**secondary**] | **mac** *mac-address slot-name* }
Parameter Description	*slot-id*: Indicates the slot ID. The slot ID ranges from 1 to 24. *slot-name*: Indicates the name of an AP card. The name is a string of 1 to 63 characters and cannot contain any space. **secondary**: Applies to the secondary AP. *mac-address*: Indicates the MAC address of the micro AP.
Defaults	An AP card is not named.
Command Mode	AP configuration mode
Usage Guide	This command takes effect only for i-Share+ APs and cannot be configured for all APs. If you want to name a secondary micro AP, add the **secondary** parameter. Micro AP names are configured based on MAC addresses, allowing for offline configuration during installation. Each slot can be configured with two MAC addresses. When the micro AP with the corresponding MAC address goes online, the micro AP can automatically switch port-based configuration based on the cascading relationships.

Updating the Installation Status of a Micro AP

- (Optional) Run the **install update** or **uninstall** command to update the installation status of a micro APs.
- If the state of a removed micro AP is displayed as offline, you can update its installation status.

Command	**install update**

Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	If a micro AP is installed in a specified slot on the i-Share+ AP but is later manually removed, the system determines that this micro AP is offline. This command is executed to query an i-Share+ AP that is currently online, and update the installation status of the online micro AP to **installed**. Configurations of this command are not saved.

Command	**uninstall** *slot-id* [**secondary**]
Parameter Description	*slot-id*: Indicates the slot ID. The slot ID ranges from 1 to 24. **secondary**: Applies to the secondary AP.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	If a micro AP is installed in a specified slot on the i-Share+ AP but is later manually removed, the system determines that this micro AP is offline. You can use this command to remove a micro AP from the corresponding slot. If the micro AP in this slot is online, this command does not take effect. Configurations of this command are not saved. In addition, the command cannot be used in all AP configuration mode. If you want to name a secondary micro AP, add the **secondary** parameter.

Restarting a Micro AP

- (Optional) Run the **reset slot** *slot-id* command to restart a micro AP in a specified slot.
- To reset a micro AP, you can use this command to power off the micro AP and then power it on again.
- This command applies to two micro APs of a slot in a cascading scenario.

Command	**reset slot** *slot-id*
Parameter Description	*slot-id*: Indicates the slot ID. The slot ID ranges from 1 to 24.
Defaults	N/A
Command Mode	AP configuration mode

Usage Guide	This command takes effect only for i-Share+ APs and cannot be used in all-AP configuration mode. Configurations of this command are not saved.

Verification

- Check the installation information of micro APs, including the names and online status.

Configuration Example

Configuring the Name of a Micro AP

Configuration Steps	• Enter the AP configuration mode on the AC. • Configure the name of a micro AP in a specified slot.

AC	The following example sets the name of micro AP1 to **1#101**.
	`Hostname(config)# ap-config AP0001`
	`Hostname(config-ap)# slot 1 Dormitory 1#101`
	The following example sets the name of AP0001, secondary micro AP1 in slot 1, to **1#102**.
	`Hostname(config)# ap-config AP0001`
	`Hostname(config-ap)# slot 1 1#102 secondary`
	The following example sets the name of the micro AP (MAC address: 0001.0001.0001) in slot 1 to **1#101** and the name of the micro AP (MAC address: 0001.0001.0002) of slot 1 to **1#102**.
	`Hostname(config)# ap-config AP0001`
	`Hostname(config-ap)# slot 1 mac 0001.0001.0001 1#101`
	`Hostname(config-ap)# slot 1 mac 0001.0001.0002 1#102`

Verification	• Display the name of the micro AP on the AC.

AC	Hostname#show ap-config summary slot Total Install Number: 2 Total Online Number: 1 Total Offline Number: 1 AP(AP0001)'s Slots Information Install Number: 2 Online Number: 1 Offline Number: 1 AP mac Slot ID Role Slot Name Model Slot Mac Radio Radio Up/Off time State -------------- ------- --------- ---------- --------- -------------- -------------------- ------------------- ----------- ------- 00d0.f822.3418 1 master Dormitory 1#101 MAP552 5869.6c36.e268 1 E 0 6* 100 2 E 0 157* 100 1:03:39:38 online 00d0.f822.3418 2 slave Dormitory 1#102 MAP552 5869.6c36.e269 3 N 4 N 1:03:39:38 offline

Common Errors

- N/A

1.4.10 Configuring the CAPWAP Control Address

Configuration Effect

- Configure an IP address for the AC to set up a CAPWAP tunnel with an AP.

Notes

- When the IP address used by the AC to set up the CAPWAP tunnel is changed, online APs may be disconnected.
- If the configured IP address does not exist on the AC, the CAPWAP tunnel cannot be set up.
- If the gateway of the AP is not located on the AC (indicating a Layer 3 topology between the AC and AP), the option field of the AP's address pool needs to be configured with the address specified in the **capwap ctrl-ip** command (if available).
- In an AC hot standby environment, if this command is used to configure the control address of the CAPWAP tunnel, the peer backup AC must configure this control address as the peer control IP address in hot standby configuration mode. The command is **peer-ip** *A.B.C.D*.

Configuration Steps

↘ **Configuring the Maximum Number of APs That Can Concurrently Go Online**

- Optional. Run this command when a non-lookback IP address needs to be configured as the CAWAP control address.
- On the AC, configure the maximum number of APs that can concurrently go online to prevent an excessively high CPU usage caused by a large number of CAPWAP control packets.
- Run the **capwap ctrl-ip** *ip-address* command to specify an IP address on the AC to set up a CAPWAP tunnel with an AP. *ip-address* indicates the IP address of an interface on the AC.

Command	**capwap ctrl-ip** *ip-address*
Parameter Description	*ip-address*: Indicates the IP address of an interface on the AC to set up a CAPWAP tunnel with an AP. The IP address of Lookback 0 interface is used by default.
Defaults	The IPv4 address of the first lookback interface on the AC is used.
Command Mode	AC configuration mode
Usage Guide	By default, the AC establishes a CAPWAP tunnel with an AP using the IP address of the first loopback interface. This command allows users to manually specify the IP address for the AC to establish a CAPWAP tunnel with an AP.

Verification

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

Configuration Example

Configuring the Control IP Address of the AC to 10.0.0.1

Configuration Steps	● Enter the AC configuration mode. ● Configure the control IP address of the AC to 10.0.0.1.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)#capwap ctrl-ip 10.0.0.1`
Verification	● On the AC, run the **show running-config** command to display the configuration.

AC	`Hostname#show current-config`
	`!`
	`ac-controller`
	`capwap ctrl-ip 10.0.0.1`
	`!`

Common Errors

- N/A

1.4.11 Configuring CAPWAP Fragmentation

Configuration Effect

- After a data packet or control packet is encapsulated on the CAPWAP tunnel, the packet length may exceed the IP MTU, and will be fragmented at the IP layer. When the IP MTUs of multiple nodes on the link are inconsistent, the

packet may be fragmented and reassembled for several times, which reduces the packet forwarding performance. After CAPWAP fragmentation is enabled, the packet will be fragmented when encapsulated on the CAPWAP tunnel. The CAPWAP packet length is specified as the minimum IP MTU on the link, thereby avoiding fragmentation at the IP layer.

Notes

- If the configured MTU is too small, a lot of fragmented packets will be generated, affecting the packet forwarding performance. Even worse, large packets may fail to be transmitted. Therefore, it is important to determine the size of the MTU.
- The configured CAPWAP MTU must be smaller than or equal to the IP MTU at the egress of the device. Otherwise, IP fragmentation will be performed after CAPWAP fragmentation. The minimum IPv6 MTU is 1280 bytes, that is, the minimum path MTU is 1280 bytes. Therefore, the CAPWAP MTU must be greater than or equal to 1280 bytes.
- Fragmentation on a control tunnel is enabled by default and cannot be disabled. Fragmentation on a data tunnel is disabled by default, and you can run the **capwap fragment enable** to enable this function.

Configuration Steps

Configuring the Path MTU of the CAPWAP Data Tunnel

- (Optional) Enter the AP or AP group configuration mode, and run the **capwap mtu** command to configure the path MTU of the CAPWAP data tunnel.
- When the length of a data packet exceeds the path MTU of the CAPWAP tunnel after the data packet is encapsulated on the CAPWAP tunnel, the data packet will be fragmented on the CAPWAP tunnel. Set the path MTU of the data tunnel on the AC to the minimum IP MTU. Otherwise, IP fragmentation and reassembly are performed again during packet forwarding, reducing the forwarding performance.

Command	**capwap mtu** *num*
Parameter Description	*num*: Indicates the size of the path MTU of the CAPWAP data tunnel, in bytes. The value ranges from 110 to 1,500.
Defaults	1500 bytes
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Configuring the Path MTU of the CAPWAP Control Tunnel

- (Optional) After entering the AP configuration mode or AP group configuration mode, run the **capwap ctrl-mtu** command to configure the path MTU of the CAPWAP control tunnel.
- When the length of a control packet exceeds the path MTU of the CAPWAP tunnel after the control packet is encapsulated on the CAPWAP tunnel, the control packet will be fragmented on the CAPWAP tunnel. Set the path MTU of the control tunnel on the AC to the minimum IP MTU. Otherwise, IP fragmentation and reassembly are performed again during packet forwarding, reducing the forwarding performance.

Command	**capwap ctrl-mtu** *num*
Parameter Description	*num*: Indicates the size of the path MTU of the CAPWAP control tunnel, in bytes. The value ranges from 256 to 1,500.
Defaults	1500 bytes

Command Mode	AC configuration mode, AP configuration mode, or AP group configuration mode
Usage Guide	N/A

Enabling CAPWAP Fragmentation on the Data Tunnel

- Optional.
- When multiple IP MTU nodes exist on the transmission network, it is recommended that CAPWAP fragmentation be enabled on the AC and the CAPWAP MTU be set to the path MTU.
- After a packet is encapsulated on the CAPWAP tunnel, the packet length may exceed the IP MTU, and will be fragmented at the IP layer. When the IP MTUs of multiple nodes on the link are inconsistent, the packet may be fragmented and reassembled for several times, which reduces the packet forwarding performance. You can run this command to enable CAPWAP fragmentation. After this function is enabled, the packet will be fragmented when encapsulated on the CAPWAP tunnel. The CAPWAP packet length can be specified in the **capwap mtu** command as the minimum IP MTU on the link, thereby avoiding fragmentation at the IP layer.

Command	**capwap fragment enable**
Parameter Description	N/A
Defaults	CAPWAP fragmentation is disabled.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Check the detailed information about the CAPWAP tunnel such as the MTU and check whether CAPWAP fragmentation is enabled.
- Alternatively, run the **show ap-config running** command to display the configuration.

Configuration Example

Configuring the MTU of AP1 and Enabling CAPWAP Fragmentation

Configuration Steps	• Set the path MTU of AP1 to 1200 bytes on the AC. • Enable CAPWAP fragmentation of AP1 on the AC.

AC	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# capwap mtu 1200`
	`Hostname(config-ap)# capwap fragment enable`

Verification	Use the **show ap-config running** command to display the configuration.

AC	Hostname#show ap-config running ! capwap fragment enable capwap mtu 1200 !

Common Errors

- N/A

1.4.12 Configuring CAPWAP Encryption

Configuration Effect

- Enable the encryption function on the CAPWAP data tunnel to enhance WLAN security.
- Disable the encryption function on the CAPWAP control tunnel to perform packet analysis when network faults occur.

Notes

- Changing the encryption mode on the data tunnel triggers re-establishment of the CAPWAP tunnel.

Configuration Steps

Configuring CAPWAP Data Tunnel Encryption

- (Optional) After entering the AP configuration mode or AP group configuration mode, run the **capwap data-tunnel encryption** command to configure CAPWAP data tunnel encryption.
- The CAPWAP data tunnel is not encrypted by default. When the transmission link between the AC and AP is deployed on a public transport network, data may be intercepted or tampered with. On the AC, configure CAPWAP data tunnel encryption to ensure the transmission security of user data packets.
- Configure data tunnel encryption to ensure the security of package exchange between the AC and AP.

Command	**capwap data-tunnel encryption** { **bf** | **des** } *key*
Parameter Description	*key*: Indicates a shared key ended with a space. The value can contain a maximum of 255 characters.
Defaults	The CAPWAP data tunnel is not encrypted.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Configuring CAPWAP Control Tunnel Encryption

- Optional.
- On the AC, disable the encryption function on the CAPWAP control tunnel when network faults occur, allowing network engineers to locate faults through packet analysis.

Command	capwap dtls enable
Parameter Description	N/A
Defaults	DTLS encryption is enabled for the CAPWAP control tunnel.
Command Mode	AC configuration mode
Usage Guide	By default, DTLS encryption is enabled for the CAPWAP control tunnel to ensure security of packet exchange between the AC and the AP. In special cases, you can disable the encryption function on the CAPWAP control tunnel to facilitate tests.

Verification

- Check the detailed information about the CAPWAP tunnel to determine the encryption policies of the control tunnel and the data tunnel.
- Run the **show running-config** command to check whether encryption is enabled on the control tunnel.

Configuration Example

Enabling Encryption on the Data Tunnel and Disabling Encryption on the Control Tunnel

Configuration Steps	• On the AC, configure the AP to encrypt the data tunnel by using the DES encryption algorithm. The key is **Hostname**. • On the AC, disable the encryption function on the AP control tunnel.
AC	`Hostname(config-ap)# no capwap dtls enable`
Verification	• Check the information about the CAPWAP tunnel on the AC. • On the AC, run the **show running-config** command to check whether encryption is disabled on the control tunnel

AC	`Hostname# show capwap detail`
	`CAPWAP process "capwap 1" with state [ Run ]`
	`Process uptime is 0 days 0 hours 0 minutes 43 seconds`
	`Echo interval is 30 secs, Dead interval is 81 secs`
	`Current timers echo interval`
	`Peer address is 10.10.10.2`
	`Peer address6 is ::`
	`Peer control port is 10000, data port is 10001`
	`My address is 1.1.1.1`
	`My address6 is ::`
	`The MAC of AP is 001a.a94e.de9d`
	`The Session ID of AP is 001aa94e.de9d8ab5.11818ab5.11818ab5`
	`Capwap fragment is disable`
	`The Path MTU is 1500`

	Recent received request's sequence number 7 Recent received response's sequence number 3 Recent send request's sequence number 3 Retransmit Count 0, Discovery Count 0, Failed DTLS Session Count 0 Sending queue length 0, Receive queue length 0 Data crypt capacity BF and DES Data crypt type plain Hostname# show running-config ! no capwap dtls enable

Common Errors

- N/A

1.4.13 Configuring CAPWAP Access Control

Configuration Effect

- Configure the maximum number of concurrent APs.

Notes

- If the configured value is too small, the total online duration of all APs connected to the AC will be relatively long.

Configuration Steps

Configuring the Maximum Number of Concurrent APs

- Optional.
- On the AC, configure the maximum number of concurrent APs to prevent high CPU usage caused by a large number of CAPWAP control packets.

Command	**capwap max-concurrent** *num*
Parameter Description	*num*: Indicates the maximum number of concurrent APs. The number ranges from 1 to 65535.
Defaults	50
Command Mode	AC configuration mode
Usage Guide	If a large number of APs go online concurrently, the CPU usage of the AC may increase or even reach 100%. Consequently, tunnels of APs that are already online will be disconnected due to keepalive failures. You can use this command to configure the maximum number of concurrent APs.

Configuring the Number of CAPWAP Discovery Packets That Can Be Processed by an AC

- Optional.

- Configure the maximum number of discovery packets that can be processed by an AC on the AC to prevent high CPU usage caused by considerable CAPWAP control packets.
- Run the **capwap disc-concurrent** *num* command to configure the number of discovery packets that can be processed.

Command	**capwap disc-concurrent** *num*
Parameter Description	*num*: Indicates the number of discovery packets that can be processed per second depends on the product capacity.
Defaults	The default value varies with the product capacities, for example, the default value is 256 for the WS7800.
Command Mode	AC configuration mode
Usage Guide	The CAPWAP module needs to restrict the number of discovery packets based on the AC capacity to prevent discovery packet attacks.

Verification

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

Configuration Example

Configuring the Maximum Number of Concurrent APs

Configuration Steps	● On the AC, configure the maximum number of APs that can concurrently go online.
AC	`Hostname(config-ac)#capwap max-concurrent 100`
Verification	● On the AC, run the **show running-config** command to display the configuration.

AC	`Hostname# show running-config`
	`!`
	`ac-controller`
	`capwap max-concurrent 100`
	`!`

Common Errors

- N/A

1.4.14 Configuring the Heartbeat Keepalive Interval of the CAPWAP Tunnel

Configuration Effect

- (Optional) Configure the interval at which a keepalive packet is sent.

Notes

- During deployment of the wireless network, the heartbeat keepalive interval of the CAPWAP tunnel can be adjusted according to the network scale to properly plan the network convergence performance. Before configuring the

heartbeat keepalive interval, ensure that you have a good understanding about the network scale and confirm that the convergence is necessary. If the heartbeat keepalive interval is set to a small value on a wireless network where a large number of APs are deployed, the network environment will be affected.

Configuration Steps

- (Optional) Enter the AP or AP group configuration mode.
- Configure the heartbeat keepalive interval of the CAPWAP tunnel on the AC to control the keepalive period of the CAPWAP tunnel.

Command	**echo-interval** *seconds*
Parameter Description	*seconds*: Indicates the heartbeat keepalive interval of the CAPWAP tunnel, in seconds. The value ranges from 5 to 255.
Defaults	30s
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	On a fit AP network, an AC is interconnected with an AP through the CAPWAP tunnel. The Echo Request and Echo Response packets are exchanged between the AP and the AC to maintain the validity of links. If other request packets are not transmitted, the AP sends an Echo Request packet to the AC at the interval specified by **echo-interval** to keep the CAPWAP tunnel alive. If the AP does not receive any Echo Response packet, the Echo Request packet will be retransmitted. The transmission interval starts at the initial transmission interval (3s or half of **echo-interval**, whichever the smaller), and then is doubled upon next retransmission. The maximum retransmission interval cannot exceed the half of **echo-interval** or 60s, whichever the smaller. If the AP does not receive the Echo Response packet when **max-retransmit (**the maximum number of retransmission attempts) is reached, it is determined that the CAPWAP tunnel is disconnected. That is, the keepalive failure time of the tunnel is equal to the keepalive time plus the retransmission interval. This command takes effect only when the tunnel is in Run state. By default, **echo-interval** is 30s, and **max-retransmit** is 5. If the Echo Response packet is not received 0s after the Echo Request packet is sent, the Echo Request packet will be retransmitted at the interval of 3s, 6s, 12s, 15s, and 15s, respectively. The same rule is observed to calculate the packet timeout time if **echo-interval** and **max-retransmit** are set to other values.

Verification

- Check the detailed information about the CAPWAP tunnel, including the modified interval at which the keepalive packet is sent.

Configuration Example

Configuring the Heartbeat Keepalive Interval of the CAPWAP Tunnel

Configuration Steps	● On the AC, set the heartbeat keepalive interval of the CAPWAP tunnel to 50s.
AC	`Hostname(config)#ap-config AP0001` `Hostname(config-ap)# echo-interval 50`
Verification	● On the AC, check the detailed information about the CAPWAP tunnel.

AC	Hostname#show capwap 1.1.1.1 detail Echo interval is 50 secs, Dead interval is 119 secs

Common Errors

- N/A

1.4.15 Configuring the Maximum Number of CAPWAP Packet Retransmission Attempts

Configuration Effect

- (Optional) Configure the maximum number of retransmission attempts for a CAPWAP packet to adjust the keepalive interval of the CAPWAP tunnel.

Notes

N/A

Configuration Steps

- (Optional) Enter the AP or AP group configuration mode.
- Configure the maximum number of retransmission attempts for a CAPWAP packet to adjust the keepalive interval of the CAPWAP tunnel.

Command	**capwap max-retransmit** *num*
Parameter Description	*num*: Indicates the maximum number of retransmission attempts for a CAPWAP packet.
Defaults	5
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	If the AP does not receive any Echo Response packet after sending an Echo Request packet, the Echo Request packet will be retransmitted. The transmission interval starts at the initial transmission interval (3s or half of **echo-interval**, whichever the smaller), and then is doubled upon next retransmission. The maximum retransmission interval cannot exceed the half of **echo-interval** or 60s, whichever the smaller. If the AP does not receive the Echo Response packet when **max-retransmit (**the maximum number of retransmission attempts) is reached, it is determined that the CAPWAP tunnel is disconnected. You can configure the maximum number of retransmission attempts for a CAPWAP packet to adjust the keepalive interval of the CAPWAP tunnel. This command takes effect only when the tunnel is in Run state.

Verification

- Check the detailed information about the CAPWAP tunnel, including the modified interval at which the keepalive packet is sent.

Configuration Example

Configuring the Maximum Number of CAPWAP Packet Retransmission Attempts

Configuration Steps	● Set the maximum retransmission attempts of AP1 to 20.
AC	`Hostname(config)#ap-config AP1` `Hostname(config-ap)# capwap max-retransmit 20`
Verification	● On the AC, check the detailed information about the CAPWAP tunnel.
AC	`Hostname#show capwap 1.1.1.1 detail` `Config maxretransmit 20`

Common Errors

- N/A

1.4.16 Configuring the AC Discovery Mode

Configuration Effect

- An AP can discover an AC in recommended mode, DHCP mode, DNS mode, static mode, or other modes (such as broadcast or multicast mode). An AC can be configured to respond only to Discovery Request packets of specific types. Only after receiving Discovery Response packets from ACs, the AP can determine whether ACs are valid and then select an AC to set up a CAPWAP tunnel.

Notes

- If all AC discovery modes are not supported, an AP cannot access an AC by sending Discovery Request packets.

Configuration Steps

Discovering an AC in Recommended Mode

- Optional.

Command	**capwap discovery-type ac-referral { allow | forbidden}**
Parameter Description	**allow**: Indicates that this type of discovery request packets can be used to discover an AC. **forbidden**: Indicates that this type of discovery request packets cannot be used to discover an AC.
Defaults	An AP can send Discovery Request packets of a recommended type to discover an AC.
Command Mode	AC configuration mode
Usage Guide	N/A

Discovering an AC Through Discovery Request Packets

- Optional.
- After this command is configured, configurations of other discovery types will be overwritten.

Command	**capwap discovery-type all { allow | forbidden}**
Parameter Description	**allow**: Indicates that Discovery Request packets can be used to discover an AC. **forbidden**: Indicates that Discovery Request packets cannot be used to discover an AC.

Defaults	An AP can send Discovery Request packets to discover an AC.
Command Mode	AC configuration mode
Usage Guide	N/A

Discovering an AC in DHCP Mode

- Optional.

Command	**capwap discovery-type dhcp { allow | forbidden}**
Parameter Description	**allow**: Indicates that DHCP packets can be used to discover an AC. **forbidden**: Indicates that DHCP packets cannot be used to discover an AC.
Defaults	An AP can send DHCP packets to obtain the AC IP address and discover the AC.
Command Mode	AC configuration mode
Usage Guide	N/A

Discovering an AC in DNS Mode

- Optional.

Command	**capwap discovery-type dns { allow | forbidden}**
Parameter Description	**allow**: Indicates that DNS packets can be used to discover an AC. **forbidden**: Indicates that DNS packets cannot be used to discover an AC.
Defaults	An AP can send DNS packets to obtain the AC IP address and discover the AC.
Command Mode	AC configuration mode
Usage Guide	N/A

Discovering an AC in Static Mode

- Optional.
- Configure static AC IP addresses and clusters.

Command	**capwap discovery-type static-config { allow | forbidden}**
Parameter Description	**allow**: Indicates that packets carrying the configured AC IP address can be used to discover an AC. **forbidden**: Indicates that packets carrying the configured AC IP address cannot be used to discover an AC.
Defaults	An AP can send Discovery Request packets to discover the AC whose IP address is manually configured.
Command Mode	AC configuration mode
Usage Guide	N/A

Discovering an AC in Other Modes

- Optional.
- Configure other AC discovery modes, such as the broadcast or multicast mode.

Command	**capwap discovery-type unknown { allow | forbidden}**

Parameter Description	**allow**: Indicates that broadcast or multicast discovery packets can be used to discover an AC. **forbidden**: Indicates that broadcast or multicast discovery packets cannot be used to discover an AC.
Defaults	An AP can send broadcast or multicast packets to discover an AC.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Forbidding an AP to Send Discovery Request Packets of a Recommended Type to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send Discovery Request packets of a recommended type to discover an AC.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# capwap discovery-type ac-referral forbidden`
Verification	● Display the AC configuration.

AC	`Hostname#show running-config`
	`!`
	`ac-controller`
	`capwap discovery-type ac-referral forbidden`
	`!`

Forbidding an AP to Send Discovery Request Packets to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send Discovery Request packets to discover an AC.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# capwap discovery-type all forbidden`
Verification	● Display the AC configuration.

AC	`Hostname#show running-config`
	`!`
	`ac-controller`
	`capwap discovery-type all forbidden`
	`!`

Forbidding an AP to Send DHCP Packets to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send DHCP packets to obtain the AC address and discover the AC.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# capwap discovery-type dhcp forbidden`
Verification	● Display the AC configuration.
AC	`Hostname#show running-config`

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send DHCP packets to obtain the AC address and discover the AC.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# capwap discovery-type dhcp forbidden`
Verification	● Display the AC configuration.

	`!`
	`ac-controller`
	`capwap discovery-type dhcp forbidden`
	`!`

Forbidding an AP to Send DNS Packets to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send DNS packets to obtain the AC address and discover the AC.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# capwap discovery-type dns forbidden`
Verification	● Display the AC configuration.

AC	`Hostname#show running-config`
	`!`
	`ac-controller`
	`capwap discovery-type dns forbidden`
	`!`

Forbidding an AP to Send Packets Carrying the Statically Configured AC IP Address to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send packets carrying the statically configured AC IP address to discover the AC.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# capwap discovery-type static-config forbidden`
Verification	● Display the AC configuration.

AC	`Hostname#show running-config`
	`!`
	`ac-controller`
	`capwap discovery-type static-config forbidden`
	`!`

Forbidding an AP to Send Other Types of Discovery Request Packets to Discover an AC

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send other types of Discovery Request packets to discover the AC.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# capwap discovery-type unknown forbidden`
Verification	● Display the AC configuration.

Configuration Steps	● Enter the AC configuration mode. ● Forbid an AP to send other types of Discovery Request packets to discover the AC.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# capwap discovery-type unknown forbidden`
Verification	● Display the AC configuration.

AC	`Hostname#show running-config`
	`!`
	`ac-controller`
	`capwap discovery-type unknown forbidden`
	`!`

Common Errors

- N/A

1.4.17 Enabling Self-Balancing Based on VAC

Configuration Effect

- When self-balancing based on VAC is enabled on a VAC network, newly added APs will be evenly distributed to each member AC. In this way, frequent migration of APs between member ACs will be avoided when the switch directly connected to the AC fails to balance the load.

Notes

- If centralized forwarding mode is adopted on the VAC network, enabling self-balancing based on VAC will affect the forwarding performance of the device. Therefore, this function is suitable for VAC networks where local forwarding mode is adopted.

Configuration Steps

- (Optional) Enter the AC configuration mode to configure this function.

Command	**virtual-ac self-balance enable**
Parameter Description	N/A
Defaults	Disabled.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to display the configuration.
- Run the **show virtual-ac balance-info** command to display the AP load balancing information.

Configuration Example

Enabling Self-Balancing on the VAC Network

Configuration Steps	● Enable self-balancing on the VAC network.
	`Hostname(config)# ac-controller` `Hostname(config-ac)# virtual-ac self-balance enable`
Verification	● On the AC, run the **show running** command to display the configuration.
	`Hostname#show running` ` virtual-ac self-balance enable`

Common Errors

- N/A

1.4.18 Configuring the Command Set File Delivered by the AC to the AP

Configuration Effect

- On the AC, the commands to be executed by the AP are written to a specified file. The AC delivers the CLI command file to the AP in batches. After receiving the file, the AP executes the commands in the file in batches.

Notes

- N/A

Configuration Steps

Configuring the Command Set File Delivered by the AC to the AP

- Optional.
- Enter the AP configuration mode, AP group configuration mode, or all-AP configuration mode on the AC, run the **auto-cfg** command to perform configuration.

Command	**auto-cfg** [**save**] **file flash:***file-name* [**force** | **once**]
Parameter Description	**save**: Indicates that the file is retained on the AP after the AP executes the commands in the file. *file-name*: Indicates the name of the file delivered to the AP, which contains commands to be executed by the AP. **force**: Forcibly sends the command set file without checking whether the file name already exists, and the AC can send the files with the same file name to the AP. **once**: Forcibly sends the command set file without checking whether the file name already exists, and the AC does not save the file delivery record.
Defaults	N/A
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	1. The size of the CLI command set file cannot exceed 2000 KB, and the size of each command cannot exceed 128 bytes. 2. After the CLI command set file is delivered, the AP automatically executes all commands in the file.

	Ensure that the commands are correct and the AP version supports the commands in the file. 3. If the **save** parameter is not specified, the AP automatically deletes the file after executing the commands in the file. In AP configuration mode, the **save** parameter is mandatory. 4. If the configuration delivery mode is **once**, the AC does not save the delivery record of the command set file, and the command set file is not delivered again after the AP is disconnected and then reconnected. If the delivery mode is **force** or this parameter is not configured, the AC will save the command set delivery record and deliver the command set file again after the AP is reconnected.

Verification

- Run the **show running-config** command to check whether the commands in the file take effect.

Configuration Examples

Configuring the Command Set file Delivered by the AC to the AP

Configuration Steps	● Configure the AC to deliver the **ap001.txt** command set file to AP-0001.
AC	`Hostname(config)# ap-config AP-0001` `Hostname(config-ap)#auto-cfg save file flash:ap001.txt force`
Verification	● Run the **show running-config** command to check whether the commands in the file take effect.

Common Errors

- N/A

1.5 Monitoring

Clearing

- N/A

Displaying

Command	Description
show ac-config active-file	Displays the list of files activated on the AC.
show ac-config serial-product	Displays the mapping between AP series configured on the AC and product models, and files used to upgrade the product series.
show ac-config upgrade-group [*group-name*]	Displays the information about the upgrade group configured on the AC.
show ap-config board-data *ap-name*	Displays the data on the master board of the AP.
show ap-config link-latency { **all** | **single** *ap-name* }	Displays the state of links between ACs and APs.
show ap-config inventory *ap-name*	Displays the AP vendor information.
show ap-config reboot *ap-name*	Displays the AP restart statistics.

Command	Description
show ap-config slot	Displays the information about micro APs connected to a specified AP.
show ap-config summary slot interface	Displays the information about downlink ports of all i-Share+ APs.
show ap-config summary group	Displays the information about i-Share+ APs in an AP group.
show ap-config static-ip{ **all** | **single** *ap-name* }	Displays the static IP address of an AP.
show ap-config summary location	Displays the AP location.
show ap-config summary slot	Displays the information about micro APs connected to all APs.
show ap-config updating-list	Displays the AP upgrade status.
show ap-config wtp-descriptor *ap-name*	Displays the AP status descriptions.
show ap-config wtp-info *ap-name*	Displays the AP status.
show capwap [index | [ip-address [port]]] **detail**	Displays the details of the CAPWAP tunnel.
show capwap state	Displays the status of the CAPWAP tunnel.
show capwap [index | [ip-address [port]]] **statistics**	Displays the statistics of the CAPWAP tunnel.
show version { **all** | *ap-name* }	Displays the AP version information.
show upgrade-appoint {summary | ap-group *apg-name***}**	Displays the scheduled time and AP upgrade status of an AP group.
tran-data-start *ap-name* {**exception** | **memory** | **tech-support** | **tech-package**} **tran-data-show** *ap-name* {**exception** | **cpuinfo** | **memory** | **syslog**| **tech-support**}	Collects and displays various logs on an AP.

Debugging

- N/A

1 Configuring Basic Configuration Management Service

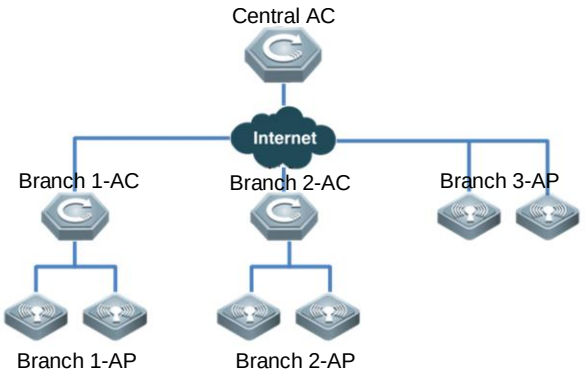
Supported functions vary depending on the product version.

1.1 Overview

In specific scenarios on a wireless network such as hierarchical access controller (AC) and all-optical i-Share+ master access point (AP) management, the identical configuration between two devices ensures better network running stability. Manual configuring the same commands on different devices is time-consuming and labor-intensive. The configuration management (CFGMG) function saves configuration information to a configuration template and allows administrators to add commands to and delete, modify, and query commands in the configuration template, providing the basic configuration service for different services. CFGMG improves the wireless network deployment efficiency and reduces the labor investment.

Protocols and Standards

1.2 Applications



Deployment

- Configure the AC at the headquarters as the central AC of the hierarchical AC networking.
- Configure the ACs in the branches as the branch ACs of the hierarchical AC networking.
- On the central AC and branch ACs, enable the wireless local area network (WLAN) hot standby function.
- On the central AC, add the hot standby peers for branch 1-AC and branch 2-AC.
- On branch 1-AC and branch 2-AC, add the hot standby peer for the central AC.
- On the central AC and branch ACs, add the AP groups to which branch 1-AP and branch 2-AP belong to the hot standby instances of the corresponding branches.
- On the central AC, create two configuration templates named **template1** and **template2**.
- Add the commands that are delivered to branch 1-AC to template1. On branch 1-AC, request template1.

- Add the commands that are delivered to branch 2-AC to template2. On branch 2-AC, request template2.

1.3 Features

Basic Concepts

A configuration template is used to store commands. Users can maintain commands in a configuration template through addition, deletion, modification, and query. Devices can associate with a configuration template to ensure batch delivery of commands in the configuration template to these devices.

Overview

Feature	Description
Creating a Configuration Template	Creates a configuration template.
Maintaining Commands in a Configuration Template	Adds commands to or deletes or modifies commands in a configuration template.

1.3.1 Creating a Configuration Template

To store commands in a configuration template, create a configuration template first. To modify commands in an existing configuration template, enter the configuration mode of the configuration template first.

Working Principle

Create a configuration template or enter the configuration mode of an existing configuration template. If you choose the former, you will enter the configuration mode after a configuration template is created.

1.3.2 Maintaining Commands in a Configuration Template

To meet command operation requirements of different services, you can add commands to and delete and modify commands in a configuration template. In addition, to add commands quickly, commands can be imported from a file in a specific format to a configuration template.

Working Principle

After a configuration template is created, a linked list is created in the memory to store commands in the configuration template. A line ID is required for each stored command to uniquely identify the command and determine the location of the command in the linked list. In this case, users can add, modify, and delete specific commands by line ID. To prevent command loss due to a process restart or device restart, commands in a configuration template are stored in file format, and command changes in the template will be synchronized to the file.

1.4 Configuration

Configuration	Description and Command	
Creating a Configuration Template	⚠ (Optional) It is used to create a configuration template.	
	cfgmg template	Creates a configuration template.

Maintaining Commands in a Configuration Template	(Optional) It is used to maintain commands in a configuration template.	
	import	Imports commands from a file to a configuration template.
	append	Appends commands to the end of a configuration template.
	insert	Inserts a command into a specific location of a configuration template.
	line	Modifies a command in a specific location of a configuration template.

1.4.1 Creating a Configuration Template

Configuration Effect

- Create a configuration template.

Notes

N/A

Creating a Configuration Template

- In AC global configuration mode, create a configuration template.

Command	**cfgmg template** *temp-name*
Parameter Description	*temp-name*: Indicates the name of a configuration template. The value is a string of 1 to 31 characters. Up to 512 configuration templates can be configured for each device.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show running** or **show cfgmg template summary** command to check whether the configuration template is configured successfully.

Configuration Example

Creating a Configuration Template

Configuration Steps	• Create a configuration template in global configuration mode.
AC	`Hostname(config)#cfgmg template wlan-temp1` `Hostname(config-temp)#`
	• Check whether the configuration template is configured successfully.

AC	`Hostname#show cfgmg template summary`
	`Cfgmg Template Name`
	`1. wlan-temp1`

Common Errors

N/A

1.4.2 Maintaining Commands in a Configuration Template

Configuration Effect

- Add commands to or delete or modify commands in a configuration template.

Notes

A configuration template supports a maximum of 128 commands.

Appending Commands to a Configuration Template

- Append commands to a configuration template.

Command	**append** *command-string*
Parameter Description	*command-string*: Indicates the command line character string to be added to a configuration template. The value is a string of 0 to 255 characters. The command format is the same as that in the **show running** command output.
Defaults	N/A
Command Mode	Template configuration mode
Usage Guide	1. This command is used to append commands to the end of a configuration template. The line ID of an added command is the current maximum command line ID in the template plus 1. 2. The command format is the same as that in the **show running** command output. For example, if the format of the **wlan-config** command in the **show running** command output is **wlan-config** 1 Hostname, the command format in the configuration template is also **wlan-config** 1 Hostname. 3. This command does not have the **no** or **default** form. To delete a command in the specified line, use the **no line** command.

Inserting Commands into a Configuration Template

- Insert a command into the specified line of a configuration template.

Command	**insert** *line command-string*
Parameter Description	*line*: Indicates the ID of the line into which a command is to be inserted. The value range is from 1 to 65,536. *command-string*: Indicates the command character string to be inserted into the configuration template. The value is a string of 1 to 255 characters. The command format is the same as that in the **show running** command output.
Defaults	N/A
Command Mode	Template configuration mode
Usage Guide	1. This command is used to insert a command into the specified line of a configuration template. If a command already exists in the line, the existing command is moved to the next line after the new command is inserted. Subsequent lines with commands are moved to the next lines accordingly. 2. The command format is the same as that in the **show running** command output. For example, if the format of the **wlan-config** command in the **show running** command output is **wlan-config** 1

	Hostname, the command format in the configuration template is also **wlan-config** 1 Hostname. 3. This command does not have the **no** or **default** form. To delete a command in the specified line, use the **no line** command. 4. A configuration template supports a maximum of 128 commands.

Modifying Commands in a Configuration Template

- Add a command to or modify the command in the specified line of a configuration template.

Command	**line** *command-string*
Parameter Description	*line*: Indicates the ID of the line where a command to be added or the command to be modified resides. The value range is from 1 to 65,536. *command-string*: Indicates the command character string to be modified or inserted. The value is a string of 1 to 255 characters. The command format is the same as that in the **show running** command output.
Defaults	N/A
Command Mode	Template configuration mode
Usage Guide	1. This command is used to add a command to or modify the command in the specified line of a configuration template. If a command already exists in the line, the existing command is overwritten. If no command exists in the line, a command is added to the line. 2. The command format is the same as that in the **show running** command output. For example, if the format of the **wlan-config** command in the **show running** command output is **wlan-config** 1 Hostname, the command format in the configuration template is also **wlan-config** 1 Hostname. 3. The **no line** command is used to delete the command in the specified line.

Importing Commands to a Configuration Template

- Import commands from a file to a configuration template.

Command	**import** *filename*
Parameter Description	*filename*: Indicates the name of the file that stores the commands to be imported to a configuration template. The value is a string of 1 to 57 characters. The command line length in the file is a string of 1 to 255 characters, and each command occupies one line. The *filename* parameter is written in **path/file name** format. The file path can be the flash directory or data directory. If the flash directory is used, path in the *filename* parameter can be omitted.
Defaults	The file in the flash directory is imported.
Command Mode	Global configuration mode
Usage Guide	1. This command is used to import commands from the specified file to a configuration template. The command lines are added to the end of the configuration template and numbered by the current maximum command line ID in the template plus 1 accordingly. 2. The command format is the same as that in the **show running** command output. For example, if the format of the **wlan-config** command in the **show running** command output is **wlan-config** 1 Hostname, the command format in the configuration template is also **wlan-config** 1 Hostname. 3. This command does not have the **no** or **default** form. To delete a command in the specified line, use

	the **no line** command. 4. Windows or Unix file formats are supported, and the UTF-8 or GBK coded character set is supported. The coded character set can be selected based on actual requirements. If a coded character set is configured for the device system, the coded character set of the device system is used. Otherwise, it is recommended that the GBK coded character set be used, which is the default coded character set of the device system in a Chinese version and can prevent abnormal display during Web page access. In addition, the coded character set must be the same as that of the terminal simulation program to prevent abnormal display. 5. Each line in the file is a command, which is the same as the **append** command. *command-string* is a string of up to 255 characters. If the number of character strings of a command exceeds the limit, the command fails to be imported and all subsequent commands are stopped to be imported.

Verification

- Run the **show this** or **show cfgmg template name** command to check whether the commands are appended to the configuration template successfully.

Configuration Example

↘ Appending, Inserting, or Importing Commands to or Modifying Commands in a Configuration Template

Configuration Steps	Append, insert, or import commands to or modify commands in a configuration template.
	● Append commands to a configuration template in template configuration mode.

AC	`Hostname(config)#cfgmg template wlan-temp1`
	`Hostname(config-temp)#append wlan-config 1 Hostname`
	`Hostname(config-temp)#append tunnel local`

	● Check whether the commands are appended to the configuration template successfully.

AC	`Hostname(config-temp)#show this`
	`Building configuration...`
	`!`
	`line 1 wlan-config 1 Hostname`
	` line 2 tunnel local`
	`!`
	`end`

	● Import commands to a configuration template in template configuration mode.

AC	`Hostname(config)#cfgmg template wlan-temp2`
	`Hostname(config-temp)#import new-branch-cfg.txt`
	
	`For example, the content of the new-branch-cfg.txt file is as follows:`
	`wlan-config 2 Hostname2`
	`tunnel local`
	`wlan-config 3 Hostname3`
	`tunnel local`

	● Check whether the commands are imported to the configuration template successfully.

AC	Hostname(config-temp)#show this Building configuration... ! cfgmg template wlan-temp2 line 1 wlan-config 2 Hostname2 line 2 tunnel local line 3 wlan-config 3 Hostname3 line 4 tunnel local ! end
	● Insert commands into a configuration template in template configuration mode.
AC	Hostname(config)#cfgmg template wlan-temp3 Hostname(config-temp)#insert 10 wlan-config 100 Hostname Hostname(config-temp)#insert 10 wlan-config 22 Hostname
	● Check whether the commands are inserted into the configuration template successfully.
AC	Hostname(config-temp)#show this Building configuration... ! line 10 wlan-config 22 Hostname line 11 wlan-config 100 Hostname ! end
	● Add commands to or modify commands in a configuration template in template configuration mode.
AC	1: Add a command to the specified line. Hostname(config)#cfgmg template wlan-temp4 Hostname(config-temp)#line 10 wlan-config 22 Hostname Hostname(config-temp)#line 50 wlan-config 50 Hostname 2: Modify the command in the specified line. Hostname(config)#cfgmg template wlan-temp4 Hostname(config-temp)#line 10 wlan-config 10 Hostname 3: Delete the command in the specified line. Hostname(config)#cfgmg template wlan-temp4 Hostname(config-temp)#no line 50
	● Check whether the commands are added or modified successfully.

```
1: Check whether a command is added to the specified line successfully.
Hostname(config-temp)#show this
Building configuration...
!
line 10 wlan-config 22 Hostname
 line 50 wlan-config 50 Hostname
!
end
2: Check whether the command in the specified line is modified successfully.
Hostname(config-temp)#show this
Building configuration...
!
line 10 wlan-config 10 Hostname
 line 50 wlan-config 50 Hostname
!
end
3: Check whether the command in the specified line is deleted successfully.
Hostname(config-temp)#show this
Building configuration...
!
line 10 wlan-config 10 Hostname
!
end
```

Common Errors

1. The imported file is not in .txt format.
2. Commands in the imported file are not written based on the rule of one line for one command.

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show cfgmg template summary	Displays the list of configuration templates.
show cfgmg template name	Displays commands in a configuration template.

Debugging

N/A

1 Configuring APMG

1.1 Overview

Tailored for the wireless network architecture that supports centralized management, AP Management (APMG) implements centralized management and configuration of access points (APs).

A Wireless Local Area Network (WLAN) refers to a network system that allows different PCs to communicate and share resources with each other by interconnecting different PCs through wireless communications technologies. The essence of a WLAN is that PCs are interconnected with each other in wireless rather than wired mode, thus constructing a network and allowing clients to move more flexibly.

A traditional WLAN adopts the fat AP network architecture in which APs work independently. On the traditional WLAN, each AP must be separately configured and managed, which increases the complexity of network management and O&M workload. In addition, problems, such as radio interference between APs and roaming of wireless users, cannot be effectively resolved due to poor collaboration between APs. To address these issues, a wireless network architecture that supports centralized management emerges. This network architecture consists of access controllers (ACs) and fit APs, and is also called fit AP network architecture. In this network architecture, APs are connected to ACs through the Control and Provisioning of Wireless Access Points (CAPWAP) tunnels, and ACs perform centralized management on APs.

Protocols and Standards

- RFC5415: Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification
- RFC5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11

1.2 Application

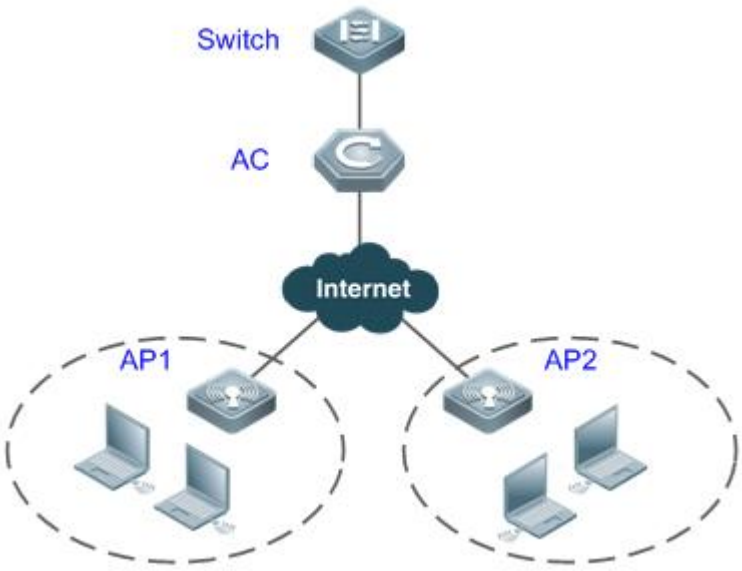
Application	Description
Fit AP Network	The network architecture consists of switches, ACs, and fit APs.

1.2.1 Fit AP Network Architecture

Scenario

A fit AP network consists of switches, ACs, and fit APs. In the fit AP network structure, APs serve as the wireless access points only and do not have the management or control function. The AC manages all the APs in a centralized manner, and delivers control policies to APs, eliminating the need to configure APs separately. As shown in Figure 1-1, the AC is connected to multiple APs through the CAPWAP tunnels. Users only need to perform configuration management on all the connected APs through the AC.

Figure 1-1 Fit AP Network Topology



Remarks	AP1 and AP2 are fit APs.

Deployment

- Configure an indicative name for each AP so that the AP can be configured based on the name.
- Create a WLAN and configure WLAN-related attributes.
- Create an AP group and add APs to a specified AP group so that all the APs in this AP group can be configured in a centralized manner.
- Deploy the WLAN on all the APs in the AP group through configuration of the AP group, after which the APs can provide the WLAN access service for wireless users.

1.3 Features

Basic Concepts

AP

AP is an access point used by wireless clients to access a wired network. It is equivalent to a bridge for communication between wireless clients and a wired network.

AC

AC is a wireless access controller. It is interconnected with APs over the wired network to manage and control APs in a centralized manner.

AC Cluster

AC cluster is also called AC redundancy. With this function, multiple ACs with different priorities are designated for an AP. When the connection between the AP and a high-priority AC is down, the AP is connected to a low-priority AC (standby

AC). When the connection to the high-priority AC is recovered, the AP disconnects the CAPWAP tunnel with the low-priority AC, and sets up a CAPWAP tunnel with the high-priority AC again.

Overview

Feature	Description
Configuration of AC Authorization Key	Configures the license activation/deactivation key of an old version system.
Configuration of AC Parameters	Configures parameters, such as the AC name and Trap message control.
Configuration of AP Parameters	Configure parameters, such as the AP name, Telnet user name and password, and periodical statistics report interval.
Configuration of AP Behaviors	Configures AP behaviors, including daily scheduled restart of an AP, restoration of AP factory settings, and AP reset.
AP Group Management	Manages APs through the AP group to reduce the workload incurred by configuring APs one by one.
AP Quantity Limit	Limits the maximum number of APs that can be connected to the AC.
AP Compliance Check	Implements the AP access control based on the bound MAC address.
AP Access Authentication	Authenticates the AP access.
AP Priority	Implements the AP access control based on the priority.
AC Cluster	Implements AC redundancy by using the AC cluster to reduce the AC single-point failure and improve availability of the wireless network.
AC Hot	Sets up the hot standby connection to ensure that the AP can set up two CAPWAP tunnels.
WLAN Configuration	Configures a WLAN and deploys the WLAN on APs to provide WLAN services for wireless users.
AP Backup	Configures the AP backup function to improve availability of the wireless network.
Hierarchical Permission-based AC Management	Virtualizes one AC into multiple ACs through permission control.
AP Virtualization	Virtualizes an AP into multiple APs to be managed by different ACs.
Default SSID Configuration	Configures the default SSID of an AP. When no tunnel is available, the AP uses the default SSID to provide the WLAN access service.
Automatic AP Grouping	Assigns an AP to a specified AP group according to the matching rules after the AP goes online.
AC/AP Version Access Control	Configures the AC version features to specify the AP software version features that can access the AP.

1.3.1 Configuration of AC Authorization Key

The AC authorization key is a license activation key of an earlier version system, and used to control the upper limit of APs supported by an AC.

Working Principle

The license activation key is used to control the upper limit of APs supported by an AC. You can use a command to configure or add a valid license. The input license must be valid, effective, and applicable to the local device. If the upper limit of APs supported by the AC is reached, no new license can be configured or added. You can also inactivate a license using the **no set license** *activation-key* command.

1.3.2 Configuration of AC Parameters

AC parameters include the AC name, Trap message control, and AC network access server (NAS) ID.

Working Principle

Configuration of AC parameters does not involve any working principle.

1.3.3 Configuration of AP Parameters

AP parameters include the AP name, Telnet user name and password, and periodical statistics report interval.

Working Principle

The AC configures AP parameters by sending CAPWAP packets to an AP.

1.3.4 Configuration of AP Behaviors

AP behaviors include daily scheduled restart of an AP, restoration of AP factory settings, and AP reset.

Working Principle

Configuration of AP behaviors is implemented by delivering CAPWAP packets to an AP. The AP performs the related behaviors based on the configuration delivered by the AC.

1.3.5 AP Group Management

The AC manages APs through the AP group. All APs in an AP group can be configured through the AP group, which reduces the configuration workload. Configurations of the AP group take effect on all the APs in the group. For the same configuration, if both the AP-based configurations and the AP-group-based configurations exist, the AP-based configurations prevail.

Working Principle

The system automatically creates a default AP group, which is named **default**. By default, APs are added to the **default** group. You can create AP groups and add APs to these groups to manage APs by group.

1.3.6 AP Quantity Limit

The maximum number of APs that can be connected to an AC is configured to limit the maximum AP load of the AC, thus avoiding overload of the AC.

Working Principle

When the number of APs connected to the AC reaches the maximum number, no more APs can access the AC.

Each wall-plate AP is treated as 0.5 device when the maximum number of APs that can be connected to an AC is calculated. That is, the maximum number of wall-plate APs that can be connected to an AC is twice the number of APs supported by the AC.

1.3.7 AP Compliance Check

The AP compliance check is also called AP access control based on the bound MAC address. If the AP compliance check is enabled, only APs with some specified MAC addresses are allowed to access the AC. This prevents access of unwanted APs and enhances security of the wireless network.

Working Principle

An AP is allowed to access the AC only when the AP configuration that is bound with the MAC address of this AP exists on the AC; otherwise, access of the AP to the AC is denied. To prevent binding MAC addresses with a large number of AP configurations, the MAC addresses of currently online APs are automatically bound when the AP compliance check is enabled. In addition, MAC addresses can be bound with specified AP configurations.

1.3.8 AP Access Authentication

AP access authentication can be implemented based on the serial number, password, or certificate. With the AP access authentication function, only authorized APs can access the AC.

Working Principle

When an AP sends an access request to the AC and uploads the authentication information, the AC verifies the authentication information. Only the AP that is successfully authenticated can access the AC.

1.3.9 AP Priority

The AP priority function is an advanced version of the AP quantity limit function. With this function, when the current number of APs connected to the AC reaches the upper limit, if a high-priority AP sends an access request, the AC proactively forces a low-priority AP to go offline and allows the access of the high-priority AP.

Working Principle

When an AP sends an access request, the current number of APs connected to the AC reaches the upper limit, and the AP priority function is enabled, the AC first compares the priorities. If the priority of an online AP is lower than the requesting AP, the AC forces a low-priority AP to go offline and allows the access of the high-priority AP.

1.3.10 AC Cluster

On the one hand, the AC cluster function enhances reliability of the AC cluster. On the other hand, this function controls the home AC of APs in stable conditions based on the priority to facilitate AP management.

Working Principle

See the CAPWAP protocol in RFC5415.

1.3.11 AC Hot Standby

The AC hot standby function enables millisecond-level switchover of the CAPWAP tunnels between ACs and APs when an AC is unreachable or faulty, thus ensuring uninterrupted services for associated STAs to the maximum extent.

Working Principle

Two tunnels are set up between an AP and two ACs, and one tunnel works in active mode, and the other works in standby mode. The AC corresponding to the active tunnel serves as the active device that processes all services and transfers the service status information to the standby device for backup purpose. The standby device does not process services, and only backs up the service data. If the active AC is faulty, the standby AC takes over all services.

For details about AC hot standby, see Configuring WLAN Hot Standby.

1.3.12 WLAN Configuration

Create and deploy a WLAN on an AP so that the AP can provide the WLAN access service for wireless users.

Working Principle

The WLAN created on the AC is used for WLAN parameter configuration. The WLAN deployment information and parameters are delivered through the packets defined in the CAPWAP protocol.

1.3.13 AP Backup

The AP backup function is used to back up radio signals transmitted by APs that are physically adjacent with each other, have overlapped coverage, and transmit different radio signals. When an AP that transmits important radio signals is faulty, one or more standby APs transmit radio signals of the faulty AP to replace the faulty AP, thus ensuring stability of radio signals. This function is generally used in special scenarios. For example, in the seamless roaming scenario of the medial industry, the AP4210 with a wide coverage is an active AP, and the APD-M connected to the AP4210 serves as a standby AP of the AP4210.

Working Principle

An AP backup group is created on the AC. In this AP backup group, one AP is selected as the active AP, and other APs are standby APs. When the active AP is faulty and goes offline, the WLAN configuration of the active AP is sent to all the standby APs in the group so that the standby APs can transmit radio signals of the active AP.

1.3.14 Hierarchical Permission-based AC Management

Hierarchical permission-based AC management virtualizes one AC into multiple ACs through permission control. Currently, the hierarchical permission-based AC management function is available only on the web management system. Users can log in to the web management page by using different administrator accounts and query and configure different WLANs, AP groups, and APs. In addition, administrators can back up information of each other. When multiple administrators share the same role, these administrators have the same permissions. When one administrator cannot perform operations due to absence or other causes, another administrator can log in to the web management page by using his or her own account and perform the operations. This ensures account security.

Working Principle

A super administrator can create different roles on the AC or by logging in to the web management page, associate administrators with different roles, and assign WLANs, AP groups, and APs to the roles. When an administrator logs in to the web management page, the administrator can only query and configure the corresponding WLANs, AP groups, and APs (STAs). This ensures that different roles manage the same AC simultaneously but do not interfere with each other, achieving the effect of virtualizing one AC into multiple ACs.

1.3.15 AP Virtualization

The AP virtualization function virtualizes one AP into multiple APs. Each virtual AP establishes a connection to an AC (not in the hot standby state), and these virtual APs share physical resources of the AP. Each AC can deliver its own configurations and configure its own wireless signals to manage the AP. When an STA receives signals broadcast by an AC, the AP serving the STA reports the corresponding data to the AC. As the data channels used by the virtual APs to report data to the ACs are different and the virtual APs are not accessible to each other, the data security is improved. In addition, as the APs are controlled by multiple ACs, the AC single point of failure (SPOF) will not occur and the AP stability is improved.

Working Principle

Create an AP virtualization template on the active AC and apply the template to an AP, an AP group, or all APs. In this case, the AP establishes connections to other ACs according to configurations of the AP virtualization template and the connected ACs can deliver their own configurations to the AP.

1.3.16 Default SSID Configuration

Configure an SSID for a fit AP to provide the WLAN access service when no CAPWAP tunnel is established.

Working Principle

The AC configures a default SSID for the AP. When the AP restarts or the tunnel is disconnected, the AP uses the SSID to provide the WLAN access service.

1.3.17 Automatic AP Grouping

On a fit AP network where many APs are deployed, plan different AP groups to manage the connected APs in a diversified and unified manner to reduce repetitive configuration workload. When APs are initially connected to an AC, the APs belong to the default AP group and you need to add each AP to a specified AP group one by one, which is cumbersome. The automatic AP grouping function provides a method for grouping APs in batches according to the preconfigured network segment matching rule in the AP group, which reduces the configuration workload of administrators.

Working Principle

Configure matching rules in the AP group, such as the source IP network segment (the IP addresses of APs). After an AP goes online, the AP is automatically assigned to the AP group if the configured rules are matched.

1.3.18 AC/AP Version Access Control

When deploying APs on a thin AP network, different software feature values of APs may cause incompatibility between APs and ACs. This issue can be resolved through version access control for the AC/AP software feature values.

Working Principle

When APs are brought online on ACs, they check the software feature values of each other. APs can access ACs only when they determine that they support each other's software feature values.

1.4 Configuration

Configuration	Description and Command	
Configuring the AC Authorization Key	(Optional) To increase the number of APs supported by an AC, purchase and install a new license.	
	set license	Configures the license activation key.
	license-idle-timeout	Configures the shared aging time of a license.
Configuring an AC Name	(Optional) It is used to configure an indicative name for the AC to facilitate management.	
	ac-name	Configures the name of the local AC.
Configuring the Trap Message Control Function	(Optional) It is used to enable sending of Trap messages. Network operation and maintenance (O&M) can be implemented based on the received Trap messages.	
	acctrl-trap	Configures whether the AC sends specified Trap messages.
Configuring the NAS ID of an AC	(Optional) By default, the NAS ID is the MAC address of the AC in dotted decimal notation.	
	nas-id	Configures the NAS ID of the AC in AC configuration mode.
Creating an AP Configuration	(Optional) It is used to create an AP configuration to configure a specified AP.	
	ap-config	Adds an AP configuration, or enters the AP configuration mode.
Creating an AP Group	(Optional) In AP group configuration mode, this command takes effect on all the online APs in the AP group.	
	ap-group	Adds an AP group configuration, or enters the AP group configuration mode.
Configuring the AP Group of an AP	(Optional) It is used to configure the AP group of a specified AP in AP configuration mode. By default, an AP belongs to the default group.	
	ap-group	Configures the AP group of an AP.
Configuring an AP Name	(Optional) It is used to configure a new name for an AP as required.	
	ap-name	Configures an AP name.
Binding an MAC Address to an AP Configuration	(Optional) It is used to bind an MAC address to an AP configuration so that the AP configuration can take effect on the AP with the MAC address.	
	ap-mac	Binds an MAC address to an AP configuration.

Configuration	Description and Command	
Configuring the User Name and Password of an AP	⚠ (Optional) It is used to modify the Telnet user name and password of an AP as required.	
	credential	Configures the user name and password of an AP.
Configuring the Interval at Which the AP Reports Statistics	⚠ (Optional) It is used to configure the interval at which the AP reports statistics as required. The default interval is 120s.	
	statistics-timer	Configures the interval at which the AP reports statistics.
Configuring the Daily Scheduled Restart Time for an AP	⚠ (Optional) It is used to configure the daily scheduled restart function for an AP to prevent the AP from working for a long time.	
	reload at	Configures the AP restart time.
Restoring Factory Settings of a Specified AP	⚠ (Optional) It is used to restore factory settings of an AP.	
	factory-reset	Restores factory settings of a specified AP.
Resetting an AP	⚠ (Optional) It is used to reset an AP.	
	reset	Resets an AP.
Configuring the AP Quantity Limit	⚠ (Optional) It is used to configure the maximum number of APs connected to the AC on demand to reduce the maximum load of the AC.	
	wtp-limit	Configures the maximum number of APs that can be connected to the AC.
Configuring the AP Compliance Check	⚠ (Optional) It is used to configure the AP compliance check to allow the access of only APs with the bound MAC addresses, thus effectively controlling the access of APs.	
	bind-ap-mac	Enables or disables the AP compliance check in AC configuration mode.
Configuring AP Access Authentication	⚠ (Optional) It is used to configure AP access authentication so that only authorized APs can access the AC, which enhances security of the wireless network.	
	ap-auth enable	Enables or disables the AP access authentication function of the AC in AC configuration mode.
	ap-auth serial-update	Updates authentication serial numbers for all online APs in AC configuration mode.
	ap-auth	Configures the access authentication information of a specified AP in AP configuration mode.
Configuring the AP Priority	⚠ (Optional) This command is available in both the AC and AP configuration modes.	
	ap-priority	Enables or disables the AP access priority function of the AC in AC configuration mode.
	priority	Configures the failover priority of a specified AP in AP configuration mode.

Configuration	Description and Command	
Configuring the AC Cluster Function	(Optional) It is used to configure the redundancy ACs of a specified AP or all APs in AP configuration mode.	
	primary-base	Configures the primary AC of an AP.
	secondary-base	Configures the secondary AC of an AP.
	tertiary-base	Configures the tertiary AC of an AP.
	backup-controller-primary	Configures the fourth AC of an AP.
	backup-controller-secondary	Configures the fifth AC of an AP.
	backup-controller-tertiary	Configures the sixth AC of an AP.
Configuring the AC Hot Standby Function	(Optional) It is used to adjust the hot standby connection parameters.	
	ap-group	Binds an AP group.
	peer-ip	Configures the peer IP address.
	peer-ipv6	Configures the peer IPv6 address.
	peer-ipv6 enable	Enables the peer IPv6.
Configuring the AP System Log Information	(Optional) It is used to configure the log information of a specified AP or all APs in AP configuration mode.	
	logging on	Enables or disables the function of displaying system logs.
	logging server	Configures the address of the system logging server.
Creating a WLAN	(Optional) A WLAN must be created before it can be deployed.	
	wlan-config	Creates a WLAN, or enters the WLAN configuration mode.
Deploying a WLAN	(Optional) It is used to configure the WLAN-VLAN mapping of a specified AP group and deploy the WLAN on all the APs in the AP group.	
	interface-mapping	Configures the WLAN-VLAN mapping of a specified AP group in AP group configuration mode.
Configuring WLAN SSID Broadcasting	(Optional) It is used to configure SSID broadcasting as required. SSID broadcasting is disabled by default.	
	enable-broad-ssid	Enables or disables SSID broadcasting of a specified WLAN in WLAN configuration mode.
Configuring the NAS ID of a WLAN User	(Optional) It is used to configure the NAS ID of a specified WLAN user. The NAS ID is a null string by default.	
	nas-id	Configures the NAS ID of a specified WLAN user.
Configuring the Fit or Fat AP Mode	(Optional) It is used to configure the fit or fat AP mode. The AP mode can be switched between the fit AP mode and the fat AP mode as required.	
	switch2fat	Switches the mode of a specified AP to the fat AP mode in AC configuration mode on the AC.

Configuration	Description and Command	
Configuring the WLAN SSID	(Optional) It is used to configure a new SSID for the WLAN as required.	
	ssid	Changes the SSID of the WLAN in WLAN configuration mode.
	ssid-code	Configures the coded character set for the SSID.
Configuring the AP Backup Function	(Optional) It is used to improve availability of the wireless network.	
	ap-backup group	Creates an AP backup group in AC configuration mode.
	ap-backup-group	Binds an AP backup group.
Configuring Hierarchical Permission-based AC Management	(Optional) It is used to assign wireless permissions and virtualize one AC into multiple ACs.	
	permit enable	Configures the local AC to enable or disable hierarchical permission-based AC management in AC configuration mode.
	master-group	Adds a role and enters the role configuration mode.
	master-group (AP configuration mode)	Assigns an AP to a specific role in AP configuration mode.
	master-group (AP group configuration mode)	Assigns an AP group to a specific role in AP group configuration mode.
	master-group (WLAN configuration mode)	Assigns a WLAN to a specific role in WLAN configuration mode.
	webmaster (role configuration mode)	Adds or deletes an administrator in role configuration mode.
Configuring the AP Virtualization Function	(Optional) It is used to enable multiple ACs to manage the same AP.	
	virtual-ap	Creates an AP virtualization template in global configuration mode.
	ac-ip	Configures the IP address of the AC to which a virtual AP is to be connected.
	wlan-capacity	Configures the number of WLANs supported by a virtual AP.
	sta-capacity	Configures the number of STAs supported by a virtual AP.
	link-interface	Configures the uplink interface used by a virtual AP to connect to an AC.
	virtual-ap	Configures a virtual AP in single AP, AP group, and all-AP configuration modes.
	ap-idle-timeout	Configures the duration for a virtual AP to provide services after the connection between the AP and active AC is down.
Configuring the Default SSID	**offline-ssid**	Configures the WLAN access signal provided when an AP is offline.

Configuration	Description and Command	
Configuring Automatic AP Grouping	(Optional) It is used to simplify the AP grouping configuration.	
	auto-join-group match src-ip	Configures the IP matching rules for automatic AP grouping in AP group configuration mode.
Configuring the AC Software Features	(Optional) By default, the AC software feature value is configured.	
	wlan-features	Configures the software feature value of the AC.

1.4.1 Configuring the AC Authorization Key

Configuration Effect

- Increase the number of APs supported by an AC.

Notes

- A configured license takes effect permanently. That is, the license never expires. Once you configure the license, you are assigned to use the function permanently.
- The license takes effect as soon as it is configured on a device, and restart of the device is not necessary.
- Multiple licenses can be configured on the same AC. That is, the maximum number of APs supported by an AC is equal to the sum of the AP quantities authorized by the licenses, but cannot exceed the capacity of the AC.
- After being deactivated, the license cannot be installed on the device again. But you can apply for a new license for another device using this license, the old SN, the deactivation key and a new SN.
- After you deactivate a license, the number of APs allowed to go online reduces immediately. The APs that are already online are not affected.
- This command is used to import the activation key of the earlier-version license system. A new license is installed by using the license file installation command. For details, see *Software Authorization Management*.

Configuration Steps

- Optional. To increase the number of APs supported by an AC, purchase and install a new license.
- The license activation key is not installed by default.
- You can run the **set license** *activation-key* command in global configuration mode to import the activation key of the earlier-version license system.

Command	**set license** *activation-key*
Parameter Description	*activation-key*: Indicates the license activation key to be configured. The format of the license key depends on the actual situations, for example, AAAA-BBBB-CCCC-DDDD-EEEE-FFFF-GGGG-HHHH.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	A license is applicable to only the device that you specify when applying for a license, and does not take effect on other devices. The same license cannot be configured for multiple times on one device.

Command	**license-idle-timeout** *timeout*
Parameter Description	*timeout*: Indicates the aging time (in hours) of the license sharing on a license sharing network after the AC stops using the license. The value ranges from 1 to 336 (14 days).
Defaults	168 (7 days)
Command Mode	AC configuration mode
Usage Guide	This command is applicable to the license sharing scenarios, such as AC virtualization scenarios.

Verification

- Run the **show license all-license** command to display the license information and check whether the configuration is successful.
- **show license unbind-code command** to check the deactivated license.

Configuration Example

Configuring the License Activation Key

Configuration Steps	• Add a license.
AC	`Hostname#config terminal` `Hostname(config)#set license4A3F-16AB-330C-B254-42C4-E18A-24F3-15CA`
Verification	• Run the **show license all-license** command to display the license.

AC	`Hostname(config)#show license all-license`
	`Searching license in the system...`
	`There's no license installed in the system.`
	
	`-----------------------------------------`
	`There are some old version licenses:`
	
	`1. 4A3F-16AB-330C-B254-42C4-E18A-24F3-15CA 128`

Common Errors

- N/A

1.4.2 Configuring an AC Name

Configuration Effect

- Set the name of an AC to a specified string.

Notes

- The AC name is a string of 1 to 63 characters, and cannot contain any space.

Configuration Steps

- Optional. Run the **ac-name** *ac-name* command in AC configuration mode to configure a new name for an AC.
- Run the **ac-controller** command to enter the AC configuration mode.

- Run the **ac-name** command to configure an AC name in AC configuration mode on an AC.

Command	**ac-controller**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**ac-name** *ac-name* **no ac-name**
Defaults	The default AC name is Hostname_Ac_*Last six digits of MAC address*. For example, if the MAC address of an AC is 001a.a916.e7b8, the default name of this AC is Hostname_Ac_16e7b8.
Parameter Description	*ac-name*: Indicates the name of an AC. The name is a string of 1 to 63 characters, and cannot contain any space.
Command Mode	AC configuration mode
Usage Guide	Different names can be configured for different ACs to facilitate management. The default AC name is Hostname_Ac_*Last six digits of MAC address*. For example, if the MAC address of an AC is 001a.a916.e7b8, the default name of this AC is Hostname_Ac_16e7b8.

Verification

- Run the **show ac-config** command to check the current AC name and determine whether the configuration is successful.

Configuration Example

Configuring the Name of an AC as Hostname-AC1

Configuration Steps	• Enter the AC configuration mode. • Configure an AC name.

AC	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#`
	`Hostname(config-ac)#ac-name Hostname-AC1`

Verification	• Run the **show ac-config** command to display the AC name.

AC	`Hostname#show ac-config`
	
	`ac_name :Hostname-AC1`

Common Errors

- N/A

1.4.3 Configuring the Trap Message Control Function

Configuration Effect

- The AC sends the following types of Trap messages: CAPWAP tunnel up/down information, failures to add APs to the AC, CAPWAP tunnel packet decryption failures, upgrade failures, time synchronization failures, and STA online/offline information.
- By default, all the preceding Trap messages are not sent. You can run the **acctrl-trap** command in AC configuration mode to enable the AC to send specified Trap messages.

Notes

- N/A

Configuration Steps

- Optional. On the AC, enter the AC configuration mode and run the **acctrl-trap** command to configure the Trap message control function.
- The AC sends the following types of Trap messages: CAPWAP tunnel up/down information, failures to add APs to the AC, CAPWAP tunnel packet decryption failures, upgrade failures, time synchronization failures, and STA online/offline information.

Command	**acctrl-trap** [**acap-updown-ctrl** | **acap-joinfail-ctrl** | **acap-decryeroreport-ctrl** | **acap-imageupdt-ctrl** | **acap-microap-ctrl** | **acap-snmpcache-ctrl** | **acap-timestamp-ctrl** | **acsta-oper-ctrl**]
Parameter Description	**acap-updown-ctrl**: Determines whether to send the Trap messages that contain the CAPWAP tunnel up/down information. **acap-joinfail-ctrl**: Determines whether to send the Trap messages that contain information about failures of adding APs to the AC. **acap-decryeroreport-ctrl**: Determines whether to send the Trap messages that contain information about CAPWAP tunnel packet decryption failures. **acap-imageupdt-ctrl**: Determines whether to send the Trap messages that contain information about the .bin file upgrade failures of the AP. **acap-microap-ctrl**: Controls forwarding of trap messages about status of micro APs. **acap-snmpcache-ctrl**: Controls forwarding of trap messages about cache for SNMP trap message updates. **acap-timestamp-ctrl**: Determines whether to send the Trap messages that contain the time synchronization information. **acsta-oper-ctrl**: Determines whether to send the Trap messages that contain the STA online/offline information.
Defaults	All types of Trap messages are not sent. You can run the **acctrl-trap** command in AC configuration mode to enable the AC to send these messages.
Command Mode	AC configuration mode
Usage Guide	This command is used to control sending of Trap messages on the AC.

Verification

- Run the **show ac-config** command to display the sending status of various Trap messages.

Configuration Example

Enabling the AC to Send the Trap Messages That Contain Information About Failures to Add APs to the AC

Configuration Steps	• Enter the AC configuration mode. • Enable the AC to send the Trap messages that contain information about failures to add APs to the AC. • Use the **no** form of this command to restore the default setting.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)#acctrl-trap acap-joinfail-ctrl`
Verification	• Run the **show ac-config** command to display the sending status of various Trap messages.

AC	`Hostname#show ac-config`
	`acctrl-trap acap-updown-ctrl :Disable`
	`acctrl-trap acap-joinfail-ctrl :Enable`
	`acctrl-trap acap-decryeroreport-ctrl :Disable`
	`acctrl-trap acap-imageupdt-ctrl :Disable`
	`acctrl-trap acap-timestamp-ctrl :Disable`
	`acctrl-trap acsta-oper-ctrl :Disable`

Common Errors

- N/A

1.4.4 Configuring the NAS ID of an AC

Configuration Effect

- On the WLAN, the NAS IDs identify different hot spot areas. By default, the NAS ID of an AC is the MAC address of the AC in dotted decimal notation.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC, enter the AC configuration mode and run the **nas-id** command to configure the NAS ID.

Command	**nas-id** *ac-nas-id*
Parameter Description	N/A
Defaults	MAC address of the AC in dotted decimal notation.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Setting the NAS ID of the AC to 123456789

Configuration Steps	• Enter the AC configuration mode. • Configure the NAS ID.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)#nas-id123456789`
Verification	• Run the **show running** command to display the AC configuration.

AC	`Hostname#show running`
	`!`
	`ac-controller`
	`nas-id 123456789`
	`!`

Common Errors

- N/A

1.4.5 Creating an AP Configuration

Configuration Effect

- Create an AP configuration with the specified name, and enter the AP configuration mode.
- If the AP configuration corresponding to a name already exists, you can directly enter the AP configuration mode after the command is executed.
- The *ap-name* parameter indicates the name of the AP configuration. When an AP goes online, the AP name uploaded by the AP matches with the AP configuration name to determine the mapping between the AP and AP configuration.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC, enter the global configuration mode and run the **ap-config** *ap-name* command to create an AP configuration.

Command	**ap-config** *ap-name*
Parameter Description	*ap-name*: Indicates the name of the AP configuration.
Defaults	No AP configuration is created.
Command Mode	Global configuration mode
Usage Guide	1. You can run the **ap-config all** command to enter the all-AP configuration mode. Configurations

	made in this mode take effect on all APs associated with the current AC. Configurations made in AP configuration mode take precedence over configurations made in all-AP configuration mode. If configurations (non-default settings) exist in AP configuration mode (entered by running the **ap-config** *ap-name* command), such configurations are preferentially used; otherwise, configurations made in all-AP configuration mode (entered by running the **ap-config all** command) are used.

Verification

- Run the **show ap-config running** *ap-name* command to display the configuration of the AP.

Configuration Example

Creating an AP Configuration Named Hostname_AP

Configuration Steps	● Create an AP configuration named **Hostname_AP**.

AC	`Hostname(config)#ap-config Hostname_AP`
	`You are going to config AP(Hostname_AP), which is not on line now.`
	`Hostname(config-ap)#`

Verification	● Run the **show ap-config running** command to display the configuration of the AP.

AC	`Hostname#show ap-config running Hostname_AP`
	`!`
	`ap-config Hostname_AP`
	`!`

Common Errors

- N/A

1.4.6 Creating an AP Group

Configuration Effect

- The AC manages APs through the AP group. All the APs in an AP group can be configured through the AP group, which reduces the configuration workload. Configurations of the AP group take effect on all the APs in the group.

Notes

- The default group is created automatically by the system, and cannot be deleted.
- When an AP group is deleted, APs of this group are automatically moved to the default group.
- Configurations made in different configuration modes take effect in descending order: ap-config ap-name > ap-group > ap-config all.

Configuration Steps

- Optional.
- On the AC, enter the global configuration mode, and run the **ap-group** *ap-group-name* command to create an AP group.

Command	**ap-group** *ap-group-name*

Parameter Description	***ap-group-name***: Indicates the name of an AP group.
Defaults	An AP group named **default** is automatically created by default after the system is started. This group can neither be created nor deleted.
Command Mode	Global configuration mode
Usage Guide	When the **no** form of the command is used to delete an AP group, APs of this group are automatically moved to the default group.

Verification

- Run the **show running** command to display configurations of all AP groups.

Configuration Example

↘ Creating an AP Group Named APG-1

Configuration Steps	● In global configuration mode, run the **ap-group** command to create an AP group.
AC	`Hostname(config)#ap-group APG-1` `Hostname(config-ap-group)#`
Verification	● Run the **show running** command to check whether the AP group named **APG-1** exists.

AC	`Hostname#show running`
	`!`
	`ap-group APG-1`
	`!`

Common Errors

- N/A

1.4.7 Configuring the AP Group of an AP

Configuration Effect

- An AP group must already exist if you want to add an AP to this group.
- By default, APs belong to the default AP group, that is, the AP group named **default**.
- APs inherit all configurations of the AP group to which APs belong. If the same configuration exists in the specified AP configurations (**ap-config** *ap-name*), all AP configurations (**ap-config all**), and AP group configurations, the configurations take effect in descending order: specified AP configurations > AP group configurations > all AP configurations. Therefore, if the AP group of an AP changes, AP group configurations inherited by this AP change as well.

Notes

- N/A

Configuration Steps

- Optional.

- Run the **ap-config** command to create an AP group or enter the AP configuration mode.
- On the AC, enter the AP configuration mode and run the **ap-group** command to configure the AP group of an AP.

Command	**ap-config** *ap-name*
Parameter Description	*ap-name*: Indicates the name of the AP configuration.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**ap-group** *ap-group-name*
Parameter Description	*ap-group-name*: Indicates the name of an AP group.
Defaults	APs are automatically added to the default group.
Command Mode	AP configuration mode
Usage Guide	When an AP group is deleted, APs of this group are automatically moved to the default group.

Verification

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

Configuration Example

Configuring the AP Group to Which Hostname-AP1 Belongs

Configuration Steps	• Create an AP group named **apg-1**. • Enter the AP configuration mode. • Use the **no** form of this command to restore the default AP group, that is, the AP group named **default**.

AC	`Hostname(config)#ap-group apg1`
	`Hostname(config-ap-group)#`
	`Hostname(config)#ap-config Hostname-AP1`
	`Hostname(config-ap)#`
	`Hostname(config-ap)#ap-group apg-1`

Verification	• Run the **show ap-config running** command to display the configuration of the AP.

AC	`Hostname(config)#show ap-config running Hostname-AP1`
	`!`
	`ap-config Hostname-AP1`
	`ap-group apg-1`
	`!`

Common Errors

- N/A

1.4.8 Configuring an AP Name

Configuration Effect

Configure an AP name on the AC.

- If the AP is online, the configuration of the AP name takes effect immediately. In addition, the AP name in the AP configuration mode (that is, the string next to **ap-config**) is immediately replaced by the new name.
- If the AP is offline, the configuration of the AP name takes effect after the AP goes online, and the AP name in the AP configuration mode is not replaced by the new name until the AP goes online.
- After the AP name is configured, you can continue to configure this AP without exiting from the AP configuration mode.
- If the corresponding AP is online, the **no** form of the command is not supported.
- If the corresponding AP is offline, the **no** form of the command can be used to delete the AP name configuration that is not effective.
- If the new name is already in use, the configuration fails.

Configure an AP name on the AP.

- If the CAPWAP tunnel is not set up, the AP name is configured directly.
- If the CAPWAP tunnel is set up, the AP name is configured first. Then the CAPWAP tunnel will be disconnected and set up again. If the AP name is already configured on the AC or configured offline, this AP name prevails.

Notes

- The AP name is a string of up to 64 characters, and cannot contain any space.
- The AP name cannot be configured as **all** or **AP**.
- Avoid configuring the same AP name for different offline APs. If the same AP name is configured for different offline APs, the new name takes effect on the AP that goes online first, and the APs that go online later still use the original names.
- Configuring the AP name on the AP only takes effect in fit AP mode.

Configuration Steps

- Optional. You can run the **ap-name** *ap-name* command in AP configuration mode to configure an AP name. You are advised to configure an indicative AP name to facilitate management.
- On the AC, enter the AP configuration mode and run the **ap-group** command to configure an AP name.

Command	**ap-name** *name*
Parameter Description	*name*: Indicates the name of an AP. The name cannot contain any space.
Defaults	The AC uses the name uploaded by the AP as the AP name. In the factory settings, the MAC address is often used as the name of an AP.
Command Mode	AP configuration mode
Usage Guide	1. Do not configure the AP name as **all** or **AP**. 2. After the command is executed, the command mode of an online AP is the command mode of the

	AP with the new name, and you can continue to configure other attributes of the AP without existing from the command mode. The command mode of an offline AP remains unchanged.

Verification

- Run the **show ap-config running** command to display the configuration of the AP.
- Run the **show ap-config summary** command to check whether the name of the online AP is the new name.

Configuration Example

Changing the Name of an Online AP from Hostname-AC1 to Hostname-AC2

Configuration Steps	• Enter the AP configuration mode. • Configure the name of an AP.
AC	`Hostname(config)#ap-config Hostname-AC1` `Hostname(config-ap)#ap-name Hostname-AC2`
Verification	• Run the **show ap-config running** command to display the configuration of the AP. • Run the **show ap-config summary** command to query the name of the online AP.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config Hostname-AC2`
	`!`
	`Hostname#show ap-config summary`
	`========= show ap status =========`
	`Radio: Radio ID or Band: 2.4G = 1#, 5G = 2#, 6G = 3#`
	`E = enabled, D = disabled, N = Not exist`
	`Current Sta number/Max Sta number supported`
	`Channel: * = Global`
	`Power Level = Percent`
	
	`Online AP number: 0`
	`Offline AP number: 1`
	
	`AP Name IP Address Mac Address Radio 1`
	`Radio 2 Up/Off time State`
	`---------- ---------- ----------`
	`---------- ---------- ---------- -----`
	`ap1 10.0.20.15 00d0.f822.33b0 1 E 0`
	`1*/2.4G 100 N -/- - - 0:00:16:03 Quit`

Changing the Name of an Offline AP from Hostname-AC1 to Hostname-AC2

Configuration Steps	• Enter the AP configuration mode. • Configure the name of an AP.
AC	`Hostname(config)#ap-config Hostname-AC1` `Hostname(config-ap)#ap-name Hostname-AC2`
Verification	• Run the **show ap-config running** command to display the configuration of the AP.

AC	Hostname#show ap-config running ! ap-config Hostname-AC1 ap-name Hostname-AC2 !

Common Errors

- N/A

1.4.9 Binding an MAC Address to an AP Configuration

Configuration Effect

- In AP configuration mode, run the **ap-mac** command to bind an MAC address to an AP configuration so that the AP configuration takes effect only on the AP with the MAC address.
- Generally, when an AP goes online, it determines the configuration to be used based on the mapping between the AP name and the AP configuration name. MAC address binding is a stronger binding relationship than name mapping, and takes precedence over name mapping. Therefore, when an AP goes online, the AP uses the configuration so far as the MAC address bound to the AP configuration is the same as the MAC address of the AP.
- If no MAC address is bound to an AP configuration, the MAC address is automatically bound when the corresponding AP goes online. This binding still takes effect when the AP goes offline. That is, the binding configuration will be automatically generated when the AP goes online.
- MAC address binding is also used for the AC access control function configured by using the **bind-ap-mac** command. For details, see the configuration description of this command.
- You can bind a specified MAC address only to the configuration of an offline AP.
- In the hot standby environment, you can ensure consistency of configurations between two ACs by binding the MAC addresses with AP configurations.

Notes

- You can bind a specified MAC address only to the configuration of an offline AP.

Configuration Steps

- Optional.
- On the AC, enter the AP configuration mode and run the **ap-mac** command to bind an MAC Address to an AP configuration.

Command	**ap-mac** *ap-mac-address*
Parameter Description	*ap-mac-address*: Indicates the MAC address that is bound.
Defaults	No AP configuration is bound to the MAC address by default. You can bind the MAC address of an AP to the AP configuration to forcibly apply this AP configuration to the AP with the MAC address.
Command Mode	AP configuration mode

Usage Guide	The **ap-mac** *ap-mac-address* command is applicable to configurations of offline APs. You can use this command to specify the MAC address of an offline AP so that the AP configuration can be located directly based on the MAC address after the AP goes online.

Verification

- Run the **show ap-config running** command to display the MAC address binding of the AP.

Configuration Example

Binding the Offline AP Hostname-AP1 to the MAC Address 001a.a979.1234

Configuration Steps	● Enter the AP configuration mode. ● The **no** form of the command is used to delete the MAC address binding.
AC	`Hostname(config)#ap-config Hostname-AP1` `Hostname(config-ap)#ap-mac 001a.a979.1234`
Verification	● Run the **show ap-config running** command to display the configuration of the AP.

AC	`Hostname(config)#show ap-config running Hostname-AP1`
	`!`
	`ap-config Hostname-AP1`
	`ap-mac 001a.a979.1234`
	`!`

Common Errors

- N/A

1.4.10 Configuring the User Name and Password of an AP

Configuration Effect

- Unauthorized users may directly login to an AP and modify the AP configuration through Telnet, which affects normal running of the WLAN. To prevent this problem, you can configure the Telnet user name and password of a specified AP.
- The **credential** command can be used in **ap-config** *ap-name*, **ap-group**, or **ap-config all** configuration mode. Configurations made by using the **credential** command take effect in descending order: **ap-config** *ap-name* > **ap-group** > **ap-config all**.

Notes

- N/A

Configuration Steps

Configuring the Username and Password for an AP

- Optional. You can run the **credential** *user-name password* command to configure a new Telnet user name and password in AP configuration mode to enhance security.
- On the AC, enter the AP or AP group configuration mode and run the **credential** command for configuration.

Command	**credential** *user-name password*
Parameter Description	*user-name*: Indicates the user name. A user name cannot contain any space. *password*: Indicates the password. A password cannot contain any space.
Defaults	The AC uses factory settings of the Telnet user name and password of an AP. You can change the Telnet user name and password of an AP as required to facilitate management.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Configuring the Username and Security Password

- (Optional) You can run the **credential username** *user-name* **password** { **0** | **7** } *password* command to configure a username and a security password for secure Telnet connection.
- A password contains at least eight characters and must be a combination of at least three types of the following: lowercase letters, uppercase letters, special characters, and numbers.
- On the AC, enter the AP configuration mode or AP group configuration mode and run the **credential** command.

Command	**credential username** *user-name* **password** { **0**	**7** } *password*
Parameter Description	*user-name*: Indicates the username without spaces. **0**: Utilizes the cleartext password. It contains at least eight characters and must be a combination of at least three types of the following: lowercase letters, uppercase letters, special characters, and numbers. **7**: Utilizes the ciphertext password that complies with the encryption standard. *password*: Indicates the password without spaces. It contains at least eight characters and must be a combination of at least three types of the following: lowercase letters, uppercase letters, special characters, and numbers.
Defaults	N/A
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	To configure a cyphertext password, you can copy one from the existing configuration.

Verification

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

Configuration Example

Configuring the User Name and Password of Hostname-AP1

Configuration Steps	● Configure the user name and password of Hostname-AP1.
AC	`Hostname(config)#ap-config Hostname-AP1` `Hostname(config-ap)#credential user pass`
Verification	● Run the **show ap-config running** command to display the configuration of the AP.
AC	`Hostname(config)#show ap-config running Hostname-AP1` `!`

	ap-config Hostname-AP1 credential user pass !

Configuring a Username and a Security Password

Configuration Steps	● Configure the username as **admin1** and set the password to **ruijie@123** on AP1. ● Configure the username as **admin2** and set the password to **1007072e0f1b4f2d704078** on AP2.
AC	Hostname(config)#ap-config AP1 Hostname(config-ap)#credential username admin1 password 0 ruijie@123 Hostname(config-ap)#exit Hostname(config)# ap-config AP2 Hostname(config-ap)#credential username admin2 password 7 1007072e0f1b4f2d704078 Hostname(config-ap)#exit
Verification	Run the **show ap-config running** command to display the AP configuration.
AC	Hostname(config)#show ap-config running ! ap-config AP1 credential username admin1 password 7 1007072e0f1b4f2d704078 ! ap-config AP2 credential username admin2 password 7 1007072e0f1b4f2d704078 !

Common Errors

- N/A

1.4.11 Configuring the Interval at Which the AP Reports Statistics

Configuration Effect

- Run the **statistics-timer** command to configure the interval at which the AP reports statistics.

Notes

- N/A

Configuration Steps

- Optional. You can adjust the interval based on the statistics accuracy requirement and loads on the AC and AP.
- On the AC, enter the AP or AP group configuration mode and run the **statistics-timer** command for configuration.

Command	**statistics-timer** *timer-interval*
Parameter Description	*timer-interval*: Indicates the interval that the AP reports statistics, in seconds.
Defaults	120s

Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Setting the Interval at Which Hostname-AP1 Reports Statistics to 300s

Configuration Steps	● Set the interval at which Hostname-AP1 reports statistics to 300s. ● Use the **no** form of the command to restore the default interval at which Hostname-AP1 reports statistics.
AC	`Hostname(config)#ap-config Hostname-AP1` `Hostname(config-ap)#statistics-timer 300`
Verification	● Run the **show ap-config running** command to display the configuration of the AP.

AC	`Hostname(config)#show ap-config running Hostname-AP1`
	`!`
	`ap-config Hostname-AP1`
	`statistics-timer 300`
	`!`

Common Errors

- N/A

1.4.12 Configuring the AP System Log Information

Configuration Effect

- Configure the function of displaying the AP system logs, and set the IP address of the server that records the AP system logs.

Notes

- N/A

Configuration Steps

- Optional.
- Run the **logging on** command to display system logs of a specified AP.
- Run the **logging server** *ip-address* **[udp-port** *num***]** command to configure the IP address of the system log server of a specified AP.

Command	**loggingon**
Parameter Description	N/A
Defaults	The system logs are displayed.

Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Command	**logging server** *ip-address*[**udp-port** *num*]
Parameter Description	*ip-address*: Indicates the IP address of the host that receives the log information. num: Indicates the port number of the host that receives the log information. This parameter is optional.
Defaults	N/A
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	You can configure at most five log server addresses. The log information will be sent simultaneously to all the configured log servers.

Verification

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

Configuration Example

Disabling the Function of Displaying System Logs on Hostname-AP1

Configuration Steps	• Enter the AP configuration mode. • Disable the function of displaying system logs.
AC	`Hostname(config)#ap-config Hostname-AP1` `Hostname(config-ap)#no logging on`
Verification	• Run the **show ap-config running** command to display the configuration of the AP.

AC	`Hostname(config)#show ap-config running Hostname-AP1`
	`!`
	`ap-config Hostname-AP1`
	`no logging on`
	`!`

Configuring the Log Server Address of Hostname-AP1

Configuration Steps	• Enter the AP configuration mode. • Set the log server address to 1.1.1.1.
AC	`Hostname(config)#ap-config Hostname-AP1` `Hostname(config-ap)#logging server 1.1.1.1`
Verification	• Run the **show ap-config running** command to display the configuration of the AP.

AC	`Hostname(config)#show ap-config running Hostname-AP1`
	`!`
	`ap-config Hostname-AP1`
	`logging server 1.1.1.1`
	`!`

Common Errors

- N/A

1.4.13 Configuring the Daily Scheduled Restart Time for an AP

Configuration Effect

- If APs work for a long time, the load may be too heavy, affecting the network access quality of users. To prevent this problem, you can configure the daily scheduled restart time for an AP so that the network access quality of users can be ensured every day.

Notes

- N/A

Configuration Steps

- Optional. You can enable the daily scheduled restart function based on the AP load.
- Configure the daily scheduled restart time to prevent APs from working for a long time, enhancing availability of the network.

Command	**reload at** [**everyday** | **everyweek** *day* | **everymonth date** *num* | **month** *month* **date** *num*] *time*
Parameter Description	**everyday**: Indicates that the AP restarts every day at the specified time. **everyweek**: Indicates that the AP restarts every week at the specified time. *day*: Indicates the day of each week on which the AP restarts. The options are **Mon**, **Tues**, **Wed**, **Thur**, **Fri**, **Sat**, and **Sun**. **everymonth**: Indicates that the AP restarts every month at the specified time. **date** *num*: Indicates the day of each month on which the AP restarts. The value range is from 1 to 31. **month** *month*: Indicates the month in which the AP restarts. The options are **Jan**, **Feb**, **Mar**, **Apr**, **May**, **Jun**, **Jul**, **Aug**, **Sept**, **Oct**, **Nov**, and **Dec**. *time*: Indicates the restart time in the hh:mm:ss format. Do not set this parameter to **00:00:00**.
Defaults	The daily scheduled restart function of an AP is disabled.
Command Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	● The **reload at** commands can be used in AP configuration mode, AP group configuration mode, and all-AP configuration mode and takes effect based on the configuration mode priority (AP configuration mode > AP group configuration mode > all-AP configuration mode). For example, if you configure the AP to restart every month in all-AP configuration mode and every day in AP configuration mode, the AP restarts every day. ● Only one AP restart rule can be configured in one configuration mode. When a new rule is configured, the original configuration is replaced.

Verification

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

Configuration Example

↘ Configuring Hostname-AP1 to Restart at 1:00:00 Every Day

Configuration	● Configure Hostname-AP1 to restart at 1:00:00 every day.

Steps	• Use the **no** form of the command to cancel the scheduled restart configuration.
AC	`Hostname(config)#ap-config Hostname-AP1` `Hostname(config-ap)#reload at everyday 1:00:00`
Verification	• Run the **show ap-config running** command to display the configuration of the AP.

AC	`Hostname(config)#show ap-config running Hostname-AP1`
	`!`
	`ap-config Hostname-AP1`
	`reload at everyday 1:00:00`
	`!`

Configuring All APs in the Ruijie-APG1 Group to Restart at 1:00:00 Every Day

Configuration Steps Configure all APs in the Ruijie-APG1 group to restart at 1:00:00 every day.

AC

```
Hostname(config)#ap-group Ruijie-APG1
Hostname(config-group)#reload at everyday 1:00:00
```

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

AC

```
Hostname(config)#show running-config
!
ap-group Ruijie-APG1
reload at everyday 1:00:00
!
```

Configuring All APs to Restart at 1:00:00 Every Day

Configuration Steps Configure all APs to restart at 1:00:00 every day.

AC

```
Hostname(config)#ap-config all
Hostname(config-ap)#reload at everyday 1:00:00
```

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

AC

```
Hostname(config)#show running-config
!
ap-config all
reload at everyday 1:00:00
!
```

Common Errors

- N/A

1.4.14 Restoring Factory Settings of a Specified AP

Configuration Effect

- Restore factory settings of a specified AP.
- The configuration takes effect only on an online AP.

Notes

- This operation will cause disconnection and reset of the AP.

Configuration Steps

- Optional. You can restore factory settings of a specified AP on demand.
- Restoring AP factory settings is an instant behavior of an AP. This command can restore factory settings of the AP and will trigger reset of the AP.

Command	**factory-reset** *ap-name*
Parameter Description	*ap-name*: Indicates the name of an AP.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	This command is used to restore factory settings of a specified AP. This operation will cause reset of the AP.

Verification

- After this command is executed for an online AP, this AP will go offline. After the AP goes online again, run the **show ap-config running** command to check whether factory settings of the AP are restored.

Configuration Example

Restoring Factory Settings of the Online AP Hostname-AP1

Configuration Steps	• Enter the AC configuration mode. • Restore factory settings of the online AP Hostname-AP1.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)#factory-reset Hostname-AP1`
Verification	• After this command is executed for an online AP, this AP will go offline. After the AP goes online again, run the **show ap-config running** command to check whether factory settings (null settings) of the AP are restored.

Common Errors

- N/A

1.4.15 Resetting an AP

Configuration Effect

- Reset an online AP.
- Reset all online APs.

Notes

- N/A

Configuration Steps

- Optional. You can reset one or more APs as required.
- If you configure AP reset on the AC, the corresponding AP will reset. You can configure reset of a specified AP or all online APs.

Command	**reset**{ **all** |**single** *ap-name*}
Parameter Description	**all**: Indicates that all online APs are reset. **single *ap-name***: Indicates that a specified AP is reset.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- After the configuration is completed, you can view the syslog record on the AC, indicating that the corresponding AP goes offline, and the AP will be reset.

Configuration Example

↘ Resetting Hostname-AP1

Configuration Steps	• Enter the AC configuration mode. • Reset Hostname-AP1.

AC	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#`
	`Hostname(config-ac)#reset Hostname-AP1`

Verification	• Check whether Hostname-AP1 is reset, and whether the following syslog record indicating the offline event of the AP can be viewed on the AC.
AC	`%APMG-6-RX_CTRL_MSG: AP(AP_20#3F_S:001a.a912.3456) leave AC.`

Common Errors

- N/A

1.4.16 Configuring the AP Quantity Limit

Configuration Effect

- The number of online APs connected to the AP does not exceed the configured maximum number of APs supported by the AC.

Notes

- The weight of an AP varies according to the AP model. For example, the weight of one wall-plate is 0.5 and two wall-plate APs are treated as one AP. When APs are connected to an AC, the weighted number of APs is calculated based on the weight. This command and the license control the weighted number of APs, instead of the actual number of APs.

Configuration Steps

- Optional. You can configure the AP quantity limit within the capacity range as required.

Command	**wtp-limit** *max-num*
Parameter Description	*max-num*: Indicates the maximum number of APs that can be connected to an AC.
Defaults	The quantity limit is equal to the number of APs supported by an AC.
Command Mode	AC configuration mode
Usage Guide	This command is used to configure the maximum number of APs connected to an AC. This number cannot exceed the maximum number of APs supported by the AC or the maximum number of APs allowed by the license.

Verification

- Run the **show ac-config** command to check the current AC name and determine whether the configuration is successful.

Configuration Example

↘ Setting the Maximum Number of APs Connected to the AC to 512

Configuration Steps	● Enter the AC configuration mode. ● Set the maximum number of APs connected to the AC to 512.

AC	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#wtp-limit 512`
	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#no wtp-limit`

Verification	● Run the **show ac-config** command to display the configured maximum number of APs that can be connected to the AC.

AC	`Hostname#show ac-config`
	`…`
	`max_wtp :512`
	`…`

Common Errors

- N/A

1.4.17 Configuring the AP Compliance Check

Configuration Effect

- The AP compliance check is also called AP access control based on the bound MAC address, or bind-ap-mac function. If AP compliance check is enabled, only APs that have offline configurations bound to their MAC addresses are allowed to associate with the AC.

Notes

- N/A

Configuration Steps

- Optional. You can enable the AP compliance check to allow only APs with specified MAC addresses to go online, thus implementing strict control on access of APs.
- When the AP compliance check is enabled, all online APs are automatically bound to MAC addresses. Therefore, you are advised to disable this function during network deployment and enable the function after all planned APs go online.
- When the **bind-ap-mac** function is enabled, MAC addresses automatically bound to all online APs are converted to the formal MAC address bindings, which are not automatically deleted when APs go offline.
- On the AC, you can run the **ap-mac** *X.Y.Z* command in AP configuration mode to configure the MAC address binding of an AP configuration.

Command	**bind-ap-mac**
Parameter Description	N/A
Defaults	The AP compliance check is disabled.
Command Mode	AC configuration mode
Usage Guide	This command is used to enable the AP compliance check.

Command	**ap-mac** *ap-mac-address*
Parameter Description	*ap-mac-address*: Indicates the MAC address that is bound.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	The **ap-mac** *ap-mac-address* command is applicable to offline APs. You can use this command to specify the MAC address of an offline AP so that the AP configuration can be located directly based on the MAC address after the AP goes online.

Verification

- Run the **show running** command to check whether the **bind-ap-mac** function is enabled.
- Run the **show ap-config running** command to display the MAC address binding information of AP configurations.

Configuration Example

Enabling the AP Compliance Check on an AC

Configuration Steps	● After all authorized APs go online, enter the AC configuration mode and run the **bind-ap-mac** command to enable the AP compliance check function.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)#bind-ap-mac`
Verification	● Run the **show running** command to check whether the AP compliance check function is

	enabled.

AC	`Hostname#show running`
	`!`
	`ac-controller`
	`  bind-ap-mac`
	`!`

Common Errors

- N/A

1.4.18 Configuring AP Access Authentication

Configuration Effect

- AP access authentication can be implemented based on the serial number, password, or certificate.

Notes

- If you run the **ap-auth** { **serial** | **password** | **certificate** } **enable** command in AC configuration mode to enable the access authentication function, but do not run the **ap-auth** { **serial** *serial-string* |**password** *password* |**ac-cert** *ac-cert-name* |**ap-cert** *ap-cert-name* } command in AP configuration mode to configure related authentication parameters, AP access authentication will fail and the AP cannot go online.

Configuration Steps

- Optional.
- Run the **ap-auth serial-update** command to update the authentication serial numbers for all online APs.
- Run the **ap-auth enable** command in AC configuration mode to enable a specified type of AP access authentication.
- Run the **ap-auth** { **serial** *serial-string* | **password** *password* | **ac-cert** *ac-cert-name* | **ap-cert** *ap-cert-name* } command to configure the related AP access authentication parameters.

Command	**ap-auth serial-update**
Parameter Description	N/A
Defaults	This function is disabled.
Command Mode	AC configuration mode
Usage Guide	All online APs use the current AP serial numbers for authentication.

Command	**ap-auth** { **serial**	**password**	**certificate** } **enable**
Parameter Description	**serial**: Indicates the authentication function based on the AP access serial number. **password**: Indicates the authentication function based on the AP access password. **certificate**: Indicates the authentication function based on the AP certificate.
Defaults	The authentication function is disabled.
Command Mode	AC configuration mode

Usage Guide	N/A

Command	**ap-auth** { **serial** *serial-string* | **password** *password* | **ac-cert** *ac-cert-name* | **ap-cert** *ap-cert-name* }
Parameter Description	*serial-string*: Specifies the AP access serial number. *password*: Specifies the AP access password. *ac-cert-name*: Specifies the AC certificate file name. *ap-cert-name*: Specifies the AP certificate file name.
Defaults	This function is disabled.
Command Mode	AP configuration mode
Usage Guide	The AP access authentication configuration takes effect only when the AP makes an access attempt. If the AP is already online, the configuration takes effect next time when the AP goes online. The **ap-auth serial** command cannot be used in all-AP configuration mode because the serial number varies according to the AP. The certificate file issued by the **ap-auth ap-cert** command will be stored as **cert.crt** on the AP, and the file name cannot be changed.

Verification

- Run the **show ap-config running** command to check whether the configuration is successful.

Configuration Example

Configuring the AP Access Authentication Based on the Serial Number

Configuration Steps	• After all authorized APs go online, update the authentication serial numbers for all online APs. • Enable the AP access authentication function based on the serial number. • Configure the authentication serial number of a specified AP.

AC	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#ap-auth serial-update`
	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#ap-auth serial enable`
	`Hostname(config)#ap-config Hostname-AP1`
	`Hostname(config-ap)#ap-auth serial G1GD10U000456`

Verification	• Run the **show running** or **show ap-config running** command to display the AP access authentication configuration.

AC	`Hostname(config)#show run`
	`!`
	`ac-controller`
	`  ap-auth serial enable`
	`!`
	`Hostname(config)#show ap-config running Hostname-AP1`
	`!`
	`ap-config Hostname-AP1`
	`ap-auth serial G1GD10U000456`

	!

Updating the Access Authentication Certificate of an AP

Configuration Steps	● Update the access authentication certificate of an AP.
AC	Hostname(config)#ap-config Hostname-AP1 Hostname(config-ap)#ap-auth ap-cret ap1_cret.crt
Verification	● Run the **show ap-config running** command to display the name of the current AC. If the corresponding AP is online, the **ap1_cret.crt** certificate file is updated to the AP instantly; otherwise, the file is updated to the AP after the AP goes online.
AC	Hostname(config)#show ap-config running Hostname-AP1 ! ap-config Hostname-AP1 ap-auth ap-cret ap1_cret.crt !

Common Errors

- N/A

1.4.19 Configuring the AP Priority

Configuration Effect

- By default, the AC allows the access of APs based on the sequence of AP association requests received by the AC. You can set the failover priorities of APs and enable the AC to support the failover priorities of APs so that the AC can allow the access of APs based on the AP priorities. The AP priority ranges from 1 to 4, where 1 is the lowest priority.

Notes

- N/A

Configuration Steps

- Optional. You can enable the AP priority function as required and configure the priority of a specified AP.
- On the AC, enter the AC configuration mode and run the **ap-priority** { **enable** | **disable** } command to enable or disable the AP priority function.
- On the AC, enter the AP configuration mode and run the **priority** *priority-value* command to configure the priority of a specified AP.

Command	**ap-priority** { **enable**	**disable**}
Parameter Description	**enable**: Enables the AP to support the failover priority. **disable**: Disables the AP to support the failover priority.
Defaults	Disabled.
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**priority** *priority-value*
Parameter Description	priority-value: Indicates the AP priority. The value ranges from 1 to 4, where 1 is the lowest priority.
Defaults	The default priority of an AP is 1. The priority can be set to a value from 1 to 4, where 1 is the lowest priority and 4 is the highest priority. You can run the **priority** command in AP configuration mode to configure the AP priority.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

↘ Setting the Priority of Hostname-AP1 to 2 and Enabling the AP Priority Function

Configuration Steps	• Enter the AP configuration mode. • Configure the AP priority. • Enter the AC configuration mode. • Enable the AP priority function.

AC	`Hostname(config)#ap-config Hostname-AP1`
	`Hostname(config-ap)#priority 2`
	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#ap-priority enable`

Verification	• Run the **show running** command to check whether the **ap-priority enable** command is configured in AC configuration mode. • Run the **show ap-config running** command to display the AP configuration.

AC	`Hostname(config)#show running`
	`!`
	`ac-controller`
	`  ap-priority enable`
	`!`
	`Hostname#show ap-config running`
	`!`
	`ap-config Hostname-AP1`
	`  priority 2`
	`!`

Common Errors

- N/A

1.4.20 Configuring the AC Cluster Function

Configuration Effect

- AC cluster is also called AC redundancy. With this function, multiple ACs with different priorities are designated for an AP. When the connection between the AP and a high-priority AC is down, the AP is connected to a low-priority AC (standby AC). When the connection with the high-priority AC is recovered, the AP disconnects the CAPWAP tunnel with the low-priority AC, and sets up a CAPWAP tunnel with the high-priority AC again.
- On the one hand, the AC cluster function enhances reliability of the AC cluster. On the other hand, this function controls the home AC of APs in stable conditions based on the priority to facilitate AP management.

Notes

- For a specified AP, the same priority must be configured for this AP on each AC that belongs to the cluster. For example, on AC1, AC2 is configured as the primary AC for AP1, and AC1 is configured as the secondary AC for AP1. On AC2, AC1 is configured as the primary AC for AP1, and AC2 is configured as the secondary AC for AP1. That is, on both AC1 and AC2, the peer AC is configured as the high-priority AC for AP1. In this way, an endless loop is formed because the AP keeps switching between tunnels with two ACs.
- The redundancy AC configuration supports both the ap-config ap-name and ap-config all configuration modes. The redundancy AC configuration made in ap-config ap-name configuration mode takes precedence over that made in ap-config all configuration mode.
- Except the **primary-base** command, commands of other priorities do not support switchback to prevent network interruption caused by the switchback. The administrator can re-configure the priorities for a manual switchover, or configure the **switch-back** parameter for an automatic switchback.

Configuration Steps

- Optional. The redundancy AC configuration does not exist on an AP by default. You can configure redundancy ACs with different priorities for an AP based on the number of ACs deployed on the wireless network.
- Run the **primary-base** *ac-name* { *ip-address* | *ipv6-address* } command to configure the primary AC for a specified AP.
- Run the **secondary-base** *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the secondary AC for a specified AP.
- Run the **tertiary-base** *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the tertiary AC for a specified AP.
- Run the **backup-controller-primary** *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the fourth AC for a specified AP.
- Run the **backup-controller-secondary** *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the fifth AC for a specified AP.
- Run the **backup-controller-tertiary** *ac-name* { *ip-address* | *ipv6-address* } [**switch-back**] command to configure the sixth AC for a specified AP.

Command	**primary-base** *ac-name* { *ip-address*	*ipv6-address* }
Parameter Description	*ac-name*: Indicates the name of the AC to be configured. *ip-address*: Indicates the IP address of the primary AC. The format is A.B.C.D. *ipv6-address*: Indicates the IPv6 address of the primary AC. The format is X;Y::Z.
Defaults	N/A
Command	AP configuration mode (supporting the **ap-config all** configuration mode)

Mode	
Usage Guide	N/A

Command	**secondary-base** *ac-name* {*ip-address* | *ipv6-address* }[**switch-back**]
Parameter Description	*ac-name*: Indicates the name of the AC to be configured. *ip-address*: Indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: Indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: Indicates the switchback function. Switchback is disabled by default.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**tertiary-base** *ac-name* {*ip-address* | *ipv6-address*}[**switch-back**]
Parameter Description	*ac-name*: Indicates the name of the AC to be configured. *ip-address*: Indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: Indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: Indicates the switchback function. Switchback is disabled by default.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**backup-controller-primary** *ac-name* {*ip-address* | *ipv6-address*}[**switch-back**]
Parameter Description	*ac-name*: Indicates the name of the AC to be configured. *ip-address*: Indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: Indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: Indicates the switchback function. Switchback is disabled by default.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**backup-controller-secondary** *ac-name* { *ip-address* | *ipv6-address*}[**switch-back**]
Parameter Description	*ac-name*: Indicates the name of the AC to be configured. *ip-address*: Indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: Indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: Indicates the switchback function. Switchback is disabled by default.
Defaults	N/A

Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Command	**backup-controller-tertiary** *ac-name* { *ip-address* | *ipv6-address* }[**switch-back**]
Parameter Description	*ac-name*: Indicates the name of the AC to be configured. *ip-address*: Indicates the IP address of the AC. The format is A.B.C.D. *ipv6-address*: Indicates the IPv6 address of the AC. The format is X;Y::Z. **switch-back**: Indicates the switchback function. Switchback is disabled by default.
Defaults	N/A
Command Mode	AP configuration mode (supporting the **ap-config all** configuration mode)
Usage Guide	N/A

Verification

- Run the **show ac-config** command to display the current AC name and check whether the configuration is successful.

Configuration Example

Configuring Hostname-AC1 as the Primary AC of Hostname-AP1, and Hostname-AC2 as the Secondary AC

Configuration Steps	• Enter the AP configuration mode. • Configure the primary AC and secondary AC of the AP.

Hostname-AC1	`Hostname(config)#ap-config Hostname-AP1`
	`Hostname(config-ap)#primary-base Hostname-AC1 5.5.5.5`
	`Hostname(config-ap)#secondary-base Hostname-AC2 6.6.6.6`

Hostname-AC2	`Hostname(config)#ap-config Hostname-AP1`
	`Hostname(config-ap)#primary-base Hostname-AC1 5.5.5.5`
	`Hostname(config-ap)#secondary-base Hostname-AC2 6.6.6.6`

Verification	• Run the **show ap-config running** command to display the AP configuration.

Hostname-AC1	`Hostname#show ap-config running`
	`!`
	`ap-config Hostname-AP1`
	`  primary-base Hostname-AC1 5.5.5.5`
	`secondary-base Hostname-AC2 6.6.6.6`
	`!`

Hostname-AC2	`Hostname#show ap-config running`
	`!`
	`ap-config Hostname-AP1`
	`  primary-base Hostname-AC1 5.5.5.5`
	`secondary-base Hostname-AC2 6.6.6.6`
	`!`

Common Errors

- N/A

1.4.21 Configuring the AC Hot Standby Function

Configuration Effect

- Set up the hot standby connection to ensure that the AP can establish two CAPWAP tunnels.

Notes

- N/A

Configuration Steps

- Optional. If an AP does not use the hot standby IP address of the AC to set up a tunnel, the AC address of the first tunnel must be specified. When the IPv6 address must be used to set up the second tunnel, the IPv6 hot standby tunnel function must be enabled.
- Run the **peer-ip** command to configure the IP address for setting up a CAPWAP tunnel with the hot standby neighbor. This IP address will be delivered to the AP, and the AP will set up the second CAPWAP tunnel with the hot standby neighbor based on the peer IP address. If the AP does not use the default hot standby IP address of the AC to set up a tunnel, you need to configure the peer IP address.
- Run the **peer-ipv6** command to configure the IPv6 address for setting up a CAPWAP tunnel with the hot standby neighbor. This IPv6 address will be delivered to the AP, and the AP will set up the second CAPWAP IPv6 tunnel with the hot standby neighbor based on the peer IPv6 address. When an AP and an AC use the IPv6 address to set up a tunnel, you need to configure the peer IPv6 address to set up the second CAPWAP IPv6 tunnel because currently the IPv6 address cannot be used for setting a hot standby connection between ACs.
- After the **peer-ipv6 enable** command is executed, the AP sets up the second CAPWAP IPv6 tunnel with the hot standby neighbor. To set up a CAPWAP IPv6 tunnel between an AP and an AC, you need to enable peer-ipv6 so that the second CAPWAP IPv6 tunnel can be set up between the AP and the AC.
- Run the **ap-group** command to bind an AP group to the hot standby instance. After the AP group is bound to the hot standby instance, data of STAs associated with APs in the AP group can be synchronized from the active AC to the standby AC.

Command	**peer-ip** *ipv4-address*
Parameter Description	*ipv4-address*: Indicates the IP address used by the hot standby neighbor to set up a CAPWAP tunnel.
Defaults	Source address used by CAPWAP.
Command Mode	Hot standby instance mode
Usage Guide	In the non-NAT environment, use the default setting, that is, the source IP address used by CAPWAP. In the NAT environment, configure the IPv6 address based on the environment where the AC and AP are located. When the AC is located inside the NAT, its address is a private network address, which is not accessible by the AP. Therefore, the AP must be notified of the configured public network address. ● If both the AP and the AC are on the same NAT intranet, use the default setting.

	● If the AP is on the NAT external network, use the IP address configured by the user as the peer AC address.

Command	**peer-ipv6***ipv6-address*
Parameter Description	*ipv6-address*: Indicates the IPv6 address used by the hot standby neighbor to set up a CAPWAP tunnel.
Defaults	Source IP address used by CAPWAP
Command Mode	Hot standby instance mode
Usage Guide	In the non-NAT environment, use the default setting, that is, the source address used by CAPWAP. In the NAT environment, configure the IPv6 address based on the environment where the AC and AP are located. When the AC is located inside the NAT, its address is a private network address, which is not accessible by the AP. Therefore, the AP must be notified of the configured public network address. ● If both the AP and the AC are on the same NAT intranet, use the default setting. ● If the AP is on the NAT external network, use the IP address configured by the user as the peer AC address. You need to run the **peer-ipv6 enable** command to enable the function of using CAPWAP to set up the dual IPv6 hot standby tunnels.

Command	**peer-ipv6 enable**
Parameter Description	N/A
Defaults	Disabled.
Command Mode	Hot standby instance mode
Usage Guide	The peer-ipv6 must be enabled when CAPWAP is used to set up an IPv6 tunnel between the AP and a hot standby AC so that the AP can use CAPWAP to set up an IPv6 tunnel with another hot standby AC.

Command	**ap-group** *ap-group*
Parameter Description	*ap-group*: Indicates the name of an AP group.
Defaults	N/A
Command Mode	Hot standby instance mode
Usage Guide	After the AP group is bound to the hot standby instance, data of STAs associated with APs in the AP group can be synchronized from the active AC to the standby AC.

Verification

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

Configuration Example

For details about the AC hot standby deployment solution, see WLAN Hot Backup.

Configuring the AC to Use the Public Network Address as the AC Address

Configuration Steps	● Configure the hot standby address and enter the hot standby configuration mode. ● Configure the hot standby instance. ● In the hot standby instance configuration mode, configure the peer IP address.
AC	`Hostname(config-hotbackup)# context 10` `Hostname(config-hotbackup-ctx)# peer-ip 1.1.1.1`
Verification	● Run the **show running** command to display the configuration.

AC	`Hostname(config)#show running`
	`wlan hot-backup 1.1.1.1`
	`!`
	`context 10`
	`peer-ip 1.1.1.1`

Common Errors

- N/A

1.4.22 Creating a WLAN

Configuration Effect

- You can create multiple WLANs on an AC and enter the configuration mode of a specified WLAN to configure related functions and attributes of the WLAN according to the actual network requirements.
- The WLAN service template that is generated based on the following configurations can take effect only after the WLAN is deployed on a specified AP group. Wireless users can access related APs to access the WLAN.
- On the wireless network, you can divide the network into multiple WLAN subnets by creating WLANs. In addition, you can configure the functions and attributes of a specified WLAN in WLAN configuration mode to provide different network services for wireless users.
- When creating a WLAN, you need to associate the WLAN with an SSID, which is the name of a network service zone. One SSID can be mapped to one or multiple WLANs.

Notes

- N/A

Configuration Steps

- Optional. No WLAN is configured by default. You need to create a WLAN before deploying the WLAN.
- Run the **wlan-config** command to create a WLAN, and use the **no** form of the command to delete the WLAN.

Command	**wlan-config** *wlan-id* [*profile –string*][*ssid-string*]
Parameter Description	*wlan-id*: Indicates the ID of a WLAN. The value ranges from 1 to 4094. *profile -string*: Indicates the profile of the WLAN. This parameter is optional. The maximum length is 32 bytes.

	ssid-string: Indicates the SSID. The maximum length is 32 bytes. When creating a WLAN, you need to specify the SSID associated with the WLAN. Use the **no** form of the command to delete a specified WLAN.
Defaults	No WLAN is created.
Command Mode	Global configuration mode
Usage Guide	One SSID can be mapped to one or multiple WLANs, but one WLAN can be associated with only one SSID.

Verification

- Run the **show running** command to display the WLAN configurations.

Configuration Example

Creating a WLAN

Configuration Steps	● Create WLAN 1. The SSID of WLAN 1 is Hostname-wireless.
AC	`Hostname(config)#wlan-config 1 Hostname-wireless` `Hostname(config-wlan)#`
Verification	● Run the **show running** command to display the WLAN configurations.

AC	`Hostname#show running`
	`!`
	`wlan-config 1 Hostname-wireless`
	`!`

Common Errors

- N/A

1.4.23 Deploying a WLAN

Configuration Effect

- The WLAN configuration takes effect only after the WLAN is deployed on a specified AP group. Wireless users can access the WLAN through the related APs. Run the **interface-mapping** command in AP group configuration mode to deploy the WLAN on a specified AP group. This command supports three mapping modes between the WLAN and VLANs, that is, single VLAN ID, VLAN group, and VLAN list, to map a specified WLAN to a corresponding VLAN of a wired network.

Notes

- When the WLAN forwarding mode is set to local forwarding, if the VLAN ID assigned to a STA by running the **interface-mapping** command is the same as the VLAN ID specified by the **ap-vlan** command, the service VLAN used by the STA for data forwarding is determined by the access switch of the AP, and is not the VLAN assigned by running the **interface-mapping** command. In particular, if the VLAN ID configured by running the **interface-mapping** command is 1, the VLAN of the STA in local forwarding mode is determined by the access switch. If no **ap-vlan** command is configured, the default VLAN ID in the **ap-vlan** command is 1.

- When using the **interface-mapping** command to configure the **list** mapping mode, you can add a single VLAN ID, but cannot remove a specified VLAN ID from the VLAN list.
- When using the **interface-mapping** command to configure the **list** mapping mode, the corresponding VLANs of the VLAN members in the VLAN list must be configured on the AC; otherwise, the IEEE 802.1X authenticated STAs cannot access the VLANs.

Configuration Steps

- Optional. You can run the **interface-mapping** command in AP group configuration mode to configure a WLAN and deploy the WLAN on all APs in the AP group.
- On the AC, enter the AP configuration mode and run the **interface-mapping** command for configuration.

Command	**interface-mapping** *wlan-id* [*vlan-id* I **group** *vlan-group-id* I **list** *vlan-list* [**def-vlan** *def-vlan-id*]] [**radio** { *radio-id* | **802.11b** | **6GHz** }] [**ap-wlan-id** *ap-wlan-id*]
Parameter Description	*wlan-id*: Indicates the ID of the specified WLAN. This WLAN must have been created. The WLAN ID ranges from 1 to 4094. *vlan-id*: Indicates the ID of the specified VLAN. The VLAN ID ranges from 1 to 4094. vlan-group-id: Indicates the ID of the specified VLAN group. The VLAN group ID ranges from 1 to 128. *vlan-list*: Indicates the specified VLAN list. The value ranges from 1 to 4094. The number of VLANs allowed in the list is 1 to 32. *def-vlan-id*: Indicates the default VLAN in the VLAN list. The value ranges from 1 to 4094. r*adio-id*: Indicates the ID of the radio of a specified AP. If radio-id is not specified, the mapping is applied to all radios of all APs in the AP group. The radio ID ranges from 1 to 96. **802.11b**: Indicates that the mapping is applied to all 2.4 GHz radios of all APs in the AP group. **802.11a**: Indicates that the mapping is applied to all 5.8 GHz radios of all APs in the AP group. **6GHz**: Indicates that the mapping is applied to all 6 GHz radios of all APs in the AP group. *ap-wlan-id*: Specifies the wlan-id that is used on the AP through interface-mapping. The value ranges from 1 to 64.
Defaults	The WLAN is not deployed on any AP.
Command Mode	AP group configuration mode
Usage Guide	● If the **ap-wlan-id** parameter is not specified, the mapping automatically selects and uses an idle ap-wlan-id. ● If the **ap-wlan-id** parameter is not specified, the first VLAN in the VLAN list is automatically selected and used for the mapping.

Verification

- Run the **show running** command to display the AP group configurations.

Configuration Example

Deploying a WLAN on a Specified AP Group

Configuration Steps	Hostname-AP1 belongs to the AP group APG-1. Create a WLAN, and deploy the WLAN on Hostname-AP1.

	● Create WLAN 1. The SSID of WLAN 1 is Hostname-wireless. ● Create VLAN 1. ● Configure the WLAN-VLAN mapping in AP group configuration mode.

AC	`Hostname(config)#wlan-config 1 Hostname-wireless`
	`Hostname(config-wlan)#exit`
	`Hostname(config)#vlan 1`
	`Hostname(config-vlan)#exit`
	`Hostname(config)#ap-group APG-1`
	`Hostname(config-ap-group)#interface-mapping 1 1`

Verification	● Run the **show running** command to check the AP group configurations.

	`Hostname#show running`
	`!`
	`wlan-config 1 Hostname-wireless`
	`!`
	`!`
	`ap-group APG-1`
	`  interface-mapping 1 1`
	`!`

Common Errors

- N/A

1.4.24 Configuring WLAN SSID Broadcasting

Configuration Effect

- On the WLAN, the AP periodically broadcasts the SSID information to notify the existence of the wireless network. Wireless users use the wireless network interface cards (NICs) to search SSIDs and detect the wireless network. The SSID broadcasting function can be enabled to prevent the wireless network from being searched and connected by unauthorized users based on the SSID.

Notes

- N/A

Configuration Steps

- Optional. WLAN SSID broadcasting is enabled by default. If the WLAN SSID needs to be hidden to prevent the wireless network from being searched and connected by unauthorized users based on the SSID, you can disable the WLAN SSID broadcasting function.
- On the AC, enter the WLAN configuration mode and run the **enable-broad-ssid** command for configuration.

Command	**enable-broad-ssid**
Parameter Description	N/A
Defaults	WLAN SSID broadcasting is enabled.
Command	WLAN configuration mode

Mode	
Usage Guide	WLAN SSID broadcasting is enabled by default. You can use the **no** form of the command to disable this function. If the SSID broadcasting configuration of the WLAN changes, users associated with the WLAN will go offline.

Verification

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

Configuration Example

Disabling SSID Broadcasting of WLAN 1

Configuration Steps	• Enter the WLAN configuration mode. • Disable SSID broadcasting.
AC	`Hostname(config)#wlan-config 1` `Hostname(config-wlan)#no enable-broad-ssid`
Verification	• Run the **show running** command to display the WLAN configuration.

AC	`Hostname#show running`
	`!`
	`wlan-config 1 Hostname-wireless`
	`  no enable-broad-ssid`
	`!`

Common Errors

- N/A

1.4.25 Configuring the NAS ID of a WLAN User

Configuration Effect

- On the WLAN, the NAS IDs of WLAN users identify different hot spot areas. By default, the NAS ID of a WLAN user is a null string.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC, enter the WLAN configuration mode and run the **nas-id** command to configure the NAS ID.

Command	**nas-id** *wlan-nas-id*
Parameter Description	N/A
Defaults	Null string
Command	WLAN configuration mode

Mode	
Usage Guide	N/A

Verification

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

Configuration Example

Configuring the NAS ID of a WLAN User

Configuration Steps	• Enter the WLAN configuration mode. • Configure the NAS ID of a WLAN user.
AC	`Hostname(config)#wlan-config 1` `Hostname(config-wlan)#nas-id0000059159100460`
Verification	• Run the **show running** command to display the WLAN configuration.

AC	`Hostname#show running`
	`!`
	`wlan-config 1 Hostname-wireless`
	`nas-id0000059159100460`
	`!`

Common Errors

- N/A

1.4.26 Configuring the Fit or Fat AP Mode

Configuration Effect

- On the AC, run the **switch2fat** command in AC configuration mode to switch the mode of an online AP to the fat AP mode.

Notes

- If the **switch2fat** command is executed on the AC in AP configuration mode to switch the mode of an online AP to the fat AP mode, the AP will be disconnected from the AC. After that, you cannot configure the AP on the AC.

Configuration Steps

- Optional. For an AC, an online AP definitely works in fit AP mode. You can run the **switch2fat** command if you need to switch the mode of the AP to the fat AP mode.
- On the AC, run the **switch2fat** command in AC configuration mode to switch the mode of an online AP to the fat AP mode.

Command	**switch2fat** *ap-name*
Parameter Description	*ap-name*: Indicates the name of a specified AP.
Defaults	All fit APs are controlled by the associated AC. A fit AP can be switched to a fat AP to implement self-control.

Command Mode	AC configuration mode
Usage Guide	This command takes effect only on an online AP.

Verification

- N/A

Configuration Example

Switching the Mode of the Online AP Hostname-AP1 to the Fat AP Mode on the AC

Configuration Steps	• Enter the AC configuration mode. • Run the **switch2fat** command.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)#switch2fat Hostname-AP1`
Verification	N/A

Common Errors

- N/A

1.4.27 Configuring the WLAN SSID

Configuration Effect

- Configure a new SSID for the WLAN. If this WLAN has been deployed, all users associated with this WLAN will go offline.
- Configure the coded character set for the SSID. If the WLAN has been deployed, all users of this WLAN will go offline.

Notes

- N/A

Configuration Steps

- Optional.
- On the AC, enter the WLAN configuration mode and run the **ssid** command to configure the new SSID.

Command	**ssid** *ssid-string*
Parameter Description	N/A
Defaults	N/A
Command Mode	WLAN configuration mode
Usage Guide	N/A

- On the AC, enter the WLAN configuration mode and run the **ssid-code** command to configure the encoding character set for the SSID.

Command	**ssid-code** { **gbk** | **utf-8** }
Parameter Description	**gbk**: Sets the character set to GBK. **utf-8**: Sets the character set to UTF-8.
Defaults	N/A. The system character set is used.
Command Mode	WLAN configuration mode
Usage Guide	1. If the WLAN has been deployed, all users of this WLAN will go offline. 2. Some wireless clients may only support UTF-8 or GBK. When the SSID is set in Chinese, these clients may fail to associate. In this case, you can use the **ssid-code** command to change the SSID to UTF-8 or GBK, thereby making it adaptive to the wireless clients.

Verification

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

Configuration Example

Setting the New SSID of WLAN 1 to Hostname

Configuration Steps	• Enter the WLAN configuration mode. • Set the new SSID of WLAN 1 to Hostname.
AC	`Hostname(config)#wlan-config 1` `Hostname(config-wlan)#ssid Hostname`
Verification	• Run the **show running** command to display the WLAN configuration.

AC	`Hostname#show running`
	`!`
	`wlan-config 1 Hostname`
	`!`

Common Errors

- N/A

1.4.28 Configuring the AP Backup Function

Configuration Effect

- If the active AP in an AP backup group is faulty and disconnected, other standby APs in the group receive the WLAN configuration of the active AP and transmit radio signals of the active AP.

Notes

- In an AP backup group, if the active AP is not selected, the AP backup function does not take effect.

Configuration Steps

Configuring an AP Backup Group

- Optional. Create an AP backup group when the wireless network of an AP needs to be backed up.
- In AC configuration mode, run the **ap-backup group** command to create an AP backup group.

Command	**ap-backup group** *backup-group*
Parameter Description	*backup-group*: Indicates the name of the AP backup group.
Defaults	If only the AP backup group named **default** exists on the AC, the backup function of this group does not take effect.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding APs to an AP Backup Group

- Optional. When the wireless network of an AP must be backed up by other APs, add the standby APs and the AP to be backed up to the AP backup group, and select the AP to be backed up as the active AP.
- In AP configuration mode, run the **ap-backup-group** command to add the AP to the AP backup group. When adding an AP to an AP backup group, you can specify whether the AP is the active AP.

Command	**ap-backup-group** *backup-group***[master]**
Parameter Description	*backup-group*: Indicates the name of the AP backup group.
Defaults	The AP is not added to the default group, and the backup function of the backup group does not take effect.
Command Mode	AP configuration mode
Usage Guide	This command does not support the ap-config all mode. The keyword master is optional. If the command contains this keyword, the AP is designated as the active AP of the group; otherwise, the AP is the standby AP. An AP backup group can have multiple standby APs but only one active AP. When the AP backup group starts to work, that is, the standby APs have inherited WLAN signals from the active AP, note that the following four operations change the WLAN configurations of the standby APs that should take effect, and the inherited WLAN signals will take effect again: 1. Modify the WLAN configurations of the AP group to which the standby APs belong. 2. Modify the WLAN configurations of the AP group to which the active AP belongs. 3. Change the AP group of the standby APs. 4. Change the AP group of the active AP. If online users already exist, these users will go offline.

Verification

- Run the **show ap-config running** and **show ac-config ap-backup-group** commands to display the configuration.

Configuration Example

Creating an AP Backup Group Named APBACK-APG-1

Configuration Steps	In AC configuration mode, run the **ap-backup group** command to create an AP backup group.
AC	`Hostname(ac-config)#ap-backup group APBACK-APG-1`
Verification	Run the **show ac-config ap-backup-group** command to check the configurations.
AC	`Hostname#show ac-config ap-backup-group` `Cnt Group-Name Master-AP cntStandby-AP cnt`

	Master-AP-Name Working ------ ---------- 1 APBACK-APG-1 1 2 AP4210-1 false

Adding AP4210-1 to the AP Backup Group Named APBACK-APG-1, and Configuring this AP as the Active AP of the Group

Configuration Steps	● In AP configuration mode, run the **backup-group** command to add the AP to the AP backup group.
AC	Hostname(ap-config)#ap-backup-group APBACK-APG-1 master
Verification	● Run the **show ac-config ap-backup-group** command to display the configuration.
AC	Hostname#show ac-config ap-backup-groupAPBACK-APG-1 Cnt Ap-Name Ap-Mac Online Is-Master Inherit-Wlan Cnt ------- ---------- ---------- ------- ---------- ---------- 1 AP4210-1 8832.0000.1111 true Yes 0

Common Errors

- N/A

1.4.29 Configuring Hierarchical Permission-based AC Management

Configuration Effect

- After an administrator logs in to the web management page, the administrator can only check and configure authorized WLANs, AP groups, and APs (STAs).

Notes

- N/A

Configuration Steps

Enabling Hierarchical Permission-based AC Management

- Optional. When multiple administrators are required in a wireless environment to manage different wireless networks and APs, enable hierarchical permission-based AC management.
- Run the **permit enable** command in AC configuration mode to enable hierarchical permission-based AC management.
- Run the **master-group** command in global configuration mode to create a role and enter the role configuration mode.
- Run the **master-group** command in AP configuration mode to assign an AP to a specific role.
- Run the **master-group** command in AP group configuration mode to assign an AP group to a specific role.
- Run the **master-group** command in WLAN configuration mode to assign a WLAN to a specific role.

- Run the **webmaster** command in role configuration mode to add or delete an administrator.

Command	**permit enable**
Parameter Description	N/A
Defaults	The AC virtualization function is disabled.
Command Mode	AC configuration mode
Usage Guide	Whether this configuration is supported depends on the actual product.

Command	**master-group** master-group-name
Parameter Description	*master-group-name*: Indicates the role name.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	When the **no** form of this command is used to delete a role, APs, AP groups, and WLANs assigned to the role are restored to the unassigned state and the administrator of this role is restored to the default role-free state. Whether this configuration is supported depends on the actual product.

Command	**master-group** master-group-name
Parameter Description	*master-group-name*: Indicates the role name.
Defaults	N/A
Command Mode	AP configuration mode, AP group configuration mode, or WLAN configuration mode
Usage Guide	After a role is deleted, APs, AP groups, and WLANs assigned to the role are restored to the default unassigned state. Whether this configuration is supported depends on the actual product.

Command	**webmaster** webmaster-name
Parameter Description	*webmaster-name*: Indicates the administrator name.
Defaults	N/A
Command Mode	Role configuration mode
Usage Guide	When a role is deleted, the administrator of the role is restored to the default role-free state. Whether this configuration is supported depends on the actual product.

Verification

- Run the **show running-config** and **show ap-config running** commands to display configurations.

Configuration Example

Enabling Hierarchical Permission-based AC Management

Configuration Steps	● Run the **permit enable** command in AC configuration mode to enable hierarchical permission-based AC management.
AC	`Hostname(ac-config)# permit enable`
Verification	● Run the **show running-config** command to display the configuration.

AC	`Hostname# show running-config | begin ac-controller`
	`ac-controller`
	` permit enable`
	` ac-name Hostname`
	` country CN`

Creating Role test-group and Adding Administrator test-admin-1 for the Role

Configuration Steps	● Run the **master-group** command in global configuration mode to create the role (test-group) and enter the role configuration mode. ● Run the **webmaster** command in role configuration mode to add the administrator (test-admin-1).
AC	`Hostname(config)# master-group test-group` `Hostname(config-master-group)# webmaster test-admin-1`
Verification	● Run the **show running-config** command to display configurations.

AC	`Hostname# show running-config | begin master-group`
	`master-group test-group`
	` webmaster test-admin-1`

Assigning AP (ap-1), AP Group (apg-1), and WLAN (1) to Role test-group

Configuration Steps	● Run the **master-group** command in AP configuration mode to assign the AP (ap-1) to the role (test-group). ● Run the **master-group** command in AP group configuration mode to assign the AP group (apg-1) to the role (test-group). ● Run the **master-group** command in WLAN configuration mode to assign the WLAN (1) to the role (test-group).

AC	`Hostname(config)# ap-config ap-1`
	`Hostname(config-ap)# master-group test-group`
	`Hostname(config-ap)# exit`
	`Hostname(config)# ap-group apg-1`
	`Hostname(config-group)# master-group test-group`
	`Hostname(config-group)# exit`
	`Hostname(config)# wlan-config 1`
	`Hostname(config-wlan)# master-group test-group`

Verification	● Run the **show running-config** and **show ap-config running** commands to display configurations.
AC	`Hostname# show running-config | begin wlan-config 1` `wlan-config 1 Hostname`

	master-group test-group ! Hostname# show running-config | begin ap-group apg-1 ap-group apg-1 master-group test-group ! Hostname# show ap-config running | begin ap-config ap-1 ap-config ap-1 master-group test-group !

Common Errors

- N/A

1.4.30 Configuring the AP Virtualization Function

Configuration Effect

- Multiple ACs can assign their own WLANs to the same AP, and the STAs connect to the virtual APs served by corresponding ACs.

Notes

- ACs cannot broadcast the same signal.

Configuration Steps

Configuring an AP Virtualization Template

- Optional. Configure an AP virtualization template when multiple ACs need to manage the same AP.
- In global configuration mode, run the **virtual-ap** command to create an AP virtualization template.

Command	**virtual-ap** *sub-ap-name*
Parameter Description	*sub-ap-name*: Indicates the name of an AP virtualization template.
Defaults	No AP virtualization template is created.
Command Mode	AC global configuration mode
Usage Guide	N/A

Configuring the IP Address of the AC to Which a Virtual AP is to Connect

- Optional. If the IP address of the AC to which a virtual AP is to connect is not configured, the virtual AP created on the AP using the AP virtualization template cannot connect to the AC.

Command	ac-ip *ip*
Parameter Description	*ip*: Indicates the IPv4 address of the AC to which a virtual AP is to connect.
Defaults	The virtual APs created on the AP using the AP virtualization template cannot connect to ACs.

Command Mode	AP virtualization template configuration mode
Usage Guide	This command is configured in the AP virtualization template. The AP disconnects all tunnels and reconnects them each time the configurations are changed. The configured IP address cannot be the IP address of the active AC, and can only be the IP address of the AC to be connected and the address of the loopback 0 interface or the CAPWAP control IP address if any.

Configuring the Number of WLANs Supported by a Virtual AP

- Optional. If the number of WLANs supported by a virtual AP is not configured, it is calculated as follows: (Total number of WLANs supported by the AP – Number of WLANs configured for virtual APs)/Number of virtual APs with the number of supported WLANs not configured

Command	**wlan-capacity** *wlan-cap*
Parameter Description	*wlan-cap*: Indicates the number of WLANs supported by a virtual AP.
Defaults	The number of WLANs supported by a virtual AP is not configured.
Command Mode	AP virtualization template configuration mode
Usage Guide	This command is configured in the AP virtualization template. In default configuration mode, if the remaining number of WLANs is 0, the virtual AP cannot broadcast wireless signals. The AP disconnects all tunnels and reconnects them each time the configurations are changed.

Configuring the Number of STAs Supported by a Virtual AP

- Optional. If the number of STAs supported by a virtual AP is not configured, it is calculated as follows: (Total number of STAs supported by the AP – Number of STAs configured for virtual APs)/Number of virtual APs with the number of supported STAs not configured

Command	**sta-capacity** *sta-cap*
Parameter Description	*sta-cap*: Indicates the number of STAs supported by a virtual AP.
Defaults	The number of STAs supported by a virtual AP is not configured.
Command Mode	AP virtualization template configuration mode
Usage Guide	This command is configured in the AP virtualization template. In default configuration mode, if the remaining number of STAs is 0, the virtual AP cannot broadcast wireless signals. The AP disconnects all tunnels and reconnects them each time the configurations are changed.

Configuring the Uplink Interface Used by a Virtual AP

- Optional. If the uplink interface used by a virtual AP is not configured, the virtual AP uses the uplink interface used by the active AC.

Command	**link-interface** { *other* | *num}*
Parameter Description	*other*: Indicates that a virtual AP uses an uplink interface different from that used by the active AC. This parameter is specified when there are two uplink interfaces and virtual AP and active AC use them for connection. *num*: Indicates the number of uplink interface used by a virtual AP.
Defaults	A virtual AP uses the uplink interface used by the active AC.
Command Mode	AP virtualization template configuration mode
Usage Guide	This command is configured in the AP virtualization template. In default configuration mode, a virtual AP uses the uplink interface used by the active AC to establish a CAPWAP tunnel. The other parameter is configured only when there are two uplink interfaces and the virtual AP and active AC use them for connection. Otherwise, the virtual AP cannot establish a CAPWAP tunnel with the corresponding AC. If the configured uplink interface number does not exist, the virtual AP cannot establish a connection to the corresponding AC. The AP disconnects all tunnels and reconnects them each time the configurations are changed. If multiple uplink interfaces exist and the **other** or **num** parameter is configured after the aggregation function is configured, the virtual AP cannot establish a CAPWAP tunnel to the corresponding AC.

Configuring Virtual APs for an AP

- Optional. If virtual APs are not configured for an AP, the AP does not create virtual APs.

Command	**virtual-ap** *sub-ap-name* {**id** *num*}
Parameter Description	*sub-ap-name*: Indicates the name of an AP virtualization template. *num*: (Optional) Indicates the number of a virtual AP on the AP, which starts from 1 by default.
Defaults	An AP does not create virtual APs.
Command Mode	AP, AP group, or all-AP configuration mode
Usage Guide	This command is configured in AP, AP group, or all-AP configuration modes. In a configuration mode, multiple virtual APs can be configured but the virtual APs cannot have the same AC IP address except the default one. The AP disconnects all tunnels and reconnects them each time the configurations are changed. Configurations of the **virtual-ap** command are delivered based on the priority in descending order: Configurations in AP configuration mode > Configurations in AP group configuration mode > Configurations in all-AP configuration mode.

Configuring the Duration for a Virtual AP to Provide Services After the AP is Disconnected from the Active AC

- Optional. If the duration for a virtual AP to provide services after the AP is disconnected from the active AC is not configured, the virtual AP continues to provide services for one day.

Command	**ap-idle-timeout** *num*
Parameter Description	*num*: Indicates the duration (in days) for a virtual AP to provide services after the AP is disconnected from the active AC. The value ranges from 0 to 14.
Defaults	A virtual AP continues to provide services for one day after the AP is disconnected from the active AC.
Command Mode	AP, AP group, or all-AP configuration mode
Usage Guide	This command is configured in AP, AP group, or all-AP configuration mode. If the **num** parameter is set to 0 to prevent tunnel instability, the tunnel between the virtual AP and corresponding AC is not disconnected immediately but retained for two minutes. After an AP is disconnected from the active AC and the time specified in **ap-idle-timeout** has not expired, a virtual AP does not associate with an AC if the tunnel between the virtual AP and corresponding AC is disconnected. Only when the connection between the AP and active AC is re-established, the virtual AP will associate with the corresponding AC.

Verification

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

Configuration Example

Creating an AP Virtualization Template Named VAP-1

Configuration Steps	Run the **virtual-ap** command in AC global configuration mode to create the AP virtualization template named VAP-1.

AC	`Hostname(config)#virtual-ap VAP-1`
	`Hostname(config-virtual-ap)# wlan-capacity 6`
	`Hostname(config-virtual-ap)# sta-capacity 6`
	`Hostname(config-virtual-ap)# ac-ip 1.1.1.1`
	`Hostname(config-virtual-ap)# link-interface 2`

Verification	Run the **show running-config** command to display configurations.

AC	`Hostname#show running-config`
	
	`Building configuration...`
	`Current configuration: 6069 bytes`
	
	`version AC_RGOS 11.1(5)B00, Release(04150906)`
	`!`
	`virtual-ap VAP-1`
	` ac-ip 1.1.1.1`
	` wlan-capacity 6`
	` sta-capacity 16`
	` link-interface 2`
	`!`

Applying AP Virtualization Template VAP-1 to AP1

Configuration Steps	● Run the **virtual-ap** command in AP configuration mode, AP group configuration mode, or all-AP configuration mode.

AC	`Hostname(config)#ap-config AP1`
	`You are going to config AP(AP1), which is not online now.`
	`Hostname(config-ap)#virtual-ap VAP-1`
	`Hostname(config-ap)#`

Verification	● Run the **show ap-config running** command to display configurations.

AC	`Hostname(config-ap)#show ap-c running`
	`!`
	`ap-config AP1`
	` virtual-ap VAP-1 id 1`
	`!`

Common Errors

- N/A

1.4.31 Configuring the Default SSID

Configuration Effect

- When a fit AP starts up or the CAPWAP tunnel of the AP is disconnected, the AP broadcasts a 2.4 GHz unencrypted SSID signal. When the CAPWAP tunnel is set up, the SSID is disabled.

Notes

- If RIPT is configured and the tunnel is disconnected, signals are not broadcast.
- The SSID in Chinese is not supported.
- When the AP is restarted, the configurations will be saved.

Configuration Steps

- Optional.
- On the AC, run the **offline-ssid** command in AP, AP group, or all-AP configuration mode to specify the SSID signal of the AP.

Command	**offline-ssid** *ssid* [**hide**]
Parameter Description	*ssid*: Indicates the SSID signal broadcasted when the AP starts up or the tunnel is disconnected. **hide**: Indicates that no SSID signal is broadcasted.
Defaults	No SSID is configured.
Command Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Setting the Default SSID of AP1 to my-def-ssid

Configuration Steps	● Set the default SSID of the default AP group to my-group-ssid.

AC	`Hostname(config)#ap-config AP1`
	`Hostname(config-ap)#offline-ssid my-def-ssid`
	`Hostname(config-ap)#exit`
	`Hostname(config)#ap-group default`
	`Hostname(config-ap-group)#offline-ssid my-group-ssid`

Verification	● Run the **show running** command to check whether the command is configured in all-AP and AP group configuration modes. ● Run the **show ap-config running** command to display the configuration of the AP.

AC	`Hostname(config)#show running`
	`!`
	`ap-group default`
	`  offline-ssid my-group-ssid`
	`!`
	`Hostname#show ap-config running`
	`!`
	`ap-config AP1`
	`  offline-ssid my-def-ssid`
	`!`

Common Errors

- N/A

1.4.32 Configuring Automatic AP Grouping

Configuration Effect

- Configure matching rules in the AP group, such as the source IP network segment (the IP addresses of APs). After an AP goes online, the AP is automatically assigned to the AP group if the configured rules are matched.

Notes

- Perform the configuration in the target AP groups for grouping. The default AP group cannot be configured.
- The configuration takes effect for the AP in the default AP group only after the AP goes online.

Configuration Steps

- Optional.
- On the AC, run the **auto-join-group match src-ip** command in AP group configuration mode to configure the network segment matching rule for automatic AP grouping.

Command	**auto-join-group match src-ip** *match-ip-address network-address-mask*
Parameter	*match-ip-address*: Specifies the IP address of the AP that meets the requirement for joining the AP

Description	group, in format of A.B.C.D. Only one IP address can be configured for a rule. A single AP group supports up to 16 rules. *network-address-mask*: Configures the subnet mask of the IP address of the AP that meets the requirement for joining the AP group, in format of A.B.C.D. **recover**: Reassign an online AP in an AP group to the default AP group when deleting the network segment matching rule in the AP group. An AP is not reassigned to the default AP group by default.
Defaults	This function is not configured.
Command Mode	AP group configuration mode
Usage Guide	● After an AP goes online, the AP is automatically added to an AP group that matches the IP rule. ● Perform the configuration in the target AP groups for grouping. The default AP group cannot be configured. ● The configuration takes effect for APs in the default AP group only. ● The automatic AP grouping function takes effect only when an AP goes online for the first time. Adding or modifying a network segment matching rule does not affect the grouping of APs that are already online. ● Reassigning an AP to the default AP group after a rule is deleted is only available for online APs in the AP group for which this command takes effect.

Verification

- Run the **show auto-join-group rule src-ip summary** command to display the configuration.

Configuration Example

↘ Configuring APs in the Network Segment 192.168.1.0 to Automatically Join Group apg1

Configuration Steps	● Configure APs in the network segment 192.168.1.0 to automatically join Group apg1.
AC	`Hostname(config)#ap-group apg1` `Hostname(config-group)#auto-join-group match src-ip 192.168.1.0 255.255.255.0`
Verification	● Run the **show auto-join-group rule src-ip summary** command to check whether the command is configured in AP group configuration mode.

AC	`Hostname #show auto-join-group rule src-ip summary`
	`RULE IP Ap Group Name`
	`------------------ ----------------------------------------`
	`192.168.1.0/24 apg1`

Common Errors

- N/A

1.4.33 Configuring the AC Software Features

Configuration Effect

- Configure the software features of the AC to a hexadecimal value.

Notes

- The maximum value is **0xFFFFFFFF**.

Configuration Steps

- Run the **ac-controller** command to enter the AC configuration mode.
- Run the **wlan-features** command in AC configuration mode on the AC to configure the software features.

Command	**ac-controller**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**wlan-features** *features* **no wlan-features** **default wlan-features**
Defaults	The default value of AC software features is the engineering configuration value of the system.
Parameter Description	*features*: Indicates the software feature value of the AC. The maximum value is **0xFFFFFFFF**.
Command Mode	AC configuration mode
Usage Guide	You can configure software features that the AC does not support to temporarily bring the AP online.

Verification

- Run the **show running-config** command to display the software features of the AC and check whether the configuration is successful.

Configuration Example

Configuring the AC Software Feature Value to 0x02

Configuration Steps	• Enter the AC configuration mode. • Configure the software feature value of the AC, assuming that the current system value is 0x01.
AC	`Hostname(config)# ac-controller` `Hostname(config-ac)# wlan-features 0x02`

Verification	Run the **show running-config** command to display the software features of the AC.

AC	`Hostname# show running-config`
	`!`
	`ac-controller`
	` wlan-features 0x3`
	` capwap ctrl-ip 10.104.22.152`
	`!`

Resuming the AC Software Feature Value to the System Value

Configuration Steps
- Enter the AC configuration mode.
- Use the **no** form of this command to resume the AC software feature value to the system value.

AC

```
Hostname(config)# ac-controller
Hostname(config-ac)# no wlan-features
```

Verification

Run the **show running-config** command to display the software features of the AC.

AC

```
Hostname# show running-config
!
ac-controller
 wlan-features 0x1
 capwap ctrl-ip 10.104.22.152
!
```

Common Errors

N/A

1.5 Monitoring

Clearing

- N/A

Displaying

Command	Description
show ac-config	Displays the basic configurations of the current AC.
show ac-config ap-backup-group	Displays the AP backup group information.
show ac-device information	Displays the wireless AC hardware information.
show ap-device information [ap-name]	Displays the hardware information of the AP associated with the AC.
show ap-config bssid	Displays the BSSID list of all APs.
show ap-config bssid cb	Displays the BSSID information of an AP.
show ap-config cb	Displays the AP status information.
show ap-config inherit-wlan	Displays the WLAN information inherited by the AP.
show ap-config product	Displays the AP product list.
show ap-config summary	Displays the current status of all APs.
show ap-config summary ap-auth	Displays the authentication-related information of all APs.
show ap-config summary deny-ap	Displays APs that attempt to associate with the AC but are rejected by the AC.
show ap-config summary hot-backup	Displays the hot standby configuration and APs associated with the active AC.
show ap-config summary virtual-ap-role	Displays the virtual APs of all APs.
show ap-config virtual-ap detail	Displays the information about the virtual AP of an AP.

Command	Description
show ap-config virtual-ap summary	Displays the operating status of the virtual AP of an AP on the AC.
show ap-group aps	Displays the APs in a specified AP group.
show ap-group aps summary	Displays the APs in all AP groups.
show ap-group cb	Displays the basic information about a specified AP.
show ap-group intf-wlan-map	Displays the WLAN-VLAN mapping of a specified AP group.
show ap-group radios	Displays AP radio statistics of an AP group.
show ap-group summary	Displays all APs
show auto-join-group rule src-ip *ip-address ip-mask* **conflict**	Displays the configuration that conflicts with the input automatic grouping IP rule.
show auto-join-group rule src-ip summary	Displays the configured automatic grouping IP rule.
show license	Displays the supported APs after the license is installed on the AC.
show virtual-ap detail	Displays the information of a virtual AP template.
show virtual-ap summary	Displays the virtual AP template list on the AC.
show wlan hot-backup	Displays the instance list on the hot standby peer.
show wlan-config cb	Displays the basic information about a specified WLAN.
show wlan-config summary	Displays the WLAN configuration list on the AC.
show device-config map summary	Displays the information about an micro AP connected to the all-optical AM

Whether this configuration is supported depends on the actual product.

Debugging

- N/A

1 Configuring ETH-MNG

1.1 Overview

Access points (APs) provide Ethernet ports, including WAN ports, LAN ports, and cascade ports. The WAN ports are used to connect to the uplink access switches, and the LAN ports provided by some APs (wall-plate APs and i-Share+ APs) are used to access wired or other devices and forward data to WAN ports. The cascade ports provided by i-Share+ APs are used to connect to micro APs or other devices. In the fit AP network architecture, an AP obtains the IP address of an AC over the WAN port to establish a CAPWAP tunnel with the AC, and the AP cannot obtain the AC IP address through DHCP over the LAN port. Therefore, the LAN port cannot be used to establish a CAPWAP tunnel.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Configuring VLANs on LAN Ports	Configure VLANs on LAN ports to separate APs and wired users.

1.2.1 Configuring VLANs on LAN Ports

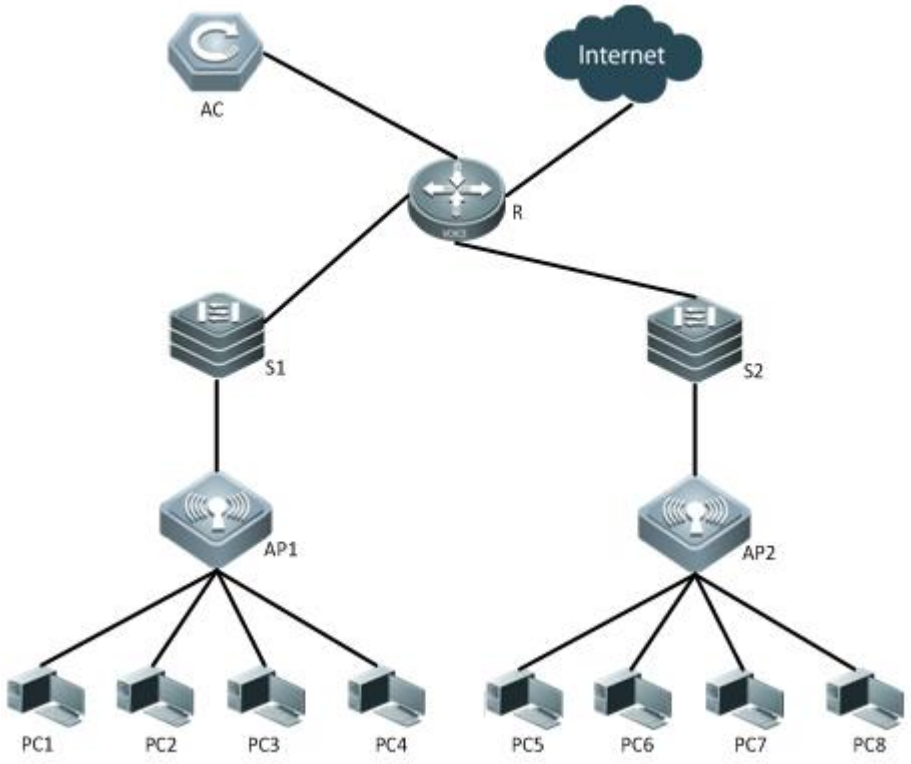
Scenario

In the fit AP architecture, configure VLANs on LAN ports.

Take the following topology as an example:

- An AC is connected to the Internet through a router. Two APs (AP1 and AP2) are connected to the router through two switches, and are associated with the AC.
- PC1, PC2, PC3, and PC4 are associated with AP1; PC5, PC6, PC7, and PC8 are associated with AP2. These PCs access the Internet through the AC.

Figure 1-1



Remarks	R: Indicates a network egress router. S1 and S2: Indicates two Layer 2 switches that serve as the access devices of APs. AP1 and AP2: Indicates two wireless access points. STA1 and STA2: Indicates two client devices connected to S1 and S2 respectively.

Deployment

- Enable the Layer 2 switch to provide the access function for the APs.
- Connect the router R to the network formed by the AC and the APs. Connect the router R to the PCs and the Internet.
- Configure VLANs for LAN ports on APs through the AC.

1.3 Features

Basic Concepts

N/A

Overview

Feature	Description

Configuring the Configuring the VLANs of an AP	Configures the default VLAN of an AP, VLANs of Ethernet ports, and transmission VLANs of i-Share+ APs.
Configuring a Bandwidth Limit for a Configuring a Bandwidth Limit for a LAN Port	Configures the maximum bandwidth for the LAN ports of APs to avoid the slow Internet access of wireless users in a scenario where wireless and wired users coexist and wired users occupy a substantial bandwidth.
Configuring the LAN/WAN Attribute of an AP Port	Configures the WAN/LAN attribute of the port to change devices with the default port attribute of WAN+LAN into dual-WAN-port devices.

1.3.1 Configuring the VLANs of an AP

Working Principle

An AP automatically removes the tag from a frame that carries the native VLAN before forwarding the frame. That is, in local forwarding mode, if the VLAN of a STA is the same as the native VLAN, the frame of the STA does not carry the tag when forwarded, and the access switch determines the VLAN to which the STA belongs. The default VLAN of the AP is VLAN 1. The default VLAN of the AP, VLAN of wireless users, and VLAN of wired users can be planned flexibly to ensure that the STAs and AP are on the same VLAN or different VLANs.

i-Share+ APs can be deployed in cascading mode, and transmission VLANs can be configured to ensure that VLAN packets of downlink devices can be forwarded by uplink devices.

1.3.2 Configuring a Bandwidth Limit for a LAN Port

Working Principle

The bandwidth limiting function is used to configure the maximum bandwidth for LAN ports of APs to avoid the slow Internet access of wireless users in a scenario where wireless and wired users coexist and wired users occupy a substantial bandwidth.

1.3.3 Configuring the LAN/WAN Attribute of an AP Port

Working Principle

When the AP starts, determine whether to use the default port attribute or the changed port attribute as the WAN/LAN capability value of the port based on whether the WAN/LAN attribute of the port has been changed. This enables switching the WAN/LAN attribute of ports and meets the deployment requirements for different AP port attributes.

1.4 Configuration

Configuration	Description and Command	
Configuring the Default VLAN of an AP	⚠ (Optional) It is used to configure the native VLAN of an AP.	
	ap-vlan	Configures the default VLAN of an AP.
Configuring the Transmission VLAN of an AP	⚠ (Optional) It is used to configure the transmission VLAN of an AP.	
	pass-vlan	Configures the transmission VLAN of an AP.

Configuring a VLAN for	(Optional) It is used to configure a VLAN for an Ethernet port that provides wired access.	
	wired-vlan	Configures a VLAN for an Ethernet port.
Configuring a VLAN for a Cascade Port	(Optional) It is used to configure a VLAN for a connected non-micro AP.	
	wired-vlan connect	Configures a VLAN for a connected non-micro AP.
Configuring the Ethernet Port Status of an AP	(Optional) It is used to disable an Ethernet port of an AP that provides wired access.	
	wired-interface	Disables an Ethernet port of an AP.
Configuring the Sub-Interface of the WAN Interface on the AP	(Optional) It is used to configure the sub-interface of the WAN interface on the AP.	
	ap-subif	Configures the sub-interface of the WAN interface on the AP.
Configuring a Bandwidth Limit for an Ethernet Port of an AP	(Optional) It is used to configure the maximum bandwidth of LAN ports of APs.	
	wired-rate *value*	Configures bandwidth limits of LAN ports of APs.
Configuring the Specified AP Port As a WAN Port	(Optional) It is used to configure the port attribute.	
	wired-mode wan eth	Configures the specified AP port as a WAN port.
Configuring the Specified AP Port As a LAN Port	(Optional) It is used to configure the port attribute.	
	wired-mode lan eth	Configures the specified AP port as a LAN port.

1.4.1 Configuring the Default VLAN of an AP

Configuration Effect

- An AP automatically removes the tag from a frame that carries the native VLAN before forwarding the frame. That is, in local forwarding mode, if the VLAN of a STA is the same as the native VLAN, the frame of the STA does not carry the tag when forwarded, and the access switch determines the VLAN to which the STA belongs.

Notes

- After this command is executed, an online AP will be disconnected and then reconnected.
- When a wireless distribution system (WDS) is deployed, the same AP-VLAN must be planned for the root bridge and non-root bridge devices; otherwise, the non-root bridge devices cannot share the same address pool with root bridge devices or the non-root bridge devices cannot even forward packets properly.
- This command needs to be configured only in the following case: In local forwarding mode, STAs and an AP are on the same subnet and VLANs have been configured for the STAs and the AP. This command is not required in other cases.

- If the static DHCP address pool is configured, and the client ID is specified to use Bridge-Group Virtual Interface (BVI) 1, configuration of this command will change the BVI interface of the AP. In this case, the DHCP server configuration must be modified; otherwise, the address cannot be obtained.
- If the AP uses the PPPoE dial-up mode to obtain the address, the CAPWAP module on the AP will select dialer 1 as the source interface, and the STA traffic will be forwarded without carrying the tag. Therefore, this command is meaningless.

Configuration Steps

Configuring the Default VLAN of an AP

- Optional.
- When the native VLAN of a STA needs to be planned, set the default VLAN of an AP to the same as the VLAN of the STA. In this way, both the VLAN of the STAr and the VLAN of the AP are determined by the access switch.

Command	ap-vlan *vlan-id*
Parameter Description	*vlan-id*: Indicates a specified VLAN ID. The value ranges from 1 to 4094. The default value is 1.
Defaults	1
Command Mode	AP configuration mode or all AP (ap-config all) configuration mode
Usage Guide	An AP automatically removes the tag from a frame that carries the native VLAN before forwarding the frame. That is, in local forwarding mode, if the VLAN of a STA is the same as the native VLAN, the frame of the STA does not carry the tag when forwarded, and the access switch determines the VLAN to which the STA belongs.

Verification

- Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configuration of a specified AP.

Configuration Example

Setting the Native VLAN ID of AP1 to 20

Configuration Steps	• Enter the AP configuration mode on the AC. • Set the VLAN ID of the native VLAN of AP1 to **20**.
AC	`Hostname(config)# ap-config AP1` `Hostname(config-ap)# ap-vlan20`
Verification	Run the **show ap-config running** command to display the location information of AP1.

AC	Hostname#show ap-config running ! ap-config AP1 ap-vlan 20 !

Common Errors

For example, the native VLAN of the switch is VLAN 20, and all wireless/wired users and APs belong to VLAN 20. The following configurations are incorrect:

On the AC:

```
Hostname(config)# ap-configAP120
Hostname(config-ap)# wired-vlan20
Hostname(config-ap)# exit
Hostname(config)#wlan-config 1 ssid
Hostname(config-wlan)#tunnel local
Hostname(config-wlan)#exit
Hostname(config)#ap-group default
Hostname(config-ap-group)#interface-mapping 1 20 radio 1
```

On the switch:

```
Hostname(config)#interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
Hostname(config-if-GigabitEthernet 0/1)#switchport trunk native vlan 20
```

The configurations here are incorrect because the VLAN of users is different from the native VLAN of APs. Therefore, the uplink packets of APs carry tag 20 when forwarded, and the access switch transparently forwards VLAN 20 and assigns addresses to users. As the native VLAN of the switch is VLAN 20, the downlink packets do not carry the tag when forwarded. The Native VLAN of APs is 1 by default. Therefore, the packets cannot be forwarded to users, causing a failure for wireless and wired users to obtain IP addresses.

Either of the following methods can be used to modify the configurations:

Method 1: Change **wired-vlan 20** to **wired-vlan 1** and **interface-mapping 1 20 radio 1** to **interface-mapping 1 1 radio 1**, and the native VLAN of the switch remains unchanged.

Method 2: Add the native VLAN configurations for APs, and other configurations remain unchanged.

On the AC:

```
Hostname(config)# ap-configAP120
Hostname(config-ap)# ap-vlan 20
```

1.4.2 Configuring the Transmission VLAN of an AP

Configuration Effect

- When the i-Share+ APs are cascaded or a ring network is deployed, configure transmission VLANs for the master APs. This allows the uplink master APs to forward packets from STAs associated with different APs when STAs are deployed on different VLANs.

Notes

- The transmission VLAN cannot conflict with the VLANs specified by the **interface-mapping**, **ap-vlan**, and **wired-vlan** commands, and cannot be VLAN 2444.

Configuration Steps

Configuring the Transmission VLAN of an AP

- Optional.
- When the i-Share+ APs are cascaded or a ring network is deployed, run this command to configure the transmission VLAN. This allows the uplink master APs to forward packets from STAs associated with different APs when STAs are deployed on different VLANs.

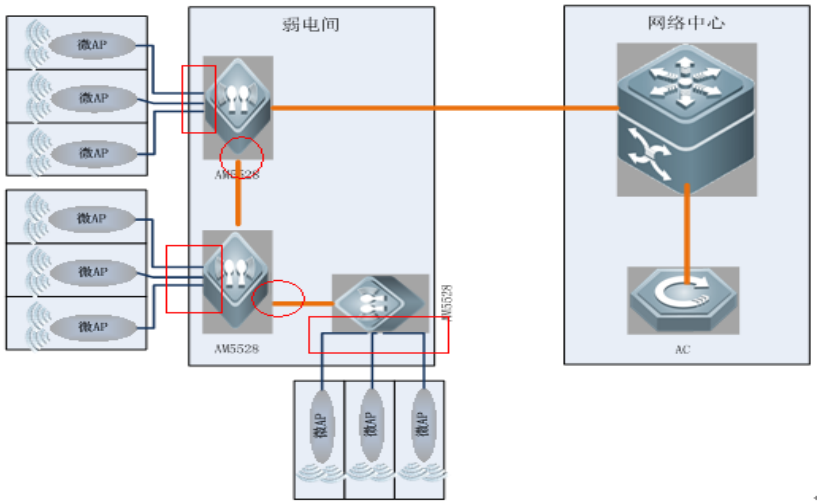
Command	**pass-vlan** *vlan-range*
Parameter Description	*vlan-range*: Indicates the VLAN ID range. Multiple VLAN IDs can be specified. Separate two VLAN IDs by a comma (,) and separate two VLAN ID ranges by a hyphen (-).
Defaults	No VLAN is configured.
Command Mode	AP configuration mode
Usage Guide	1. This command can be configured for all APs but takes effect only on the i-Share+ master AP. 2. When this command is run, the transmission VLAN will be created on the i-Share+ master AP, enabling the master AP to forward packets based on the transmission VLAN. In addition, the transmission VLAN will be automatically pruned on the downlink port of the master AP, to prevent broadcast and multicast packets of other master APs from being flooded to micro APs connected to the master AP.

Verification

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

Configuration Example

↘ **Configuring the Transmission VLAN of an i-Share+ Master AP**

Scenario **Figure 1-3**	 As shown in the cascading deployment topology, provided that the VLANs for the three AM5528 master APs from top to bottom are set to VLAN 10, VLAN 20, and VLAN 30 respectively.
Configuration Steps	● Enter the AP configuration mode of the AC. ● Configure the transmission VLANs of AM-1 as VLAN 20 and VLAN 30 to enable interconnection with the VLANs of AM-2 and AM-3. ● Configure the transmission VLAN of AM-2 as VLAN 30 to enable interconnection with the VLAN of AM-3.

AC	`Hostname(config)#ap-config AM-1`
	`Hostname(config-ap)# pass-vlan 20,30 //VLAN 20 and VLAN 30 for interconnection with AM-2 and AM-3`
	`Hostname(config-ap)# exit`
	`Hostname(config)#ap-config AM-2`
	`Hostname(config-ap)# pass-vlan 30  // VLAN 30 for interconnection with AM-3`

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

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AM-1`
	`pass-vlan 20,30`
	`!`
	`ap-config AM-2`
	`pass-vlan 30`
	`!`

Common Errors

N/A

1.4.3 Configuring a VLAN for an Ethernet Port of an AP

Configuration Effect

- Specify the VLAN of wired users when the AP provides Ethernet ports for access of wired users.

Notes

- This command can be configured on all APs, but the configuration take effect only on APs that provide Ethernet ports.
- If this command does not contain the **port** parameter, the same VLAN is configured for all Ethernet ports. When the same VLAN needs to be configured for all ports, the command is configured without the **port** parameter.
- In wireless AP mode, the AP implements only the wireless access function, but does not assign addresses to users. In this mode, if the VLAN used by the Ethernet port is configured the same as the VLAN of the AP, the VLAN of the packets sent over the Ethernet port will be determined by the access switch, instead of the VLAN specified in this command. If the packets sent over the Ethernet port must contain the tag when forwarded, the native VLAN of the access switch cannot be the same as the VLAN of the Ethernet port; otherwise, the packets cannot be forwarded to the Ethernet port.
- In wireless routing mode, the AP can assign addresses to users. In this mode, wired users obtain IP addresses from the DHCP address pool, and the VLAN corresponding to the address pool must be the same as the VLAN specified in this command.
- When the configuration of the Ethernet port is automatically saved on the AP and the VLAN of the Ethernet port is different from the native VLAN of the AP, and the IP address of the Ethernet port cannot be obtained after the AP is restarted, management cannot be implemented through the Ethernet port. In this case, press and hold the Reset button on the AP to restore the factory settings.

Configuration Steps

↘ Configuring the Access VLAN of an Ethernet Port of an AP

- Optional.
- To configure a different VLAN for the Ethernet port from the VLAN of the AP, run the **wired-vlan** command on the AC.

Command	**wired-vlan** *vlan-id* [**slot** *slot-id* [**secondary**]] [**port** *port-id*] **auto-save**
Parameter Description	*vlan-id*: Indicates the specified VLAN ID. The VLAN ID ranges from 1 to 4094. By default, the VLAN used by the Ethernet port is the same as the VLAN of the AP. *slot-id*: Indicates the slot to which a micro AP belongs. The value ranges from 1 to 24. **secondary**: Applies to the secondary device in the slot. *port-id:* Indicates the Ethernet port ID. The value ranges from 1 to 8. **auto-save**: Indicates that configuration is automatically saved on the AP. After the AP is restarted, the configuration can be restored.
Defaults	The VLAN of the Ethernet port is not configured, indicating that this VLAN is the same as the VLAN of the AP.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode

Usage Guide	The *slot* parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all micro APs. If the secondary parameter is configured, the configuration applies to the secondary device in a cascading scenario. Otherwise, the configuration takes effect for the primary device in a non-cascading or cascading scenario. In wireless AP mode, the AP implements only the wireless access function, but does not assign addresses to users. In this mode, if the VLAN used by the Ethernet port is configured the same as the VLAN of the AP, the VLAN of the packets sent over the Ethernet port will be determined by the access switch, instead of the VLAN specified in this command. If the packets sent over the Ethernet port must contain the tag when forwarded, the native VLAN of the access switch cannot be the same as the VLAN of the Ethernet port; otherwise, the packets cannot be forwarded to the Ethernet port. In wireless routing mode, the AP can assign addresses to users. In this mode, wired users obtain IP addresses from the DHCP address pool, and the VLAN corresponding to the address pool must be the same as the VLAN specified in this command. The fit AP is started without being configured, and its configurations are delivered from the AC. The **auto-save** parameter can be configured to automatically save the Ethernet port configurations on the AP. In this way, when the AP is disconnected from the AC, the Ethernet port configurations can be restored after the AP is restarted, and users can still access the network through the Ethernet port.

Verification

Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Configuring VLAN 20 for the Ethernet Port of AP1

Configuration Steps	Enter the AP configuration mode on the AC. Configure VLAN 20 for the Ethernet port of AP1.
AC	`Hostname(config)# ap-config AP1` `Hostname(config-ap)# wired-vlan20`
Verification	Run the **show ap-config running** command to display the configuration of AP1.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP1`
	`wired-vlan 20`
	`!`

Common Errors

N/A

1.4.4 Configuring a VLAN for a Cascade Port

Configuration Effect

- In i-Share+ scenarios, configure a VLAN for the connected non-micro APs (such as external IoT devices directly connected to the master AP or external IoT devices connected to micro APs). This VLAN is called a connect VLAN for differentiation from the VLAN of the Ethernet port.

Notes

- This command is available only for the i-Share+ APs.
- A connect VLAN is configured for a non-micro AP connected to a cascade port. If a connect VLAN is configured and then a micro AP is connected, a fault may occur. For example, the micro AP cannot access the master AP.
- Set the *slot* parameter to specify a port. Otherwise, the configuration takes effect on all ports.
- When the **secondary** parameter is not contained in this command, a connect VLAN is configured for the cascade port of the master AP. If this command carries the **secondary** parameter, a connect VLAN is configured for cascade ports of micro APs.

Configuration Steps

↘ Configuring a VLAN for a Cascade Port

- Optional.
- To configure a VLAN for a device connected to a cascade port, run this command on the AC.

Command	**wired-vlan** *vlan-id* [**slot** *slot-id*] **connect** [**secondary**]
Parameter Description	*vlan-id*: Specifies the connect VLAN ID. The value ranges from 1 to 4094. By default, the connect VLAN of a cascade port is the same as the default VLAN of a micro AP. *slot-id*: Specifies the slot to which a micro AP is connected. The value ranges from 1 to 24. **secondary**: Specifies the cascade device in the current slot.
Defaults	No VLAN is configured for a cascade port.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	This command is available only for the i-Share+ APs. A connect VLAN is configured for a non-micro AP connected to a cascade port. If a connect VLAN is configured and then a micro AP is connected, a fault may occur. For example, the micro AP cannot access the master AP. Set the *slot* parameter to specify a port. Otherwise, the configuration takes effect on all ports. When the **secondary** parameter is not contained in this command, a connect VLAN is configured for the cascade port of the master AP. If this command carries the **secondary** parameter, a connect VLAN is configured for cascade ports of micro APs.

Verification

- Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Configuring Connect VLAN 20 for the Non-micro AP Connected to Slot 1 of the Master AP

Configuration Steps	• Enter the AP configuration mode on the AC. • Configure connect VLAN 20 for the non-micro AP.
AC	`Hostname(config)# ap-config AP1` `Hostname(config-ap)# wired-vlan 20 slot 1 connect`
Verification	• Run the **show ap-config running** command to display the configuration of AP1.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP1`
	`wired-vlan 20 slot 1 connect`
	`!`

Configuring Connect VLAN 30 for the Non-micro AP Connected to the Cascade Port of the Micro AP That Is Connected to Slot 2 of the Master AP

Configuration Steps	• Enter the AP configuration mode on the AC. • Configure connect VLAN 30 for the non-micro AP.
AC	`Hostname(config)# ap-config AP1` `Hostname(config-ap)# wired-vlan 30 slot 2 connect secondary`
Verification	• Run the **show ap-config running** command to display the configuration of AP1.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP1`
	`wired-vlan 30 slot 2 connect secondary`
	`!`

Common Errors

- N/A

1.4.5 Configuring the Ethernet Port Status of an AP

Configuration Effect

- Enable or disable an Ethernet port of an AP.

Notes

- This command can be configured on all APs, but the configuration takes effect only on APs that provide Ethernet ports.
- If this command does not contain the **port** parameter, the same configuration is applied to all Ethernet ports. When all ports needs to be disabled, the command without the **port** parameter is configured and displayed. The *slot* parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all micro APs connected to 24 slots.
- When the Ethernet port is disabled, management cannot be implemented through the Ethernet port after the AP is restarted. In this case, you can press and hold the Reset button on the AP to restore factory settings.

Configuration Steps

Configuring the Status of an Ethernet Port of an AP

- Optional.
- To enable or disable an Ethernet port of an AP, run the **wired-interface** command on the AC.

Command	**wired-interface** [**slot** *slot-id* [**secondary**]] [**port** *port-id*] **enable**
Parameter Description	*slot-id*: Indicates the slot to which a micro AP is connected. The value ranges from 1 to 24. **secondary**: Applies to the secondary device in the slot. *port-id:* Indicates the Ethernet port ID. The value ranges from 1 to 8. **enable**: Enables the specified Ethernet port.
Defaults	All Ethernet ports are enabled.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	The Ethernet ports of APs can be disabled when APs provide the Ethernet ports for access of wired users, but the application scenario does not require access to the wired network or deployment of the wired network is not completed yet. The *slot* parameter takes effect only for i-Share+ APs. If no slot is specified, the configuration applies to all micro APs. If the **secondary** parameter is configured, the configuration applies to the secondary device in a cascading scenario. Otherwise, the configuration takes effect for the primary device in a non-cascading or cascading scenario.

Verification

Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Disabling All Ethernet Ports of AP1

Configuration Steps	Enter the AP configuration mode on the AC. Disable all Ethernet ports of AP1.
AC	`Hostname(config)# ap-config AP1` `Hostname(config-ap)# no wired-interfaceenable`
Verification	Run the **show ap-config running** command to display the configuration of AP1.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP1`
	`no wired-interfaceenable`
	`!`

Common Errors

N/A

1.4.6 Configuring the Sub-Interface of the WAN Interface on the AP

Configuration Effect

- A wireless AP creates a sub-interface of the WAN interface by default to forward tagged packets sent from STAs. In wireless routing mode where the AP can assign addresses to STAs, the AP functions as the gateway for STAs, and the packets do not need to contain a tag when forwarded. You can run the **ap-subif enable** command to delete the sub-interface of the WAN interface on the AP to prevent an address conflict caused by the same gateway address of STAs.

Notes

- If the AP obtains the address in PPPoE dial-up mode, the sub-interface of the WAN interface on the AP will be automatically deleted. In dial-up mode, this command cannot be used to configure the sub-interface of the WAN interface on the AP.

Configuration Steps

↘ Configuring the Sub-Interface of the WAN Interface on the AP

- Optional.
- In wireless routing mode, delete the sub-interface of the WAN interface on the AP; otherwise, an address conflict occurs when a large number of packets are forwarded through the sub-interface because the gateway addresses of STAs are the same.

Command	**ap-subif enable**
Parameter Description	N/A

Defaults	A sub-interface of the WAN interface is created.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Verification

Run the **show running** command to display the configurations of all APs, or the **show ap-config running** command to display the configurations of a specified AP.

Configuration Example

Deleting the Sub Interface of the WAN Interface on AP1

Configuration Steps	Enter the AP configuration mode on the AC. Delete the sub-interface of the WAN interface on AP1.
AC	`Hostname(config)# ap-config AP1` `Hostname(config-ap)# no ap-subif enable`
Verification	Run the **show ap-config running** command to display the configuration of AP1.

AC	`Hostname#show ap-config running`
	`!`
	`ap-config AP1`
	` no ap-subif enable`
	`!`

Common Errors

N/A

1.4.7 Configuring a Bandwidth Limit for an Ethernet Port of an AP

Configuration Effect

- Configure a bandwidth limit for a LAN port.

Notes

- N/A

Configuration Steps

Configuring a Bandwidth Limit for a LAN Port

- Optional.

- Perform this configuration on the AC.
- Run the **wired-rate** command to configure a bandwidth limit for a LAN port.

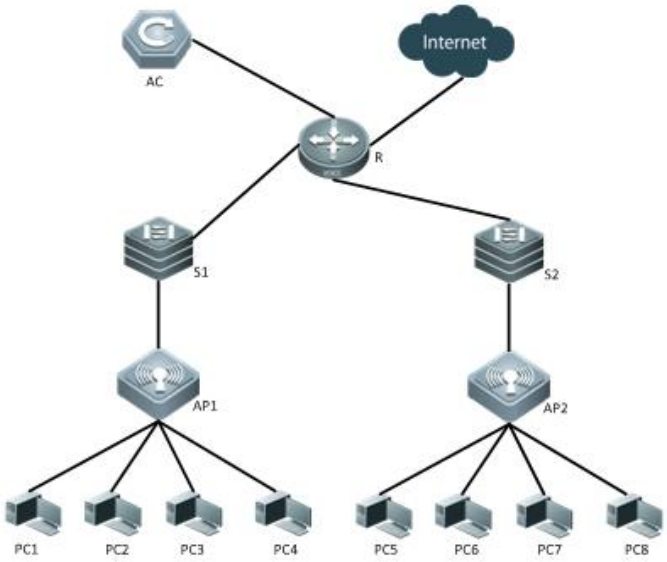
Command	**wired-rate** *value* [**port** *port-id*]
Parameter Description	If no port ID is specified, all ports are configured.
Defaults	The bandwidth of each LAN port is not limited. The maximum bandwidth for each LAN port is auto-negotiated.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	The bandwidth of each LAN port is not limited by default. The supported configuration may vary depending on the actual product.

Verification

- Run the **show running-config** command to display the bandwidth limit configuration of LAN ports.

Configuration Example

Configuring LAN Port Bandwidth Restriction

Scenario **Figure 1-4**	 Assume that the bandwidths of the LAN ports need to be limited on the fit AP network. • Configure the maximum bandwidth for LAN ports.
Configuration Steps	• On the AC, set the maximum bandwidth of port 3 on the AP to 30 Mbps.
AC	`Hostname(config)# ap-config [ap-name]` `Hostname(config-ap)# wired-rate 30 port 3`
	• On the AC, set the maximum bandwidth of port 3 in the AP group to 30 Mbps.
AC	`Hostname(config)# ap-group default`

	`Hostname(config-group)#wired-rate 30 port 3`
	● On the AC, set the maximum bandwidth of all LAN ports in the AP group to 30 Mbps.
AC	`Hostname(config)# ap-group default` `Hostname(config-group)#wired-rate 30`
	● On the AC, set the maximum bandwidth of port 3 on all APs to 30 Mbps.
AC	`Hostname(config)# ap-config all` `Hostname(config-ap)# wired-rate 30 port 3`
	● On the AC, set the maximum bandwidth of port 3 of slot 3 on the i-Share+ AP to 30 Mbps.
AC	`Hostname(config)# ap-config am5528` `Hostname(config-ap)# wired-rate 30 port 3 slot 3`
	● On the AC, set the maximum bandwidth of all LAN ports of slot 3 on the i-Share+ APs to 30 Mbps.
AC	`Hostname(config)# ap-config am5528` `Hostname(config-ap)# wired-rate 30 slot 3`
Verification	● On the AC, run the **show ap-config running-config** command to display the configuration.

AC	`Hostname(config)# show ap-config running-config`
	`ap-config ap120w-4`
	`wired-rate 30 port 3`

	● On the AC, run the **show running-config** command to display the configuration.

AC	`Hostname(config)# show running-config`
	`ap-group default`
	`wired-rate 30 port 3`

	● On the AC, run the **show running-config** command to display the configuration.

AC	`Hostname(config)# show running-config`
	`ap-group default`
	`wired-rate 30`

	● On the AC, run the **show running-config** command to display the configuration.

AC	`Hostname(config)# show running-config`
	`ap-config all`
	`…`
	`wired-rate 30 port 3`
	`…`
	
	`Hostname(config)# show running-config`

```
ap-config am5528
 …
 wired-rate 30 port 3 slot 3
 …
```

```
Hostname(config)# show running-config
ap-config am5528
 …
 wired-rate 30 slot 3
 …
```

Common Errors

- N/A

1.4.8 Configuring the Specified AP Port As a WAN Port

Configuration Effect

Configure the specified AP port as a WAN port.

Notes

- The configuration takes effect after the device is restarted if the specified port is a LAN port, and its default port attribute is LAN.
- This command is effective only for RG-AP880-AR, RG-AP880-A, RG-AP840-I(V2), RG-AP850-AR(V3), and RG-AP820-AR(V3) devices with the port attribute of WAN+LAN.

Configuration Steps

↘ Configuring the Specified AP Port As a WAN Port

Optional. Run the **wired-mode wan eth** *port_idx* command to configure the specified AP port as a WAN port.

Command	**wired-mode wan eth** *port_idx*
Parameter Description	*port_idx*: Indicates the number of the port to be configured as a WAN port. The value is an integer with a length of 1.
Defaults	By default, the port attribute is not configured.
Command Mode	AP configuration mode
Usage Guide	This command is used to change the attribute of the specified AP port to WAN. It does not take effect on WAN ports.

Verification

Run the **show ap-config running** *ap-name* command on the AC to check whether the configuration is successful.

Configuration Example

Configuring the Specified AP Port As a WAN Port

Configuration Steps The following example configures the attribute of the gigabitEthernet 0/2 port to WAN on the AC.

AC

```
Hostname(config)#ap-config 00d0.f822.3383
Hostname(config-ap)#wired-mode wan eth 2
```

Verification Run the **show ap-config running** *apname* command on the AC to display the AP information.

AC

```
Hostname#show ap-config running 00d0.f822.3383
Building configuration...
Current configuration: 199 bytes
!
ap-config 00d0.f822.3383
 ap-mac 00d0.f822.3383
 wired-mode wan eth 2
!
end
```

1.4.9 Configuring the Specified AP Port As a LAN Port

Configuration Effect

Configure the specified AP port as a LAN port.

Notes

- The configuration takes effect after the device is restarted if the specified port is a WAN port, and its default port attribute is LAN.
- This command is effective only for RG-AP880-AR, RG-AP880-A, RG-AP840-I(V2), RG-AP850-AR(V3), and RG-AP820-AR(V3) devices with the port attribute of WAN+LAN.

Configuration Steps

Configuring the Specified AP Port As a LAN Port

Optional. Run the **wired-mode lan eth** *port_idx* command to configure the specified AP port as a LAN port.

Command	**wired-mode lan eth** *port_idx*
Parameter Description	*port_idx*: Indicates the number of the port to be configured as a LAN port. The value is an integer with a length of 1.
Defaults	By default, the port attribute is not configured.
Command Mode	AP configuration mode
Usage Guide	This command is used to change the attribute of the specified AP port to LAN. It does not take effect on LAN ports and ports with the default attribute of WAN.

Verification

Run the **show ap-config running** *ap-name* command to check whether the **wired-mode wan eth** *port_idx* configuration is cleared.

Configuration Example

Configuring the Specified AP Port As a LAN Port

Configuration Steps

The following example configures the attribute of the gigabitEthernet 0/2 port to LAN on the AC.

AC

```
Hostname(config)#ap-config 00d0.f822.3383
Hostname(config-ap)#wired-mode lan eth 2
```

Verification

Run the **show ap-config running** *apname* command on the AC to display the AP information.

AC

```
Hostname#show ap-config running 00d0.f822.3383
Building configuration...
Current configuration: 199 bytes
!
ap-config 00d0.f822.3383
 ap-mac 00d0.f822.3383
!
end
```

1.5 Monitoring

Clearing

N/A

Displaying

N/A

Debugging

N/A

1 Configuring AMMG

1.1 Overview

AM Management (AMMG) is used to manage all-optical i-Share master access points (all-optical AMs) and micro access points (APs).

Protocols and Standards

N/A

1.2 Features

Basic Concepts

MAP

Downlink micro APs connected to all-optical AMs are called MAPs.

MQTT

Message Queuing Telemetry Transport (MQTT) is a transmission protocol of the International Organization for Standardization (ISO) standard (ISO/IEC PRF 20922) and a lightweight message protocol in binary transmission mode.

On a simplified all-optical i-Share+ network, MQTT clients are all-optical AMs, and MQTT servers are access controllers (ACs). In the following sections, MQTT servers are referred to as ACs. An MQTT channel is a message channel established between an all-optical AM and an AC.

Four Power Output Ports

An all-optical AM provides four 56 V power output ports, achieving centralized power supply for downlink MAPs.

Overview

Feature	Description
Upgrading an All-Optical AM	Upgrades the software of an all-optical AM.
Configuring Basic Information of All-Optical AMs	Configures the name, command template, statuses of the four power output ports, and status description of the four power output ports of an all-optical AM.
Configuring the Working Mode of an All-Optical AM	Configures the working mode of an all-optical AM. An all-optical AM can work in i-Share mode that supports only MAPs and common mode that support any APs.

1.2.1 Upgrading an All-Optical AM

An AC can upgrade the software of all all-optical AMs or a specific all-optical AM.

Working Principle

After all-optical AM upgrade is initiated manually on an AC, the AC verifies the model, version, and other information of the all-optical AMs and upgrades the software of the all-optical AMs that meet the conditions. Currently, all-optical AMs can be upgraded using a File Transfer Protocol (FTP) channel. The detailed procedure is described as follows:

Upgrade through an FTP channel: The AC functions as the FTP server. The all-optical AMs that need to be upgraded function as the FTP clients, obtain the software version package from the AC using the FTP mode, and complete the upgrade.

1.2.2 Configuring Basic Information of All-Optical AMs

Configure basic information of all all-optical AMs, including their name, pre-configured template information, and statuses of the four power output ports on the AC in a unified manner, enabling administrators to perform quick network planning.

Working Principle

After an all-optical AM goes online, the AC delivers the pre-configured template information to the all-optical AM over an MQTT channel.

1.2.3 Configuring the Working Mode of an All-Optical AM

An all-optical AM can work in i-Share mode or common mode.

Working Principle

The two working modes differ in the type of APs allowed to connect to the downlink ports of an all-optical AM, the method for discovering an AC, and the MAP management method.

- i-Share mode

  Only MAPs are allowed to access an all-optical AM working in i-Share mode.

  The all-optical AM establishes an MQTT channel with an AC. After the channel is established, the all-optical AM advertises the AC IP address to an MAP. The MAP attempts to establish a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel with the AC based on the IP address of the AC. When a non-MAP attempts to access a downlink port of the all-optical AM, the port is automatically shut down.

  After the MAP accesses the AC through the CAPWAP channel, the all-optical AM reports the port, media access control (MAC) address, and name of the MAP to the AC. The AC centrally manages MAPs through the all-optical AM.

- Common mode

  All APs are allowed to interconnect with an all-optical AM working in common mode.

  Functioning as a common switch, the all-optical AM establishes an MQTT channel with an AC. This channel is only used by the AC to manage the all-optical AM. When an AP accesses a downlink port of the all-optical AM, the AP discovers an AC through the DHCP or domain name system (DNS) mode and establishes a CAPWAP tunnel with the AC. After the AP accesses the AC through the CAPWAP tunnel, the AP reports its basic information to the AC. The AC manages APs connected to the all-optical AM and common APs in the same way.

1.3 Configuration

Configuration	Description and Command	
Upgrading an All-Optical AM Through an FTP Channel	(Optional) It is used to upgrade the software of an all-optical AM through an FTP channel.	
	device-upgrade	Upgrades the software of an all-optical AM through an FTP channel.
Configuring a Name for an All-Optical AM	(Optional) It is used to configure a name for an all-optical AM.	
	device-name	Configures a name for an all-optical AM.
Creating AM Configuration	(Optional) It is used to add the configuration of the specified all-optical AM based on the MAC address.	
	device-config	Adds AM configuration or enters the AM configuration mode.
Configuring Template Information for an All-Optical AM	(Optional) It is used to configure a template for an all-optical AM.	
	cfgmg template	Adds a configuration template for an all-optical AM.
Configuring Statuses of the Four Power Output Ports for an All-Optical AM	(Optional) It is used to configure the statuses of the four power output ports of the specified AM.	
	power-central enable	Configures the statuses of the four power output ports of the specified all-optical AM.
Configuring the Working Mode of an All-Optical AM	(Optional) It is used to configure the working mode of an all-optical AM.	
	am-mode	Configures the working mode of the specified AM.

1.3.1 Upgrading an All-Optical AM Through an FTP Channel

Configuration Effect

- The AC upgrades the software of an all-optical AM through an FTP channel, and the upgrade is successful.

Notes

This command applies to all-optical AMs only.

Running the Upgrade Command

- Run the upgrade command on the AC.

Command	**device-upgrade** [**mac** *am-mac*] **url** *url-addr*
Parameter Description	*am-mac*: Indicates the MAC address of the all-optical AM to be upgraded. *url-addr*: Indicates the URL of the software version to be upgraded, including the FTP server address, account and password used to log in to the FTP server, and software version. The parameter is in ftp://user:pass@ip/filename format. **ip** indicates the IP address of the AC used to communicate with the all-optical AM. **filename** indicates the software version uploaded to the AC.
Defaults	If no MAC address of an all-optical AM is configured, the upgrade command takes effect to all all-optical

	AMs.
Command Mode	Global configuration mode
Usage Guide	1. A maximum of five all-optical AMs can be upgraded concurrently. 2. If the upgrade command does not carry the **mac** parameter, all all-optical AMs are upgraded. When the command is run, the AC starts upgrade and circularly searches for all-optical AMs that can be upgraded. If an all-optical AM can be upgraded, the AC delivers the **url** parameter of the software version to the all-optical AM. The AC detects whether the download progress on all-optical AMs changes at intervals. If the download progress on an all-optical AM does not change in three detection intervals, the AC determines that the download fails and adds the all-optical AM to the failure list. To achieve upgrade success, ensure that the FTP server channel is not occupied by other processes during the upgrade. Otherwise, the upgrade may fail. 3. Before running the upgrade command, enable the FTP function on the AC and upload the AM software version to the AC in advance. 4. If an all-optical AM is restarted or disconnected from the AC during the upgrade process and is not reconnected within the keepalive period (30s by default), the AC stops to upgrade the AM. If an all-optical AM re-associates with the AC in the keepalive period after it is disconnected from the AC, the upgrade continues. 5. After the command is configured, AMs that match the upgrade package after they go online can be upgraded automatically. To disable automatic upgrade, run the **no device-upgrade** url url-addr command. 6. Pay attention to the AM and AC connection environment. If AMs are serially-connected, they are upgraded in sequence. If one AM is restarted, the other AM that depends on this AM to connect with the network may fail to be upgraded. 7. If the username or password used to log in to the FTP server carries special characters, such as the at sign (@), pound sign (#), colon (:), comma (,), and exclamation mark (!), use **%** and the hexadecimal ASICLL code of a special character to replace it during command configuration. For example, "username chy#wuxian!01! password 123.1!2" can be replaced with ftp://chy%23wuxian%2101%21:123%2E1%212@1.1.1.1/123.bin.

Verification

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

Configuration Example

↘ Running the Upgrade Command

Configuration Steps	● Enable the FTP function on the AC.

AC	`Hostname# config terminal`
	`Hostname(config)#ftp-server enable`
	`Hostname(config)#ftp-server topdir flash`
	`Hostname(config)#ftp-server username acuser password acpasswd`

	● Display the FTP configuration.
AC	`Hostname(config)#show ftp-server` `ftp-server information`

	========== enable : Y topdir : flash:/ timeout: 10min username:acuser password:(PLAINT)acpasswd
	● Obtain the IP address for communicating with the all-optical AM on the AC.
AC	Hostname(config)#show ip interface brief Interface IP-Address(Pri) IP-Address(Sec) Status Protocol VLAN 1 172.30.103.158/24 no address up up
	● Upload the AM software version to the AC. ● Run the upgrade command.
AC	Hostname(config)#device-upgrade mac c0b8.e64b.9ee0 url ftp://acuser:acpasswd@172.30.103.158/filename.bin
	● Display the version information.
AM	AM5552-SF#show version System description : Hostname indoor AM5552-SF (802.11a/n/ac/ax and 802.11b/g/n/ax) By Hostname Networks. System start time : 2021-03-23 17:47:45 System uptime : 7:18:09:33 System hardware version : 1.00 System software version : AM_RGOS 11.9(0)B0, Release(08152214) System patch number : NA System serial number : G1P90PR00086A System boot version : 1.2.41 Module information: Slot 0 : AM5552-SF Cpu 0: Hardware version : 1.00 Boot version : 1.2 Software version : AM_RGOS 11.9(0)B0, Release(08152214) Serial number : G1P90PR00086A

Common Errors

N/A

1.3.2 Configuring a Name for an All-Optical AM

Configuration Effect

- Configure a name for an all-optical AM.

Notes

N/A

Configuration Steps

- Optional.
- Run the **device-name** command on the AC to configure a name for an all-optical AM in all-optical AM configuration mode.

Command	**device-name** *device-name*
Parameter Description	*device-name*: Indicates the name configured for an all-optical AM.
Defaults	N/A
Command Mode	All-optical AM configuration mode
Usage Guide	1. If the all-optical AM is online, the configured name takes effect immediately. 2. If the all-optical AM is offline, the configured name takes effect after the all-optical AM goes online. 3. After the name of the all-optical AM is configured, you can continue to configure the AM without exiting the all-optical AM configuration mode. 4. If the new name is already used by another all-optical AM, the configuration fails. 5. An all-optical AM name contains a maximum of 64 characters and cannot contain spaces. 6. Do not configure the same name for different offline all-optical AMs. The AM that goes online first uses the configured name, and AMs that go online later cannot use the configured name and will retain their original names.

Verification

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

Configuration Example

↘ Configuring a Name for an All-Optical AM with MAC Address 00ff.ffff.1111

Configuration Steps	● Set the new name of the all-optical AM to **Hostname_DEVICE** on the AC.
	`Hostname(config)# device-config 00ff.ffff.1111`
	`Hostname(config-device)#device-name Hostname_DEVICE`

	● Delete the name configuration of the all-optical AM.
	`Hostname(config)# device-config 00ff.ffff.1111`
	`Hostname(config-device)#no device-name`

Verification	Run the **show running-config** command to display the configuration of the all-optical AM.

AC	`Hostname#show running-config`
	`!`
	`device-name Hostname_DEVICE`
	`!`

Common Errors

N/A

1.3.3 Creating AM Configuration

Configuration Effect

- After the configuration for the AM with the specified MAC address is created, enter the AM configuration mode.
- If the configuration of the AM with this MAC address already exists, enter the AM configuration mode directly.
- The *device-mac* parameter carried in the **device-configdevice-config** command is the MAC address of the AM. When the all-optical AM goes online, the MAC address uploaded by the AM matches with the MAC address in the AM configuration to determine the relationship between the AM and the AM configuration.

Notes

N/A

Configuration Steps

- Optional.
- Run the **device-config** *device-mac command* on the AC in global configuration mode to create AM configuration.

Command	**device-config** *device-mac*
Parameter Description	*device-mac*: Indicates the MAC address of the all-optical AM.
Defaults	No AM configuration is created.
Command Mode	Global configuration mode
Usage Guide	1. You can run the **device-config** *device-mac command* to create AM configuration or enter the configuration mode of the specified all-optical AM. 2. You can run the **no device-config** *device-mac* command to delete the configuration of the specified all-optical AM unless it is online. The supported configuration may vary depending on the actual product.

Verification

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

Configuration Example

Creating the Configuration for the AM with the MAC Address 00ff.ffff.1111

Configuration Steps	● Create the configuration for the AM with the MAC address 00ff.ffff.1111.
AC	`Hostname(config)# device-config 00ff.ffff.1111` `Hostname(config-ap)#`
Verification	Run the **show running-config** command to display configuration of the all-optical AM.

AC	`Hostname#show running-config`
	`!`
	`device-config 00ff.ffff.1111`

	!

Common Errors

N/A

1.3.4 Configuring Template Information for an All-Optical AM

Configuration Effect

- When an all-optical AM accesses the AC for the first time, a configuration template is automatically synchronized. Based on the configuration of the all-optical AM, the network administrator determines whether commands in the configuration template are synchronized to the all-optical AM.
- Manually trigger configuration template synchronization on the AC. Based on the configuration of the all-optical AM, the network administrator determines whether commands in the configuration template are synchronized to the all-optical AM.

Notes

- A configuration template needs to be created before it is applied.
- An AC synchronizes the configuration template to an all-optical AM only when the all-optical AM accesses the AC for the first time.

Configuration Steps

- Optional.
- Configure template information on the AC in all-optical AM configuration mode.

Command	**cfgmg template** *temp-name*
Parameter Description	*temp-name*: Indicates the name of the configuration template specified for an all-optical AM on the AC. The configuration template needs to be created on the AC in advance.
Defaults	N/A
Command Mode	All-optical AM configuration mode
Usage Guide	1. A maximum of eight configuration templates can be applied. 2. When multiple configuration templates are applied, the sequence for synchronizing commands in these templates depends on the sequence when these templates are applied. 3. Applied configuration templates are delivered to an all-optical AM only when the all-optical AM associates with the AC for the first time. Subsequent template configuration changes are not proactively synchronized to the all-optical AM. 4. Applied configuration templates are not forcibly bound to configuration templates of the CFGMG module. A non-existent configuration template can be applied. However, no configuration can be synchronized. When configuration templates of the CFGMG module are deleted, applied configuration templates are not deleted. 5. When an all-optical AM goes online, it uploads the name, working mode, status of the power supplies, and status description to the AC. You do not need to configure the information in the configuration template. Otherwise, conflicts may occur, resulting in inconsistent configurations. A configuration template is delivered after the **device-config** command is run. Therefore, ensure

	consistent content at two ends to prevent misunderstandings caused by configuration changes after the configuration is overwritten. 6. When a configuration template is delivered to the AM, the AM updates the configuration based on the sequence of the commands in the template. If a command fails to be run, other commands in the template are not run. To address this issue, ensure that the AM supports all the commands in the template.

Verification

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

Configuration Example

↘ Creating a Configuration Template for an All-Optical AM with the MAC Address 00ff.ffff.1111

Configuration Steps	● Create a configuration template named **wlan-temp1**.
AC	`Hostname(config)#cfgmg template wlan-temp1` `Hostname(config-temp)#`
	● Configure the all-optical AM whose MAC address is 00ff.ffff.1111 and associate it with the configuration template **wlan-temp1**.

	`Hostname(config)#device-config 00ff.ffff.1111`
	`Hostname(config-device)#cfgmg template wlan-temp1`
	`Hostname(config-device)#`

Verification	Run the **show running-config** command to display the configuration of the all-optical AM.

AC	`Hostname#show running-config`
	`!`
	`device-config 00ff.ffff.1111`
	` cfgmg template wlan-temp1`
	`!`
	`cfgmg template wlan-temp1`
	`!`

Common Errors

N/A

1.3.5 Configuring Statuses of the Four Power Output Ports for an All-Optical AM

Configuration Effect

- Configure the statuses of the four power output ports for the specified all-optical AM. The four power output ports can be controlled independently.

Notes

N/A

Configuration Steps

Configuring the Statuses of the Four Power Output Ports

- Optional.
- Configure the statuses of the four power output ports on the AC in all-optical AM configuration mode.

Command	**power-central enable** *power-supply-index*
Parameter Description	*power-supply-index*: Indicates the ID of a power output port. The value range is from 1 to 4.
Defaults	The four power output ports are enabled.
Command Mode	All-optical AM configuration mode
Usage Guide	1. If the configuration on an all-optical AM is inconsistent with that on the AC, the configuration on the AC prevails. When the all-optical AM goes online, the AC delivers the configuration to the all-optical AM and the all-optical AM modifies the configuration. 2. The default statuses of the four power output ports are **enable**, which can be viewed by running the **show running-config** command. The supported configuration may vary depending on the actual product.

Configuring Status Description of the Four Power Output Ports

- Optional.
- Configure status description of the four power output ports on the AC in all-optical AM configuration mode.

Command	**power-central description** *power-supply-index desc*
Parameter Description	*power-supply-index*: Indicates the ID of a power output port. The value range is from 1 to 4. *desc:* Indicates the status description of the four power output ports.
Defaults	N/A
Command Mode	All-optical AM configuration mode
Usage Guide	1. If the configuration on an all-optical AM is inconsistent with that on the AC, the configuration on the AC prevails. When the all-optical AM goes online, the AC delivers the configuration to the all-optical AM and the all-optical AM modifies the configuration. 2. Status description of the four power output ports is null by default. You can configure the status description as required. Status description of each power supply cannot exceed 128 bytes. 3. Status description cannot contain spaces and must be consecutive character strings. The supported configuration may vary depending on the actual product.

Verification

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

Configuration Example

Disabling the Power Supply Function of the First Power Output Port on an All-optical AM

Configuration Steps	Disable the power supply function of the first power output port on an all-optical AM.
AC	`Hostname(config)# device-config 00ff.ffff.1111` `Hostname(config-device)# no power-central enable 1`
Verification	Run the **show running-config command** to display the configuration of the all-optical AM.

AC	`Hostname#show running-config`
	`!`
	`device-config 00ff.ffff.1111`
	`  no power-central enable 1`
	`!`

Common Errors

N/A

1.3.6 Configuring the Working Mode of an All-Optical AM

Configuration Effect

- Configure the working mode (i-Share mode or common mode) of an all-optical AM as required.

Notes

N/A

Configuration Steps

- Optional.
- Configure the i-share mode or common mode in all-optical AM configuration mode on the AC.

Command	**am-mode** { **normal** | **smart** }
Parameter Description	**normal**: Sets the working mode of an all-optical AM to the common mode. **smart**: Sets the working mode of an all-optical AM to the i-Share mode.
Defaults	The working mode of an all-optical AM is the i-Share mode.
Command Mode	All-optical AM configuration mode (AC)
Usage Guide	• When the working mode of an all-optical AM is changed on the AC and the all-optical AM is online, the working mode takes effect immediately. If the all-optical AM is offline, the working mode takes effect after the all-optical AM goes online. • After the working mode of an all-optical AM is changed, you can continue to configure the AM without exiting the all-optical AM configuration mode. • You are advised to change the working mode of an all-optical AM on the AC and the AC advertises the working mode configuration to the all-optical AM, ensuring consistent configurations at both ends. • If the working mode is changed on the all-optical AM, the all-optical AM needs to go offline and associate with the AC again. In this case, the devices at both ends automatically synchronize the working mode configuration. Principles for configuring automatic synchronization:

	1. If the working mode configuration exists on the AC or both ends, the AC delivers the working mode configuration to the AM to update the configuration on the AM. 2. If the working mode configuration exists only on the all-optical AM, the AC automatically saves the working mode configuration on the all-optical AM. ● When the all-optical AM is restored to factory settings, the default working mode is the i-Share mode. When the **no/default am-mode** command is run, the default working mode is the common mode. ● When the all-optical AM works in i-Share mode and the AP connected to the downlink port of the AM is not an MAP, the **shutdown/no shutdown** command is run to disconnect the AP.

Verification

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

Configuration Example

↘ Configuring an All-Optical AM to Work in i-Share Mode

Configuration Steps	Configure an all-optical AM to work in i-Share mode.
AC	`Hostname(config)# device-config 00ff.ffff.1111` `Hostname(config-device)# am-mode smart`
Verification	Run the **show running-config** command to display the configuration of the all-optical AM.

AC	`Hostname#show running-config`
	`!`
	`device-config 00ff.ffff.1111`
	` am-mode smart`
	`!`

1.4 Monitoring

Clearing

N/A

Displaying

Command	Description
show device-config interfaces fiber-channel	Displays the optical channel information of an all-optical AM associated with an AC.
show device-config interfaces transceiver	Displays the optical module information of an all-optical AM associated with an AC.
show device-config map summary	Displays the downlink MAP list of all all-optical AMs associated with an AC.
show device-config summary	Displays the list of all all-optical AMs associated with an AC.

show device-config summary by-name	Displays the list of all all-optical AMs associated with an AC in the sequence of names.
show device-config upgrading-list	Displays the list of all-optical AMs that are being upgraded.
show device-config version summary	Displays the version list of all all-optical AMs associated with an AC.
show device-config power summary	Displays the statuses of the four power output ports of all all-optical AMs associated with an AC.

Debugging

N/A

1 Configuring LED

1.1 Overview

Light Emitting Diode (LED) is a solid luminous semiconductor. It serves as an indicator light to display the working status of an access point (AP) in different colors.

The following part only introduces LED.

Protocols and Standards

N/A

1.2 Applications

N/A

1.3 Features

An AP provides one or multiple LEDs to display its working status. For example, the LED of an Ethernet interface blinks when a data flow exists on the Ethernet interface. The LED is controlled through a General Purpose Input/Output (GPIO) interface or Complex Programmable Logic Device (CPLD) to change the status and colors, such as solid green, blinking green, blinking red and so on. By observing the LED, you can easily tell AP's working status and faults.

1.4 Configuration

Configuration	Description and Command	
Configuring AP Location	(Optional) It is used to locate an AP.	
	led on	Turn on the LED to locate an AP.
Configuring Quiet Mode	(Optional). It is used to enable LED quiet mode.	
	quiet-mode session	Enable LED quiet mode.

1.4.1 Configuring AP Location

Configuration Effect

- Turn on the LED to locate an AP.

Notes

- Disable the configuration after location. Otherwise, the lighting of LEDs no longer changes.

Configuration Steps

Configuring AP Location

- Optional.
- Enable this configuration before location and disable it after location.

Command	**led on** [**slot** *slot-id* [**secondary**]]
Parameter Description	*slot-id*: Indicates the slot ID corresponding to the RF card. **secondary**: Applies to the secondary device in the slot.
Defaults	This function is disabled.
Configuration Mode	AP configuration mode
Usage Guide	Use this command to turn on the LED for locating an AP. For i-Share+ micro APs, specify the slot ID for each RF card. For non-i-Share+ micro APs, the *slot-id* parameter is invalid. The **secondary** parameter indicates that the command applies to the secondary device. If the **secondary** parameter is not configured, this command takes effect on the primary device.

Verification

- Check whether the location LED is on the AP.

Configuration Examples

Locating AP 00d0.f822.33bc

Scenario	N/A
Configuration Steps	Configure AP location on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config 00d0.f822.33bc`
	`Hostname(ap-config)# led on`

Verification	Check whether the location LED is on the AP.

Common Mistakes

N/A

1.4.2 Configuring Quiet Mode

Configuration Effect

- All LEDs on an AP are off when this command takes effect.

Notes

- The effective time for the quiet mode must be configured first.

Configuration Method

Creating a Session

- Optional.
- Create a session before configuring the quiet mode.
- Configure the effective time for the session.

Command	**schedule session** *sid* **time-range** *n* **period** *day1* [**to** *day2*] **time** *hh1:mm1* **to** *hh2:mm2*
Parameter Description	*sid*: Indicates the scheduling session ID. *n*: Indicates the scheduling session time period number. *day1*: Indicates the start date of the scheduling time period, in the range of { sun | mon | tue | wed | thu | fri | sat }. **to** *day2*: Indicates the scheduling time period is set to one day by default. *day 2* indicates the end date of the scheduling time period. **time** *hh1:mm1* **to** *hh2:mm2*: Indicates the scheduling time. *hh1:mm1* is the start time and *hh2:mm2* the end time in the range from 0 to 23 hours and 0 to 59 minutes.
Defaults	The scheduling time period is set to null.
Command Mode	Global configuration mode
Usage Guide	Create a session first.

Configuring Quiet Mode

- Optional.
- Configuring LED quiet mode.

Command	**quiet-mode session** *session-num*
Parameter Description	session-num: Specifies a session ID.
Defaults	This function is disabled.
Configuration Mode	AP configuration mode
Usage Guide	Configure the session first.

Verification

- All LEDs are off when the system time is within the session interval.

Configuration Examples

Enabling LED Quiet Mode from 11 PM on Monday to 7 AM on Tuesday Every Week

Configuration Steps	● Configure a session. ● Configure the session ID for the quiet mode.
	Hostname# configure terminal Hostname(config)#schedule session 1 Hostname(config)#schedule session 1 time-range 1 period Mon time 23:00 to 7:00 Hostname(config)#ap-config 00d0.f822.33bc Hostname(config-ap)#quiet-mode session 1
Verification	When the system time is within the session interval, all LEDs on the AP are off.

Common Errors

- The configured session ID does not exist.

1.5 Monitoring

Clearing

N/A

Displaying

N/A

Debugging

N/A

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 Bluetooth Low Energy (BLE) technology, specifically, a broadcast frame named advertising in BLE. The advertising frame is sent periodically. 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 integration with an iBeacon base station to achieve connections. 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 messages such as coupons or information about commodities in the store to your phone through 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 Applications

Application	Description
WeChat Shake	iBeacon protocol and WeChat Shake are supported.

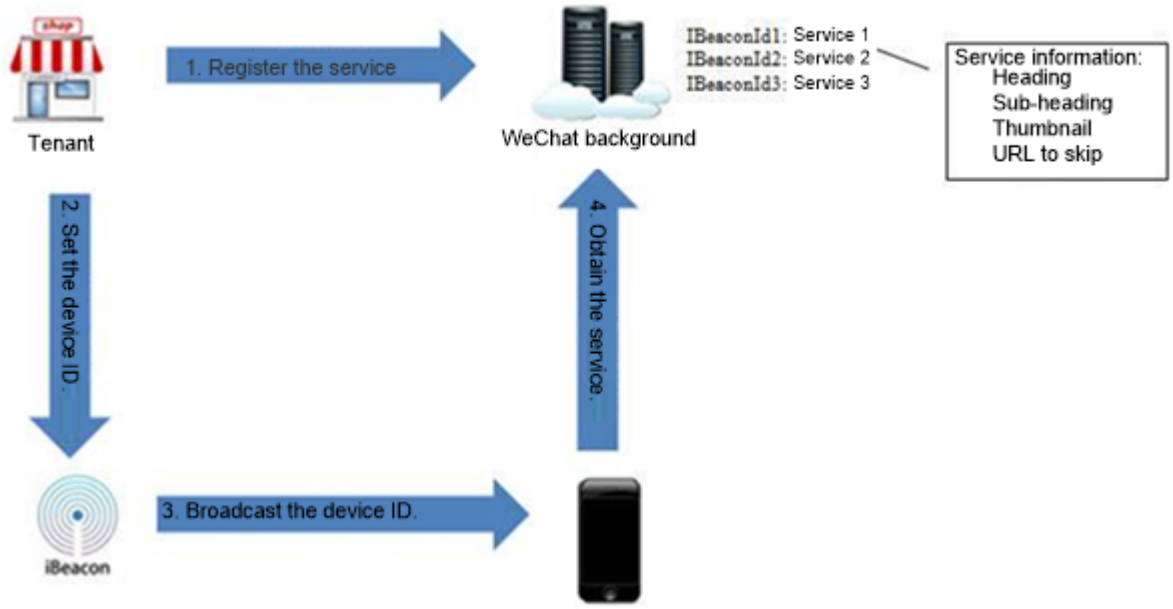
1.2.1 WeChat Shake

Scenario

The following figure shows the workflow:

1) The service provider (SP) applies to the WeChat backend for a service. The WeChat backend generates an iBeaconID, maps it to the service provided by the SP, and informs the SP of the iBeaconID.
2) The SP sets the iBeaconID on an iBeacon device and enables the iBeacon device to broadcast the iBeaconID.
3) After a user in the signal coverage of the iBeacon device enables the WeChat Shake function, the WeChat App obtains the iBeaconID.
4) Based on the obtained iBeaconID, the WeChat App pulls the corresponding service from the WeChat backend and shows the service in the result of shaking.
5) After the user clicks the result of shaking, together with the user information, the browser embedded in WeChat redirects to the URL filled in by the SP when the SP applies for the service in Step 1 and the application page is displayed.

Figure 1-1 WeChat Shake Workflow



Deployment

- The wireless access controller (AC) delivers related iBeacon configurations to APs.

1.3 Features

Basic Concepts

iBeacon Technology

- Beacon data consists of the following information: Unique General Identifier (UUID), Major, Minor, and Measured Power.
- **UUID** is a 128-bit identifier compliant with 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.

1.3.1 iBeacon

iBeacon is implemented through transmission of Bluetooth broadcast.

Working Principle

When the iBeacon configuration is modified on an AC, 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 through I2C.

After receiving the packet, the CC2541 Bluetooth chip parses the configuration packet and updates the iBeacon packet.

1.4 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	**ibeacon uuid major minor radio**	Configures the iBeacon function based on BT radio.

1.4.1 Configuring iBeacon

Configuration Effect

- Configure global (AP) iBeacon parameters.

Notes

- If the current device does not support Bluetooth, the configuration cannot take effect. Device models supporting iBeacon include: AP520(BT)v1.x, AP520 v1.x, AP4220, MA1220, AM5528 (EP).

Configuration Steps

Configuring iBeacon 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 APs supporting Bluetooth.

Command	**ibeacon uuid** *uuid* **major** *major* **minor** *minor*
Parameter Description	*uuid*: Indicates the **UUID** that is a string of 32 hexadecimal characters. *major*: Indicates the **Major** value that is a string of four hexadecimal characters. *minor*: Indicates the **Minor** value that is a string of four hexadecimal characters.
Defaults	iBeacon is not configured.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group 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. The iBeacon function cannot be configured on all APs.

Verification

- Run the **show ap-config running** *ap-name* command on an AC to check whether the configuration is successful.

Configuration Examples

Configuring iBeacon for the Specified AP

Configuration Steps	• Configure iBeacon for the specified AP.
	Hostname# configure terminal Hostname(config)#ap-config ap520(bt) Hostname(config-ap)# ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154
Verification	After configuring iBeacon for the specified AP, you can run the **show ap-config running** *ap-name* command on an AC to check the configuration.
	AC: Hostname(config)#show ap-config running ap520(bt) ! ap-config ap520(bt) ... ... ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154... ... !

1.4.2 Configuring iBeacon Based on BT Radio

Configuration Effect

Configure iBeacon parameters based on BT radio.

Notes

If the device does not support Bluetooth, the configuration does not take effect. Device models supporting iBeacon based on BT radio include: AP520(BT)v1.x, AP520 v1.x, AP4220, MA1220, AM5528 (EP)

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 in AP configuration mode.
- The configuration takes effect on only the APs supporting Bluetooth.

Command	**ibeacon uuid** *uuid* **major** *major* **minor** *minor* **radio** *radio-id*
Parameter Description	*uuid*: Indicates the **UUID** that is a string of 32 hexadecimal characters. *major*: Indicates the **Major** value that is a string of four hexadecimal characters. *minor*: Indicates the **Minor** value that is a string of four hexadecimal characters. *radio-id*: Indicates the radio value that is an integer ranging from 1 to 255. The number of supported radios varies with products.
Defaults	iBeacon is not configured.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	Use this command to configure iBeacon based on BT radio. The configuration takes effect on only the APs supporting Bluetooth. The iBeacon function cannot be configured on all APs.

Verification

- Run the **show ap-config running** *ap-name* command on an AC to check whether the configuration is successful.

Configuration Example

Configuring iBeacon Based on BT Radio

Configuration Steps	● Configure iBeacon based on BT radio on the specified AP.

	`Hostname# configure terminal`
	`Hostname(config)#ap-config ap520(bt)`
	`Hostname(config-ap)# ibeacon uuid FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154 radio 13`

Verification	After configuring iBeacon based on BT radio, you can run the **show ap-config running** *ap-name* command on an AC to check the configuration.

	`AC:`
	`Hostname(config)#show ap-config running ap520(bt)`
	`!`
	`ap-config ap520(bt)`
	`...`
	`...`
	`ibeacon uuid  FDA50693A4E24FB1AFCFC6EB07647825 major 2714 minor 3154 radio 13`
	`...`
	`!`

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show ap-config running *ap-name*	Displays the AP configuration on the AC.

Debugging

N/A

Configuring STA Management

1. Configuring WLAN WBS-FWD
2. Configuring STA Management
3. Configuring VIP-FIRST
4. Configuring Hotspot 2.0
5. Configuring STA Identification
6. Configuring STA Connectivity Test

1 Configuring WLAN WBS-FWD

1.1 Overview

WLAN Basic Service-Forwarding Mode (WBS-FWD) is used to control the forwarding modes of packets on access points (APs). An Access controller (AC) communicate with an AP through the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel. The AP forwards data packets in one of the following modes:

- Centralized forwarding mode: An AP encapsulates user data packets into 802.3 frames and sends them over a CAPWAP tunnel to an AC. The AC then forwards these packets to an upper-layer networks. When the AC receives the data packets, it sends the packets over the CAPWAP tunnel to the AP. Then the AP converts the packets into 802.11 frames and sends them to STAs.
- Local forwarding mode: An AP encapsulates user data packets into 802.3 frames and implements Layer 2 or Layer 3 forwarding. That is, the AP forwards the packets to an upper-layer network without transmitting them over a CAPWAP tunnel.
- Local authentication forwarding mode: An AP forwards user data packets locally and wireless users are authenticated on the AP.
- VLAN priority: In metro scenarios, the VLAN priority feature is enabled on specified APs. After configuring the priority VLAN, when the packets of the VLAN pass, the VLAN priority feature is activated, that is, only the packets with the configured priority VLAN ID can pass, and the packets with non-priority VLAN are discarded, and a multicast packet is sent in the priority VLAN. The multicast address of the multicast packet can be configured.

You can configure the forwarding mode for all APs on the wireless local area network (WLAN), or you can specify the forwarding mode for a specified virtual local area network (VLAN), IP address, or a packet of a certain type. You can configure the AP forwarding mode based on diverse requirements such as the AP load and centralized management in various scenarios so that packets of different types are forwarded as required.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Centralized Forwarding Mode	All branch APs are managed by an AC and all packets are forwarded by the AC.
Local Forwarding Mode	All branch APs are managed by an AC and the packets are forwarded by the AP locally.
VLAN Priority	An AP allocates different VLANs to customers of different priorities. When one AP-S3 is faulty, high-priority users automatically connect to the other AP-S3. In this case, to ensure the bandwidth of high-priority user, the common user network of the AP needs to be disabled, that is, only the packets of the priority VLANs can pass through the AP. When there is no packet of this priority VLAN passing

	through for more than 60s, the packets of normal VLANs are allowed to pass through.

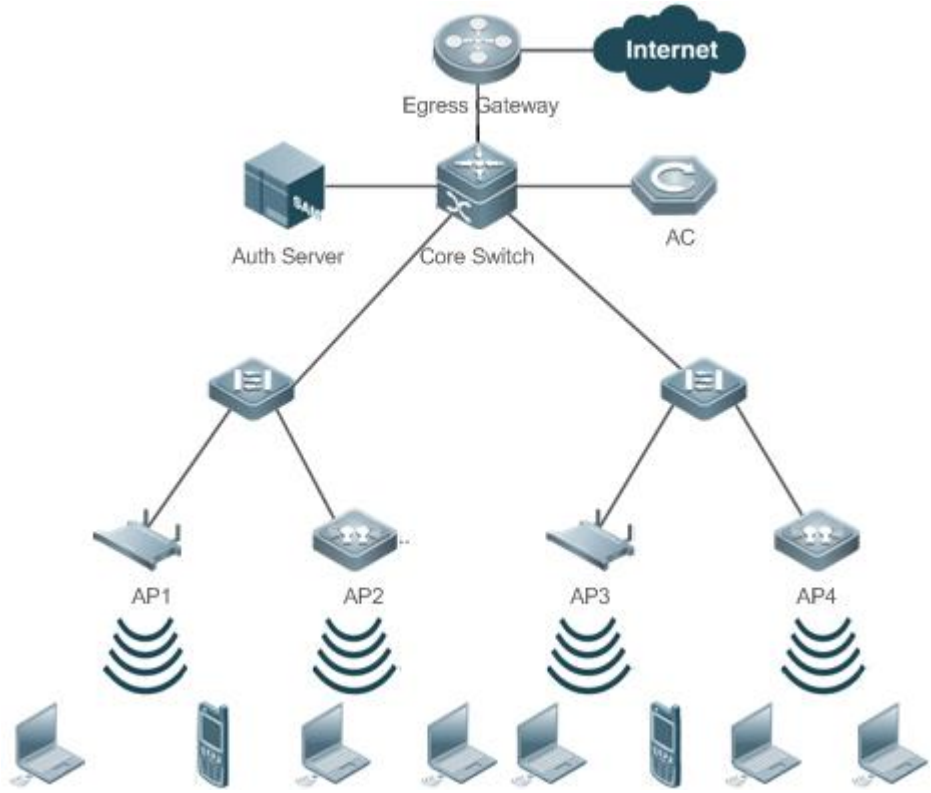
1.2.1 Centralized Forwarding Mode

Scenario

Centralized forwarding mode is applicable to the following scenarios:

- All APs and the AC are on the same LAN with sufficient bandwidth.
- The AC has high forwarding performance.
- The network egress is unified.

Figure 1-1



Deployment

On the AC, configure centralized forwarding mode for APs.

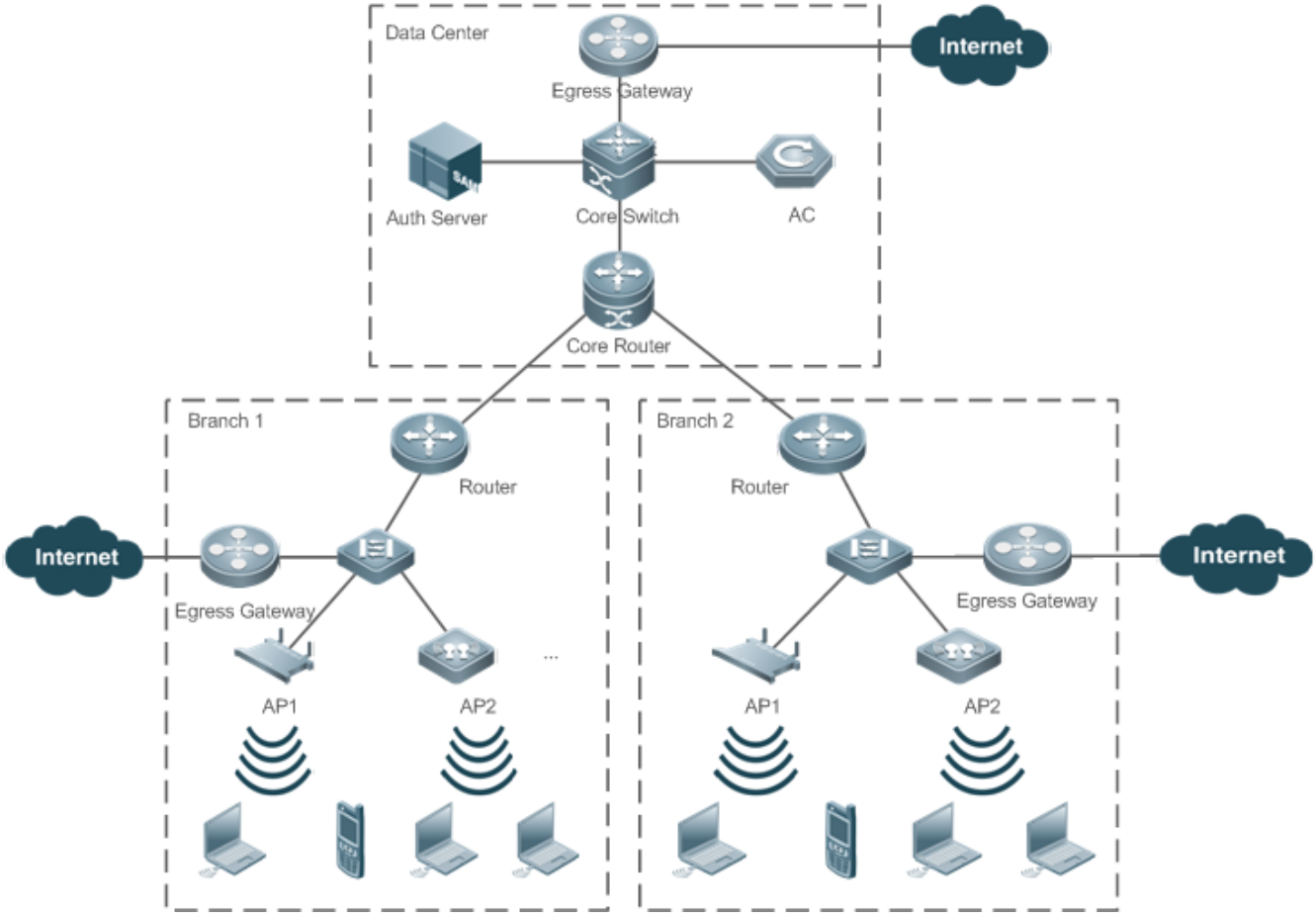
1.2.2 Local Forwarding Mode

Scenario

Local forwarding mode is applicable to the following scenarios:

- APs are deployed in different branches and are managed by the AC in the headquarters.
- The bandwidth of the links between branches and the headquarter is low.
- Each branch has an independent egress.

Figure 1-2



Deployment

- On the AC, configure local forwarding mode for APs.
- On the AC, configure centralized forwarding mode for Dynamic Host Configuration Protocol (DHCP).

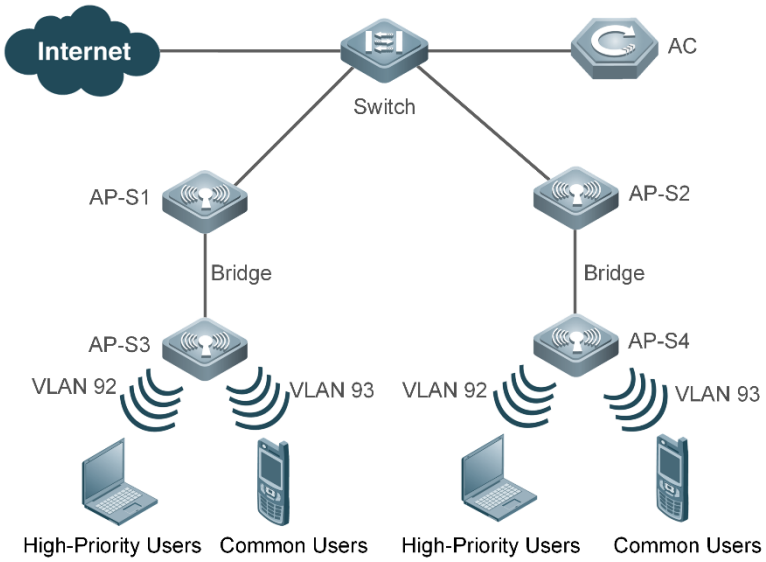
1.2.3 VLAN Priority

Scenario

VLAN priority is applicable to the following scenarios:

An AP allocates different VLANs to users of different priorities. When one AP-S3 is faulty, high- priority users automatically connect to the other AP-S3. In this case, the network is disabled for common users on the AP to ensure the bandwidth of high-priority users. That is, only the packets of high-priority VLANs can be forwarded through the AP. When no packets of high-priority VLANs are forwarded for more than 60s, the packets of normal VLANs are allowed to be forwarded.

Figure 1-3



Deployment

Configure it on the AC: Enable the VLAN priority feature on specified APs.

1.3 Features

Basic Concepts

Centralized Forwarding Mode and Local Forwarding Mode

An AP communicates with an AC through the CAPWAP tunnel. The AP forwards data packets in one of the following modes:

- Centralized forwarding mode: An AP encapsulates user data packets into 802.3 frames and sends them over a CAPWAP tunnel to an AC. The AC then forwards these packets to an upper-layer networks. When the AC receives the data packets, it sends the packets over the CAPWAP tunnel to the AP. Then the AP converts the packets into 802.11 frames and sends them to STAs. In this case, packets are forwarded by an AC, facilitating centralized management and maintenance while increasing the load on the AC. Moreover, the AC need to provide high performance in centralized forwarding mode.
- Local forwarding mode: An AP encapsulates user data packets into 802.3 frames and implements Layer 2 or Layer 3 forwarding. That is, the AP forwards the packets to an upper-layer network without transmitting them over a CAPWAP tunnel, which reduces the load on the AC. However, centralized control, management, and maintenance cannot be achieved in this mode.
- Comparison of two forwarding modes:

Forwarding Mode	Advantage	Disadvantage	Scenario
Centralized forwarding mode	Centralized control, management, and maintenance on an AC; flexible scalability	High requirement for AC performance	High-performance AC, high bandwidth of links between APs and AC, a few APs managed by an AC, and service flexibility

Local forwarding mode	Low requirement for AC performance	No centralized control and maintenance	Low- performance AC, low bandwidth of links between APs and AC, and many APs managed by an AC

Overview

Feature	Description
Configuring the Forwarding Mode of an AP	Specifies the forwarding mode of different packets on an AP.
Configuring the Forwarding Mode of an AC	Specifies the forwarding mode of different packets on an AC.
Configuring Configuring VLAN Priority	Configures the VLAN priority for the specified AP.
Configuring WLAN Forwarding Acceleration	Enables WLAN forwarding acceleration for the specified AP.

1.3.1 Configuring the Forwarding Mode of an AP

You can configure the AP forwarding mode based on diverse requirements such as the AP load and centralized management in various scenarios so that packets of different types are forwarded as required.

Working Principle

Forwarding Mode

Two forwarding modes are available: centralized forwarding and local forwarding. When an AP receives a wireless packet, it forwards the packet based on the configured mode.

You can configure the packet forwarding mode for an AP on an AC.

Forwarding Mode Settings

Products support the following forwarding modes:

- WLAN-based forwarding mode: Forwards the packets on all APs based on the forwarding mode (centralized forwarding mode or local forwarding mode) specified for the WLAN.
- Forwarding mode based on AP group and WLAN: Specifies a forwarding mode for a WLAN of a specific AP group for forwarding and access authentication. The AC delivers the configuration to the AP for storage. Based on the WLAN associated with the STA, the AP determines whether STA access authentication is implemented on the AP or AC and whether data packets is forwarded locally or centrally.
- VLAN-based forwarding mode: Forwards the packets on a specified VLAN of a WLAN based on the forwarding mode (centralized forwarding mode or local forwarding mode) specified for the VLAN.
- IP-based forwarding mode: Forwards the packets of a specified destination IP address in local forwarding mode.

- DHCP-based centralized forwarding mode: Forwards all DHCP packets in centralized forwarding mode. If this mode is configured, all DHCP packets will be sent in centralized forwarding mode.

Priorities of Different Forwarding Modes

Products support the preceding five forwarding modes. These modes can be configured at the same time and their priorities are ranked as follows (in descending order):

1. DHCP-based centralized forwarding mode
2. IP-based forwarding mode
3. VLAN-based forwarding mode
4. Forwarding mode based on AP group and WLAN
5. WLAN-based forwarding mode

After a wireless packet is received by an AP, the packet will be forwarded based on the priority of the forwarding mode. If a high-priority mode is detected, the packet will be forwarded in this mode; if not, the packet will be forwarded in the default centralized forwarding mode. The forwarding mode setting based on the AP group and WLAN is ultimately reflected on the AP as the WLAN-based forwarding mode configuration.

For example:

1. If DHCP-based centralized forwarding mode is configured, all the DHCP packets will be forwarded in centralized mode.
2. For a non-DHCP packet, if its IP address is specified for local forwarding, the packet will be forwarded in local forwarding mode. If not, Step 3 will be performed.
3. If the VLAN where the packet belongs is configured with a forwarding mode, the packet will be forwarded in this mode. If not, Step 4 will be performed.
4. If the WLAN where the packet belongs is configured with a forwarding mode, the packet will be forwarded in this mode. If not, Step 5 will be performed.
5. The packet will be forwarded in the default centralized forwarding mode.

1.3.2 Configuring the Forwarding Mode of an AC

You can configure the forwarding mode for an AC based on the load of the entire wireless network, unified management requirement, and the actual service environment. The AC adjusts internal parameters to better adapt to the current service environment based on the configured forwarding mode,.

Working Principle

Forwarding Mode

Hybrid forwarding mode and local forwarding mode are available. When hybrid forwarding mode is configured for ACs, WLANs support both centralized forwarding and local forwarding. That is, some WLANs use centralized forwarding while other WLANs use local forwarding. When local forwarding mode is configured for ACs, WLANs support only local forwarding mode (including local authentication forwarding mode).

Forwarding Mode Settings

You can configure the forwarding mode for an AC.

1.3.3 Configuring VLAN Priority

You can configure the VLAN priority for specified APs as required.

Working Principle

Configuring the VLAN Priority

Configure the VLAN priority. When packets with the specified VLAN priority pass through, the feature takes effect, and subsequent packets with the same VLAN priority are allowed to pass through, while packets with other VLANs are directly discarded. The timer is enabled to detect packet timestamps. If no packets with the specified VLAN priority come in within 60 seconds, packets with other VLANs are allowed to pass through. By default, there is no specified VLAN priority, and packets from all VLANs are allowed to pass through.

Configuring the Multicast Address

After the VLAN priority configuration takes effect, a multicast packet will be sent once on the priority VLAN and the multicast address can be configured.

1.3.4 Configuring WLAN Forwarding Acceleration

You can configure WLAN forwarding acceleration as needed.

Working Principle

Forwarding Acceleration Mode

Forwarding acceleration differs from normal forwarding. Configuring forwarding acceleration will improve the overall forwarding performance of the AP, but may cause certain features to become unavailable (see the supported AP models and unsupported features below). The device supports the following forwarding acceleration mode:

Software: Software-based forwarding acceleration mode. Wireless data packets are not processed by the wireless driver, but are directly forwarded through the wired driver. Because the packet transmission path of the wired driver is much shorter than that of the wireless driver, this mode can improve the forwarding performance of wireless data packets.

After this function is configured, the support for some features of the device will change.

Series	Model	tware-based Forwarding	Hardware-based Forwarding
AP180 series	AP180-I AP180P-L	Supported Features not supported: 1. WIDS 2. Wireless location 3. WAPI 4. Dynamic EDCA 5. WIS	Not supported
AP680 series	AP680-O(P) M7000L-AP842O-RU		Not supported
AP810 series	AP810-L SAP815-SP		Not supported

Series	Model	tware-based Forwarding	Hardware-based Forwarding
AP820 series	AP820-L(V3) TS-MWI3000CPRO AP820-A(V3) M7000L-AP842I-RU TS-MWI3000C SAP825-SP AP800	6. TXSEQ and RXSEQ is not displayed in the **show dot11 associations all-client** command output. 7. In the **show int counter** and **show int counters summary** command outputs, the number of sent/received multicast packets, the number of sent/received broadcast packets, and the numbers of different bytes are displayed as 0.	Not supported Not supported
SOE i-Share+	MAP852-SF-S	8. Two MIB objects of RRM are affected: ruijieRrmAPIfStationRSSICoverageInfoTable_oid[] = { 1, 3, 6, 1, 4, 1, 4881, 1, 1, 10, 2, 63, 1, 4, 9, 1} ruijieRrmAPIfStationSNRCoverageInfoTable_oid[] = { 1, 3, 6, 1, 4, 1, 4881, 1, 1, 10, 2, 63, 1, 4, 10, 1} 9. xspeed, hutong, and some radio-specific MIB information 10. WDS	Not supported

1.4 Configuration

Configuration	Description and Command	
Configuring WLAN-based Forwarding Mode	⚠ (Mandatory) It is used to specify the forwarding mode for a WLAN.	
	tunnel	Specifies the forwarding mode for an AP on a WLAN.
Configuring Forwarding Mode Based on AP Group and WLAN	⚠ (Optional) It is used to set the forwarding mode for a specific WLAN of an AP group.	
	tunnel local-auth wlan	Sets the forwarding mode for a specific WLAN of an AP group to local authentication forwarding mode.
Configuring VLAN-based Forwarding Mode	⚠ (Optional) It is used to specify the forwarding mode for a specified VLAN of a WLAN.	
	tunnel local wlan	Specifies local forwarding as the forwarding mode for a specified VLAN of a WLAN.
	tunnel 8023 wlan	Specifies centralized forwarding as the forwarding mode for a specified VLAN of a WLAN.
Configuring IP-based Forwarding Mode	⚠ (Optional) It is used to specify local forwarding as the forwarding mode for a specified IP address.	
	local fw ip	Forwards all packets of a specified IP address in local forwarding mode.
	⚠ (Optional) It is used to specify centralized forwarding as the forwarding mode for DHCP packets.	

Configuration	Description and Command	
Configuring DHCP-based Centralized Forwarding Mode	**central dhcp enable**	Forwards all DHCP packets on a WLAN in centralized forwarding mode.
Configuring AC-based Forwarding Mode	(Optional) It is used to specify the forwarding mode for an AC.	
	tunnel-mode	Specifies the forwarding mode for an AC.
Configuring VLAN Priority	(Optional) It is used to configure VLAN priority for a specific AP.	
	vlan-first	Configures VLAN priority for a specified AP.
Configuring WLAN Forwarding Acceleration	(Optional) It is used to configure WLAN forwarding acceleration.	
	wlan forward acceleration software	Configures software-based forwarding acceleration for the AP.

1.4.1 Configuring WLAN-based Forwarding Mode

Configuration Effect

- Specify a forwarding mode for APs on a WLAN, including local forwarding mode, centralized forwarding mode, and local authentication forwarding mode.

Notes

- The **tunnel local-auth** command takes effect only when remote intelligent perception technology (RIPT) is enabled.

Configuration Steps

- Mandatory.
- In WLAN configuration mode on an AC, configure the forwarding mode for all APs on the WLAN as local forwarding mode, centralized forwarding mode, or local authentication forwarding mode.
- The default forwarding mode is centralized forwarding.
- Configure the forwarding mode before applying the WLAN template to a specified AP group. Otherwise, the configuration will not take effect.

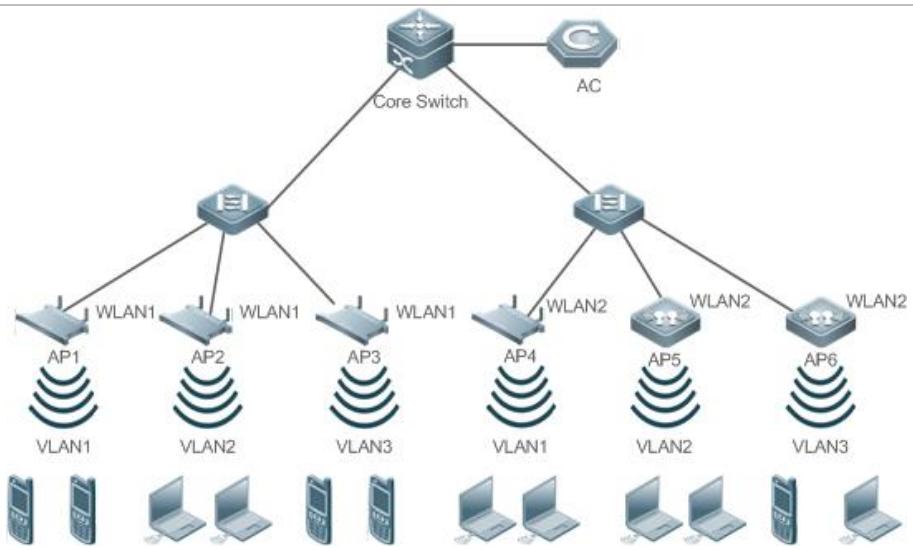
Command	**tunnel** { **8023** | **local** }
Parameter Description	**8023**: An AP encapsulates received data packets into 802.3 frames and forwards the packets to an AC. **local**: An AP forwards packets locally.
Defaults	Centralized forwarding mode
Command Mode	WLAN configuration mode
Usage Guide	-

Verification

- Verify the WLAN configuration.

Configuration Example

Configuring the Forwarding Mode for All APs on a WLAN

Scenario **Figure 1-4**	 ● AP 1, AP 2, and AP 3 on WLAN 1 are used for mobile device connections. Centralized forwarding mode is configured due to lower traffic volume. ● AP 4, AP 5, and AP 6 on WLAN 2 are used for office PC connections. Local forwarding mode is configured due to higher traffic volume.
Configuration Steps	● Enter WLAN configuration mode. ● Configure the forwarding mode for a WLAN.
WLAN1	`Hostname(config)#wlan-config 1` `Hostname(config-wlan)#tunnel local`
WLAN2	`Hostname(config)#wlan-config 2` `Hostname(config-wlan)#tunnel 8023`
Verification	N/A

1.4.2 Forwarding Mode Based on AP Group and WLAN

Configuration Effect

- The forwarding mode for a specific WLAN of an AP group is set to local authentication forwarding mode.

Notes

- In local authentication forwarding mode, an AP forwards the received data packets locally and STAs are authenticated for access on the AP.
- Local authentication forwarding mode can be configured on WLANs that support OPEN/PSK authentication. However, this mode is unavailable on WLANs that support 802.1X authentication, web-based authentication, and other authentication methods. If this mode is applied to WLANs that adopt 802.1X or web-based authentication, access authentication errors may occur on STAs.

- If the WLAN does not exist or is not mapped to the AP group, the configuration will be saved but not take effect. After the WLAN is added or is mapped to the AP group, the configuration automatically takes effect.

Configuration Steps

Configuring the Forwarding Mode Based on AP Group and WLAN

- Optional. If a WLAN requires a forwarding mode that differs from the overall WLAN configuration in a specific AP group, you can set it to the forwarding mode based on AP group and WLAN.
- If it is not configured, data packets are forwarded in the WLAN-based forwarding mode.
- In the AP group configuration mode on the AC, run the **tunnel local-auth wlan** *wlan-id* command to specify the local authentication forwarding mode for a specific WLAN of an AP group.

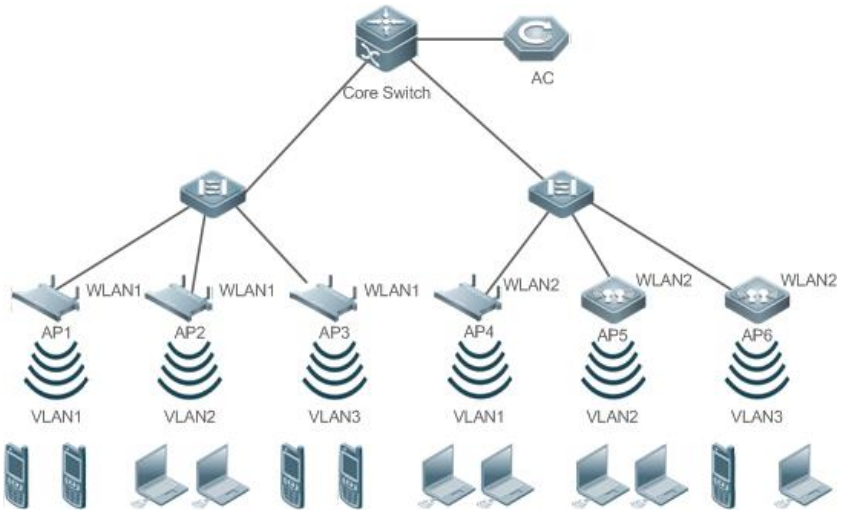
Command	**tunnel local-auth wlan** *wlan-id*
Parameter Description	*wlan-id*: Indicates the ID of the WLAN where local authentication forwarding mode is configured. The WLAN must be created first. The value ranges from 1 to 2,048.
Defaults	N/A
Command Mode	AP group configuration mode
Usage Guide	1. In local authentication forwarding mode, the AP forwards the received data packets locally and STAs are authenticated for access on the AP. 2. After the WLAN forwarding mode is configured through the **tunnel local-auth wlan** command, only OPEN/PSK authentication are supported for STA access. If 802.1X, web-based, or other authentication methods are used, access authentication errors may occur on STAs. 3. If the WLAN does not exist or is not mapped to the AP group, the configuration will be saved but not take effect. After the WLAN is added or is mapped to the AP group, the configuration automatically takes effect.

Verification

- N/A

Configuration Example

Configuring the Local Authentication Forwarding Mode for a WLAN of an AP Group

Scenario **Figure 1-5**	 ● AP1, AP2, and AP3 are on WLAN 1, where AP 1 belongs to APG1 group, AP2 belongs to APG2 group, and AP3 belongs to APG3 group. There is an unstable middle link between AP1 and the AC. Therefore, local authentication forwarding mode needs to be applied to APG1 group, and local forwarding mode to APG2 and APG3 groups.
Configuration Steps	● Enter WLAN configuration mode. ● Configure the forwarding mode for a WLAN. ● Specify the forwarding mode for a WLAN of an AP group.

WLAN1	`Hostname(config)#wlan-config 1`
	`Hostname(config-wlan)#tunnel local`
	`Hostname(config-wlan)#exit`
	`Hostname(config)#ap-group APG1`
	`Hostname(config-ap-group)#tunnel local-auth wlan 1`

1.4.3 Configuring VLAN-based Forwarding Mode

Configuration Effect

- Configure the forwarding mode for a specified VLAN on a WLAN: local or centralized forwarding.

Notes

- You can configure the forwarding mode for the entire WLAN as WLAN-based forwarding mode, or you can set the forwarding mode for a specified VLAN on the WLAN to VLAN-based forwarding mode.
- As VLAN-based forwarding mode prevails over WLAN-based forwarding mode, if both of these modes are configured, the packets on the specified VLAN will be forwarded in VLAN-based forwarding mode and the others will be forwarded in WLAN-based forwarding mode.
- Configure either local forwarding or centralized forwarding for a VLAN.
- The VLAN can be a port-based VLAN, MAC-based VLAN, or authentication-based VLAN.

Configuration Steps

Configuring the Forwarding Mode for a VLAN

- (Optional) If a specified VLAN on a WLAN requires a different forwarding mode from that of the other VLANs, specify a forwarding mode for this VLAN.
- The default is WLAN-based forwarding mode.
- In AP group configuration mode on an AC, run **tunnel local wlan** *wlan-id* **vlan** *vlan-id* to specify local forwarding mode for a specified VLAN.
- In AP group configuration mode on an AC, run **tunnel 8023 wlan** *wlan-id* **vlan** *vlan-id* to specify centralized forwarding mode for a specified VLAN.

Command	**tunnel local wlan** *wlan-id* **vlan** *vlan-id*
Parameter Description	*wlan-id*: Indicates the WLAN ID. The WLAN must be created first. The value ranges from 1 to 2,048. *vlan-id*: Indicates the VLAN ID. The VLAN must be created first. The value ranges from 1 to 4,094.
Defaults	Local forwarding mode is not configured for a specified VLAN. The forwarding mode is the same as that configured by the **tunnel** command.
Command Mode	AP group configuration mode
Usage Guide	11. In WLAN configuration mode, you can run the **tunnel 8023** command to specify centralized forwarding mode for the entire WLAN, or you can run **tunnel local wlan** to specify local forwarding mode for a specified VLAN on the WLAN. 12. After the WLAN forwarding mode is configured through the **tunnel local wlan** command, only OPEN/PSK authentication is supported for STA access. If 802.1X, web-based, or other authentication methods are used, access authentication errors may occur on STAs.

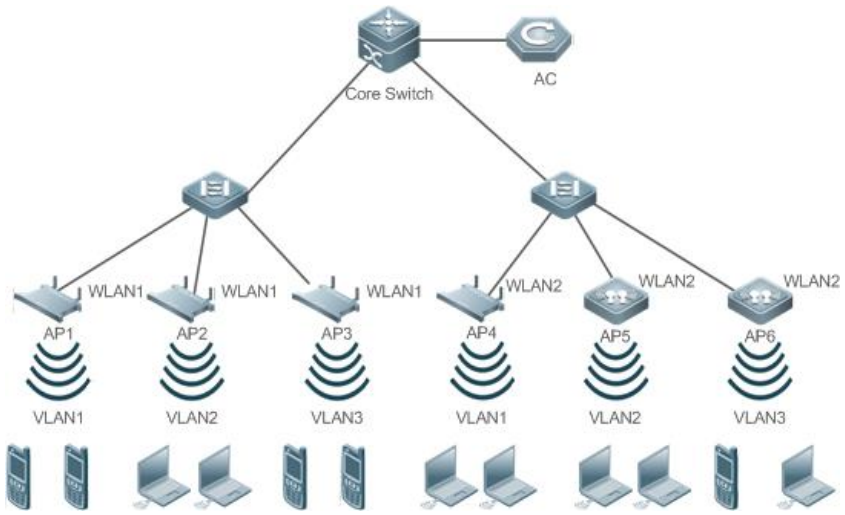
Command	**tunnel 8023 wlan** *wlan-id* **vlan** *vlan-id*
Parameter Description	*wlan-id*: Indicates the ID of the WLAN where centralized forwarding mode is configured. The WLAN must be created first. The value ranges from 1 to 2,048. *vlan-id*: Indicates the ID of the VLAN where centralized forwarding mode is configured. The WLAN must be created first. The value ranges from 1 to 4,094.
Defaults	Centralized forwarding mode is not configured for a specified VLAN. The forwarding mode is the same as that configured by the tunnel command.
Command Mode	AP group configuration mode
Usage Guide	1. In WLAN configuration mode, you can run the **tunnel local** command to specify local forwarding mode for the entire WLAN, or you can run the **tunnel 8023 wlan** command to specify centralized forwarding mode for a specified VLAN. 2. After the WLAN forwarding mode is configured through the **tunnel 8023 wlan** command, only OPEN/PSK authentication is supported for STA access. If 802.1X, web-based, or other authentication methods are used, access authentication errors may occur on STAs.

Verification

- N/A

Configuration Example

Configuring the Forwarding Mode for a Specified VLAN on a WLAN

Scenario **Figure 1-6**	 ● AP1, AP2 and AP3 on WLAN1 belong to VLAN1, VLAN2 and VLAN3 respectively. VLAN1 and VLAN 3 are used for the access of mobile phones while VLAN 2 for PCs which require high bandwidth. Therefore, VLAN2 is configured with local forwarding mode. ● AP4, AP5 and AP6 on WLAN2 belong to VLAN 1, VLAN 2 and VLAN 3 respectively. VLAN1 and VLAN 2 are used for the access of PCs while VLAN 3 for mobile phones which require low bandwidth. Therefore, VLAN 3 is configured with centralized forwarding mode.
Configuration Steps	● Enter WLAN configuration mode. ● Configure the forwarding mode of a WLAN. ● Specify a forwarding mode for the specified VLAN on the WLAN.

WLAN1	`Hostname(config)#wlan-config 1`
	`Hostname(config-wlan)#tunnel 8023`
	`Hostname(config-wlan)#exit`
	`Hostname(config)#ap-group default`
	`Hostname(config-ap-group)#tunnel local wlan 1 vlan 2`

WLAN2	`Hostname(config)#wlan-config 2`
	`Hostname(config-wlan)#tunnel local`
	`Hostname(config-wlan)#exit`
	`Hostname(config)#ap-group default`
	`Hostname(config-ap-group)#tunnel 8023 wlan 2 vlan 3`

Verification	N/A

1.4.4 Configuring IP-based Forwarding Mode

Configuration Effect

- Configure local forwarding mode for packets of a specified IP address.

Notes

- You can set the forwarding mode of an AP to WLAN-based forwarding mode and VLAN-based forwarding mode, or you can further configure local forwarding mode for packets of a specified IP address.
- As IP-based forwarding mode prevails over WLAN-based forwarding mode and VLAN-based forwarding mode, if all of these modes are configured, packets of a specified address will be forwarded locally, and the others will be forwarded in WLAN-based forwarding mode or VLAN-based forwarding mode.

Configuration Steps

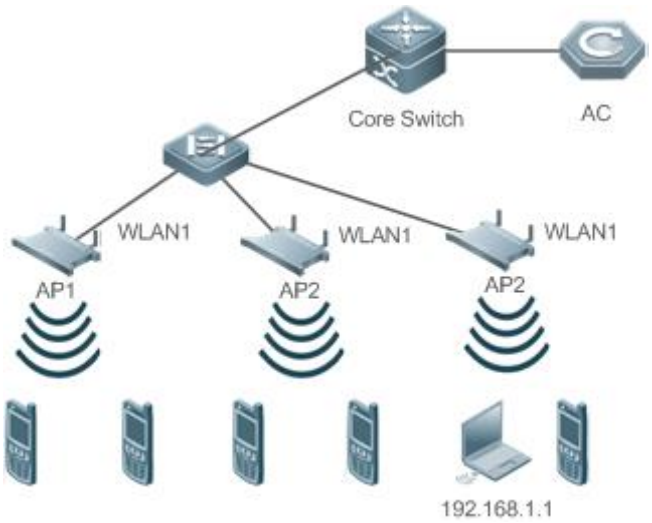
Configuring IP-based Forwarding Mode

- (Optional) You can configure local forwarding mode for packets of a specified IP address.
- In AC configuration mode on an AC, configure local forwarding mode for a specified IP address.
- If IP-based forwarding is not configured, packets are forwarded based on WLAN or VLAN. If IP-based forwarding is configured, packets of a specified IP address are forwarded locally.

Command	**local fw ip** [*ip address*]
Parameter Description	*ip address*: Indicates the IP address of a STA.
Defaults	All IP packets are forwarded in WLAN-based forwarding mode.
Command Mode	AC configuration mode
Usage Guide	The AC can automatically identify data packets based on access conditions and determine whether to use local or centralized forwarding. Currently, the AC selects the forwarding mode based on the IP addresses of an STA.

Configuration Example

Configuring Local Forwarding for Packets of a Specified IP Address

Scenario **Figure 1-7**	 - AP1, AP2 and AP3 on WLAN1 are typically used for the access of mobile phones which require low bandwidth. Therefore, centralized forwarding mode is configured. When a PC with

	an IP address **192.168.1.1** is connected to AP2 and the PC requires high bandwidth, local forwarding is configured for **192.168.1.1**.
Configuration Steps	● Enter AC configuration mode. ● Configure local forwarding mode for a specified IP address.
AC	`Hostname(config)#ac-controller` `Hostname(config-ac)#local fwip 192.168.1.1`
Verification	N/A

1.4.5 Configuring DHCP-based Centralized Forwarding Mode

Configuration Effect

- Configure centralized forwarding mode for all DHCP packets.

Notes

- DHCP-based centralized forwarding mode prevails over WLAN-based forwarding mode, VLAN-based forwarding mode, and IP-based forwarding mode. If DHCP-based centralized forwarding mode is configured, all DHCP packets on a specified WLAN will be forwarded in centralized mode.
- To facilitate management of the DHCP address pool and simplify the DHCP topology, you are advised to enable this function.

Configuration Steps

↘ Configuring DHCP-based Centralized Forwarding Mode

- (Optional) Perform the configuration when the AC assigns IP addresses to STAs uniformly.
- If DHCP centralized forwarding mode is not configured, DHCP packets will be forwarded in the same mode as other packets. If DHCP centralized forwarding mode is configured, all DHCP packets will be forwarded in centralized mode.
- Configure the forwarding mode before applying the WLAN template to a specified AP group. Otherwise, the configuration will not take effect.

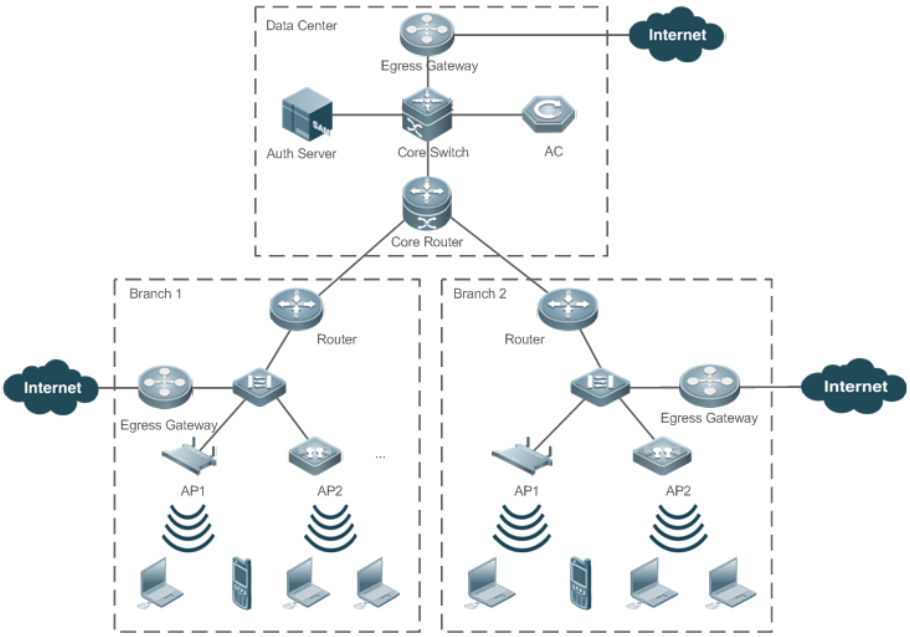
Command	**central dhcp enable**
Parameter Description	N/A
Defaults	All packets are forwarded in WLAN-based forwarding mode.
Command Mode	WLAN configuration mode
Usage Guide	To facilitate management of the DHCP address pool and simplify the DHCP topology, you are advised to enable this function.

Verification

- Verify the WLAN configuration.

Configuration Example

↘ Configuring DHCP Services on an AC

Scenario **Figure 1-8**	 ● APs are deployed in different branches and are managed by the AC in the headquarters. ● The bandwidth of the links between branches and the headquarters is low. ● Each branch has an independent egress. ● IP addresses are assigned by the AC.
Configuration Steps	● Enter WLAN configuration mode. ● Configure the forwarding mode of the WLAN. ● Configure DHCP-based centralized forwarding mode.

AC	`Hostname(config)#wlan-config 100 Hostname_wlan`
	`Hostname(config-wlan)#tunnel local`
	`Hostname(config-wlan)#central dhcp enable`

Verification	N/A

1.4.6 Configuring AC-based Forwarding Mode

Configuration Effect

- Hybrid forwarding mode and local forwarding mode are available. When hybrid forwarding mode is configured for ACs, WLANs support both centralized forwarding and local forwarding. That is, some WLANs use centralized forwarding while other WLANs use local forwarding. When local forwarding mode is configured for ACs, WLANs support only local forwarding mode (including local authentication forwarding mode).

Configuration Steps

- Optional.
- In AC configuration mode on an AC, set the forwarding mode of the AC to hybrid forwarding or local forwarding.
- If no forwarding mode is configured for an AC, the AC uses the hybrid forwarding mode by default.
- Save the configuration and restart the device after configuration. Otherwise, the configuration does not take effect.

Command	**tunnel-mode** { **hybrid** | **local** }

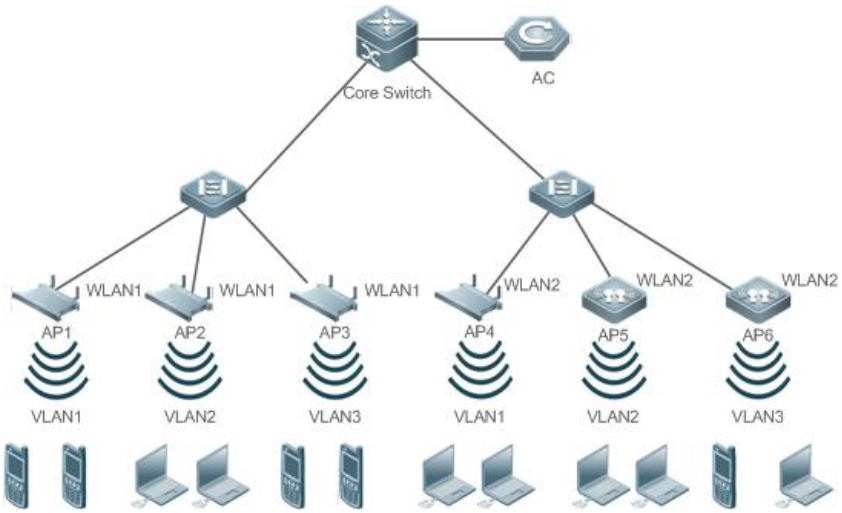
Parameter Description	**hybrid**: Indicates hybrid forwarding mode. In this mode, WLANs support both centralized forwarding mode and local forwarding mode, that is, some WLANs use centralized forwarding while some WLANs adopt local forwarding. **local**: Indicates local forwarding mode. In this mode, WLANs support only local forwarding mode (including local authentication forwarding mode).
Defaults	Hybrid forwarding mode.
Command Mode	AC configuration mode
Usage Guide	1. The AC forwarding mode switching takes effect only after the configuration is saved and the device is restarted. Mode switching does not trigger device restart and you need to manually restart the device. 2. If the AC is restarted after the forwarding mode configuration is added to or modified in the **config.text** file, the configuration takes effect only after the AC is restarted again. It is invalid to delete the AC forwarding mode configuration from the **config.text** file. 3. The AC forwarding mode configuration is preconfigured in the system. That is, the configuration takes effect after the AC is restarted even if the **write** command is not executed. 4. If the tunnel mode is set to **hybrid** for an AC, the AC is explicitly configured to adopt the hybrid forwarding mode. After configuration, the tunnel mode remains unchanged when the default configuration is updated due to the AC version upgrade. 5. When an AC switches from hybrid forwarding mode to local forwarding mode, WLANs using centralized forwarding automatically switch to local forwarding mode after the AC is restarted. 6. When an AC switches from local forwarding mode to hybrid forwarding mode, the forwarding mode of WLANs does not change automatically after the AC is restarted. 7. In local forwarding mode, service configurations that need to be supported by centralized forwarding keep unchanged but their functions do not take effect. Such configurations include but are not limited to the broadcast forwarding proportion and token bucket configuration of the data plane, WQoS AC-based rate limit, WIDS AC-based/AC-SSID-based Layer 2 isolation, and application identification. 8. The maximum number of managed APs and STAs changes accordingly after the AC forwarding mode is changed. 9. The AC forwarding mode does not support default configuration restoration using the reset button.

Verification

- Check the AC configuration.
- Run the **show ac-config** command to display the current effective forwarding mode of the AC.

Configuration Example

Setting the Forwarding Mode of an AC to Local Forwarding

Scenario **Figure 1-9**	 ● The AC is deployed in bypass mode. All STA traffic does not need to pass through the AC. The AC is configured in local forwarding mode so as to manage more APs.
Configuration Steps	● Enter the AC configuration mode. ● Configure the forwarding mode for the AC, save the configuration, and restart the AC.

AC	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#tunnel-mode local`
	`Hostname(config-ac)#end`
	`Hostname#write`
	
	`Building configuration...`
	
	`[OK]`
	`Hostname#reload`
	`Reload system?(Y/N)y`

Verification	N/A

1.4.7 Configuring VLAN Priority

Configuration Effect

- Configure the VLAN priority feature for a specified AP to enable the priority VLAN and multicast address.

Notes

- N/A

Configuration Steps

↘ Enabling VLAN Priority

- Optional.
- This configuration can be performed if you need to enable the VLAN priority feature.
- Enable VLAN priority in AP configuration mode on the AC.

Command	**vlan-first global-enable**
Parameter Description	N/A
Defaults	Disabled
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the Priority VLAN

- Optional.
- You can configure priority VLAN for a specific AP.
- Configure the priority VLAN in AP configuration mode on the AC.

Command	**vlan-first vlan** *vian-id*
Parameter Description	*vian-id*: Specifies the priority VLAN. The value ranges from 1 to 4,094.
Defaults	All VLANs are non-priority VLANs.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the Multicast Address for the VLAN Priority Feature

- Optional.
- You can configure a multicast address for the VLAN priority feature of a specific AP.
- Configure the multicast address in AP configuration mode on the AC.

Command	**vlan-first ip** *sip dip*
Parameter Description	*sip*: Configures the source IP address of a multicast packet. *dip*: Configures the destination IP address of a multicast packet.
Defaults	No multicast address is configured.
Command Mode	AP configuration mode

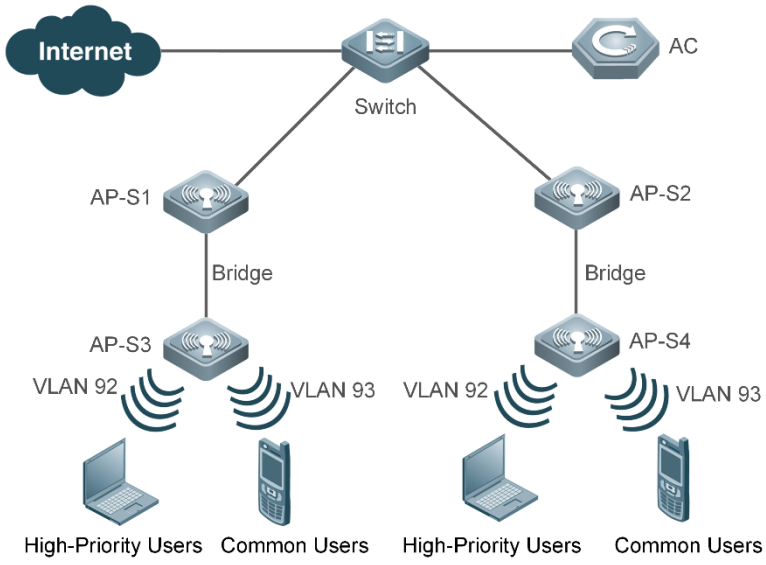
Usage Guide	N/A

Verification

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

Configuration Example

Configuring the Multicast Address for the VLAN Priority Feature

Scenario **Figure 1-10**	 **Note**: ● AP-S1 bridges with AP-S3, different VLANs are assigned to priority users and common users on AP-S3 and all APs are centrally managed by the AC. ● The multicast address for the VLAN priority feature on AP-S3 can be configured on the AC.
Configuration Steps	● Enter AP configuration mode on the AC. ● Configure the multicast address for the VLAN priority feature.
AC	`Hostname(config)#ap-config AP1` `Hostname(config-ap)# vlan-first ip 192.168.100.7 224.1.1.1`
Verification	Run the **show run** command to display the configuration.

1.4.8 Configuring WLAN Forwarding Acceleration

Configuration Effect

Configuring forwarding acceleration will improve the overall forwarding performance of the AP.

Notes

In the multi-user scenario where software-based forwarding acceleration is enabled, the recommended number of users is 32. If more than 32 users are configured, the performance will be lowered.

Configuration Steps

Configuring Software-based WLAN Forwarding Acceleration

Optional.

Command	**wlan forward acceleration software**
Parameter Description	N/A
Defaults	Software-based forwarding acceleration is disabled by default.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	• Configuring software-based forwarding acceleration will cause functions such as WIDS, dynamic EDCA, WIS, and wireless location to become unavailable. For details, see Configuring WLAN Forwarding Acceleration. • After software-based forwarding acceleration is configured on the AP, restart the AP to make the function to take effect. That is, after this command is configured, a confirmation prompt will appear. You need to input y, after which the AP will automatically restart, and WLAN forwarding acceleration will be activated.

Verification

Run the **show running-config** or **show wlan forward acceleration** command to display the configuration.

Configuration Example

Configuring Software-based WLAN Forwarding Acceleration

Configuration Steps	• Enter the AP configuration mode on the AC. • Configure software-based forwarding acceleration.
AC	`Hostname(config)#ap-config AP1` `Hostname(config-ap)# wlan forward acceleration software`
Verification	Run the **show running-config** or **show wlan forward acceleration** command to display the configuration.

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show wlan-config cb *wlan-id*	Displays the WLAN configuration.
show ac-config	Displays the AC forwarding mode.
show running-config	Displays the VLAN priority configuration.
show wlan forward acceleration	Displays the WLAN forwarding acceleration configuration of the AC or AP.

1 Configuring STA Management

1.1 Overview

STA Management (STAMG) implements station (STA) management, including STA access control management and STA event notification. Event notification is mainly used to serve other function modules. Applications of the STAMG functions are as follows:

- The dynamic blocklist is used on a security-sensitive network to prevent user attacks.
- The STA limit is used when the number of STAs exceeds the AP capacity.
- Load balancing is used when STAs need to be evenly distributed to multiple APs.
- Association control is used in the e-bag scenario.

Protocols and Standards

- N/A

1.2 Applications

Application	Description
Fit AP Networking	In fit AP network mode, at least one AC and one AP are required.
Large Conference Room	In fit AP network mode, at least one AC and two APs are required.
E-	In fit AP network mode, at least one AC and two APs are required.

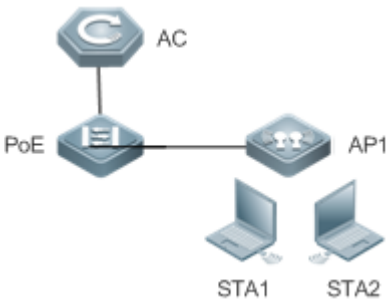
1.2.1 Fit AP Networking

Scenario

One AC is deployed on the wireless network, and dynamic blocklist and STA limit are enabled on the AC.

As shown in Figure 1-1, dynamic blocklist and STA limit are enabled on the AC.

Figure 1-1



Remarks	AC: Indicates a wireless access controller. PoE: Indicates the switch that functions as the gateway of APs. AP: Indicates a wireless access point.

	STA1 and STA2: Indicates two client devices.

Deployment

- Enable dynamic blocklist and STA limit on the AC.

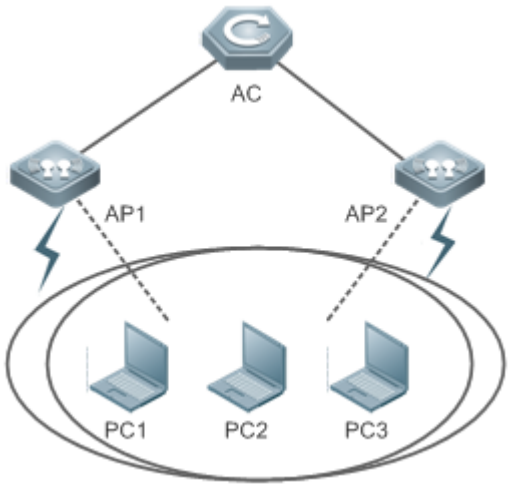
1.2.2 Large Conference Room

Scenario

In a large conference room, the number of STAs is generally large, and STAs must be evenly distributed to multiple APs. Otherwise, too many STAs are connected to some specific APs, resulting in a low network speed and a poor user experience.

As shown in Figure 1-2, two APs (AP1 and AP2) are deployed in the conference room so that STAs can be evenly distributed to the two APs.

Figure 1-2



Remarks	AC: Indicates a wireless access controller. AP1 and AP2: Indicates two wireless access points. PC1, PC2, and PC3: Indicates three STAs.

Deployment

- Enable load balancing on the AC, and add AP1 and AP2 to the load balancing group.

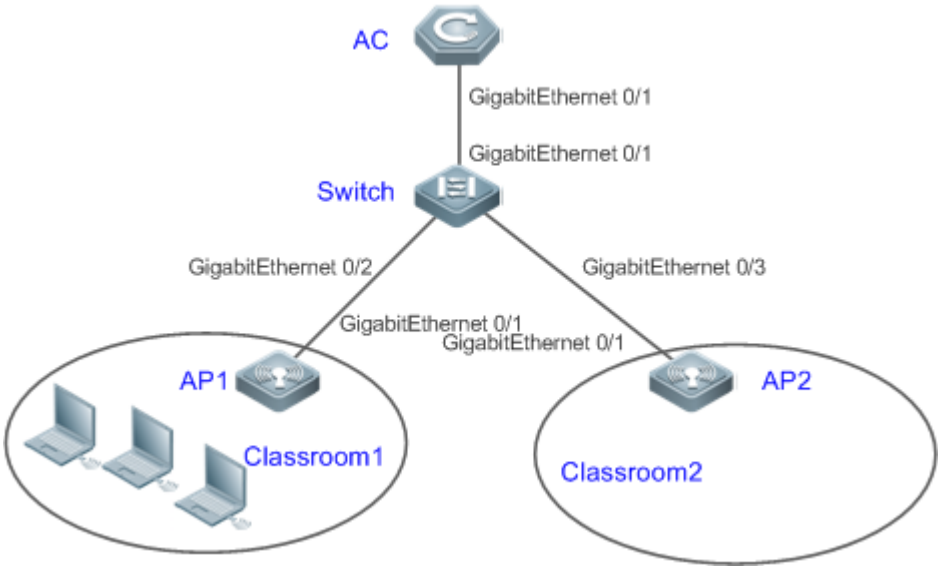
1.2.3 E-bag

Scenario

One AC is deployed on the wireless network, and multiple APs are deployed in different classrooms. When the teacher's STA is associated with an AP, the students' STAs must also be associated with the same AP. This ensures the network transmission speed.

As shown in Figure 1-3, AP1 is deployed in Classroom1 and AP2 is deployed in Classroom2. When the teacher's STA is associated with AP1, the students' STAs must also be associated with AP1, instead of AP2. In this way, traffic destined for Classroom1 is only sent to AP1 without affecting users on AP2.

Figure 1-3



Remarks	AC: Indicates a wireless access controller. PoE: Indicates the switch that functions as the gateway of APs. AP1 and AP2: Indicates two wireless access points.

In an e-bag scenario, if the teacher uses the wired network connection, one of STAs used by students must be configured as the primary STA to implement association control. Who uses this primary STA is determined by users. For example, the primary STA can be used by the class monitor or the teacher so that secondary STAs can be associated properly. After proper association of the secondary STAs, the teacher can put this primary STA aside, and use the wired network connection during the class.

Deployment

- Enable association control on the AC, and add APs to a specified association control zone.

1.3 Features

Overview

Feature	Description
Dynamic	Detects association of unauthorized users.
STA Limit	Limits the number of STAs.
Load Balancing	Distributes STAs evenly to multiple APs.
Inter-Radio Load Balancing (by Number of STAs/Traffic/Ratio)	Distributes STAs evenly to multiple radios of the same AP.

Inter-Radio Load Balancing (by Bandwidth Resources)	Compares the weights of radio frequency band resources, hides SSID signals with few radio resources, and balances the access STAs among the radios.
Association Control	Associates secondary STAs with APs in the same control domain if the primary STA is associated with these APs.
STA Management	Disassociates STAs without traffic forcibly to recycle resources.
STA Informational Syslog Suppression	Suppresses the informational syslog output rate of STAs.
Intelligent SSID Hiding	Hides the SSID when the number of STAs on an AP or radio reaches the upper limit.
STA Jitter Prevention	Retains the STA entry for a period of time after the STA is disassociated from the WLAN.
Syslog Format Upon STA Association	Adds the syslog format for obtaining an IP address when a STA goes online.
Fast STA Association	Indicates that during the STA association process, the AC does not wait for the response packet that the STA is successfully added from the AP, improving STA access efficiency.
IP Address Detection	Indicates that the STA will be disconnected and reacquire IP address if it fails to obtain an IP address.
DHCP Proxy	Indicates the DHCP proxy request feature.

1.3.1 Dynamic Blocklist

The AC can use the dynamic blocklist to punish malicious or unauthorized STAs so that these STAs cannot be associated within a period of time. In addition, the dynamic blocklist can be used to disassociate these STAs.

Working Principle

The number of STA association failures (including failures caused by incorrect user names or passwords) is counted in a period of time. When the number of association failures of a STA exceeds a certain threshold, the STA is added to the blocklist. STAs in the blocklist cannot be associated within a period of time.

1.3.2 STA Limit

STA limit aims to limit the number of STAs that can be associated with an AP based on the load capacity. This prevents the risk of insufficient resources caused by overload of APs.

Working Principle

When STAs are associated, the AP checks whether the number of associated STAs exceeds the threshold. If so, STAs cannot be associated.

1.3.3 Load Balancing

Load balancing can balance the load among APs managed by an AC. The load here can be traffic or the number of associated STAs. Load balancing is used to address the problem that some APs are overloaded and some APs are in the idle state.

Working Principle

When a STA attempts to access an AP, if the load on the AP associated by the STA exceeds the preset threshold, the system checks whether the load difference between all the APs in the load balancing group of this AP exceeds the threshold. If so, the STA is not allowed to associate with this AP. The load difference can be configured as the number of STAs or the traffic.

To address the issue that the STA can receive signals from only one AP but fails to be associated due to load balancing, the maximum number of load balancing times can be configured. If two consecutive association failures occur due to load balancing, load balancing is not performed for the third time and the STA can be associated with the AP.

1.3.4 Inter-Radio Load Balancing (by Number of STAs/Traffic/Ratio)

Inter-radio load balancing can balance the load among radios of the same AP to prevent overload of a single radio. Similarly, the load here can be the traffic or the number of associated STAs.

Working Principle

The principle of inter-radio load balancing is similar to that of load balancing group except that you can configure the load balancing thresholds respectively for intra-frequency radios (2.4 GHz, 5 GHz) or inter-frequency radios. The load ratio, that is, the radio weight ratio, can be configured for radios. The default radio weight is 100. For example, if weight of radio 1 is set to 50 and that of radio 2 is set to 100, the load ratio between radio 1 and radio 2 is 1:2. When load balancing is performed, load is balanced to radio 1 and radio 2 according to this load ratio.

1.3.5 Inter-Radio Load Balancing (by Bandwidth Resources)

This feature balances the load among radios based on the bandwidth resources.

Working Principle

When automatic load balancing is configured among radios, the resource weight is calculated for radios based on the channel bandwidth, utilization, and number of STAs accessing the AP. A greater weight indicates that the radio uses more resources. The formula is as follows: Radio weight = (Channel idle rate × Channel bandwidth)/Number of STAs. The channel idle rate equals 100 minus channel utilization rate, which is an integer in the range from 0 to 100, for example, 50 indicates that the channel utilization rate is 50%. By comparing the resource weights of radios accessing the AP, SSID signals on radios with fewer resources are hidden, and inter-radio load balancing guidance is provided for STAs accessing the AP.

1.3.6 Association Control

Association control is a method for controlling association behaviors of wireless STAs. STAs are divided into two groups. In each group, only one STA is defined as the primary STA, and the other STAs are defined as secondary STAs. The secondary STAs must follow the association behaviors of the primary STA. That is, the primary and secondary STAs must be associated with the same wireless network. In this way, association behaviors of wireless STAs can be properly controlled.

Working Principle

The coverage area of a wireless network is divided into several association control domains. One or several APs are deployed in each domain, and wireless clients are divided into groups. The control domains that can be associated with the clients are strictly controlled. For example, a school has many classrooms, and a wireless AP is deployed in each

classroom. Radio signals travel in the space. When e-bags are used in two adjacent classrooms at the same time, the ideal condition is that all clients of the teachers and students are associated with the AP in their own classrooms respectively, avoiding mutual interference. In this case, a classroom must be defined as an association control domain and all clients of the teacher and students in a classroom must be associated with the AP in the classroom.

Association control aims to prevent clients from associating with a wireless network at random when multiple wireless networks are available for selection. The following are prerequisites for network configurations:

- Based on the pre-configured association control domains and package information, the AC delivers the information about primary STAs in all packages to all APs in the association control domains and generates an allowlist of primary STAs on these APs.
- The information about primary STAs in all packages is available in the AP allowlist. Therefore, before association control is enabled, the primary STA must associate itself with the corresponding SSID in the specified control domain. After that, the AC assigns all corresponding secondary STAs to all APs in the association control domain and generates an allowlist based on the configuration of the primary STA package to allow the secondary STAs to associate themselves with the control domain.
- When the primary STA is de-associated from the control domain, all the secondary STAs will also be de-associated and deleted from the AP allowlist.
- The above process can be summarized as follows: The secondary STAs must follow the primary STA to associate themselves with an AP in the same control domain, with which the primary STA is associated. Only the APs in this control domain have an allowlist of the corresponding secondary STAs. This ensures that STAs are not randomly associated with APs in other control domains.

1.3.7 STA Management

STA management is used to manage association and disassociation logic processing of STAs.

Working Principle

In normal cases, a STA sends a disassociation frame to inform the AC that the STA is disassociated. If the STA does not send a disassociation frame to the AC when it is disassociated abnormally (for example, because the user removes the network interface card (NIC)), the AC cannot learn the disassociation of the STA. In this case, the AC detects the STA traffic and finds that the STA has no traffic within a period of time, and concludes that the STA had been disassociated. Then, the AC performs disassociation processing on the STA.

1.3.8 STA Informational Syslog Suppression

STA informational syslog suppression prevents a high CPU usage caused by the large number of informational syslogs generated when STAs are frequently associated or disassociated.

Working Principle

The number of syslogs output per second is counted. When this number reaches the upper limit, no more syslog is output within the second, thereby suppressing the syslog. In the next second, the number of syslogs is counted again.

1.3.9 Intelligent SSID Hiding

When the number of STAs on an AP or a radio reaches the upper limit, new STAs are not allowed to go online but the STAs can still scan the SSID and attempt to perform association. After the intelligent SSID hiding feature is enabled, new STAs cannot detect the signal and will not attempt to perform association. This prevents STAs from performing association even when the STA quantity exceeds the upper limit.

Working Principle

When the number of STAs on an AP or a radio reaches the upper limit, the Beacon frame sent by the AP does not carry the SSID. When a new STA sends a probe request, the AP does not respond with a Probe response.

1.3.10 STA Jitter Prevention

STA jitter prevention is used to retain a STA entry on the AC for a period of time after a STA is disassociated. In this time period, if the STA goes online from the same WLAN of the AP again, it is regarded that the STA has never gone offline. If the STA goes online from the same WLAN of another AP, it is regarded that the STA roams to the AP with the same SSID. If the STA goes online from another WLAN, it is regarded that the STA is switched to another AP with a different SSID. If the AP or authentication server proactively forces a STA to go offline, the STA jitter prevention function does not take effect and the STA goes offline immediately.

STA jitter prevention enables a STA to perform Layer 3 roaming, preventing a roaming failure caused by a disassociation request proactively sent by the STA in the coverage hole.

Working Principle

After STA jitter prevention is enabled and a STA is disassociated, the AC adds the STA to the offline queue and starts a timer according to the expected deletion time specified based on the jitter prevention time. If the STA re-associates with an AP before the timer expires, the AC removes the STA from the offline queue and regards it as an online STA. Otherwise, the AC forces the STA to go offline when the timer expires.

1.3.11 Syslog Format Upon STA Association

The syslog format for obtaining an IP address is provided when a STA goes online, facilitating interconnection with log systems.

Working Principle

The device determines whether the format switching command is configured when the syslog format is output after the IP address is successfully obtained when the STA goes online. If not, output the default format; otherwise, output the configured format.

1.3.12 Fast STA Association

When a STA goes online, the AC does not wait for the response packet from AP indicating that the STA is added.

Working Principle

When this feature is disabled, during STA online interaction, the AC will process the next association request packet after the STA is associated with the AP. When this feature is enabled, the AC will no longer wait, improving concurrent STA access performance.

1.3.13 IP Address Detection

IP address detection is used to detect whether a STA has obtained an IP address.

Working Principle

The system detects the IP addresses of STAs. STAs without IP address will be disconnected to reacquire IP address. STAs disconnected by IP detection mechanism will not be checked again for a period of time.

1.3.14 DHCP Proxy

The STA management module notifies whether DHCP proxy is enabled or disabled.

Working Principle

The STA management module notifies the DHCP module to enable or disable DHCP proxy through the command. When DHCP proxy is enabled, the device will replace the STA to initiate DHCP discover packets, exchange packets with the DHCP server, and generate DHCP snooping entries on the AC, eliminating the need for STA to participate in this process.

1.4 Configuration

Configuration	Description and Command	
Configuring Dynamic	⚠ (Mandatory) It is used to enable the dynamic blocklist function.	
	sta-blacklist enable	Enables the dynamic blocklist function.
	⚠ (Optional) It is used to configure the parameters of the dynamic blocklist.	
	sta-blacklist lifetime	Configures the aging time of the dynamic blocklist.
	sta-blacklist detect-time	Configures the detection time of the dynamic blocklist.
	sta-blacklist fail-limit	Configures the maximum number of association failures.
Configuring STA Limit	⚠ (Optional) It is used to configure the maximum number of STAs.	
	sta-limit	Configures the maximum number of STAs.
	sta-limit per-ap	Configures the STA quantity limit for each AP on a WLAN.
	sta-limit radio	Configures the maximum number of STAs that can be associated with a radio of the AP.
Configuring Load Balancing	⚠ (Mandatory) It is used to configure load balancing.	
	num-balance-group enable	Enables the number-based balancing feature.

	num-balance-group create	Creates a number-based balancing group.
	num-balance-group add	Adds an AP to the number-based balancing group.
	num-balance-group del	Deletes an AP from the number-based balancing group.
	flow-balance-group enable	Enables the traffic balancing feature.
	flow-balance-group create	Creates a traffic-based balancing group.
	flow-balance-group add	Adds an AP to the traffic-based balancing group.
	flow-balance-group del	Deletes an AP from the traffic-based balancing group.
	(Optional) It is used to configure the load balancing parameters.	
	num-balance-group num	Configures the threshold of the number-based balancing group.
	num-balance-group mode	Configures the working mode of the number-based balancing group.
	flow-balance-group flow	Configures the threshold of the traffic-based balancing group.
	flow-balance-group radio-flow	Enables a specified traffic balancing group to use the traffic uploaded by APs.
	flow-balance-group base	Configures the traffic base value.
	sta-balance num-limit enable	Configures the number of the load balancing attempts.
Configuring Inter-Radio Load Balancing (by Number of STAs/Traffic/Ratio)	(Mandatory) It is used to enable inter-radio load balancing.	
	inter-radio-balance flow-balance enable	Enables inter-radio traffic-based balancing.
	inter-radio-balance num-balance enable	Enables inter-radio number-based balancing.
	(Optional) It is used to configure the load balancing parameters.	
	inter-radio-balance flow-balance dual-band	Configures parameters for traffic-based balancing among inter-frequency radios.
	inter-radio-balance flow-balance same-band	Configures parameters for traffic-based balancing among intra-frequency radios.
	inter-radio-balance num-balance dual-band	Configures parameters for number-based balancing among inter-frequency radios.

	inter-radio-balance num-balance same-band	Configures parameters for number-based balancing among intra-frequency radios.
Configuring Inter-Radio Load Balancing (by Bandwidth Resources)	(Mandatory) It is used to enable inter-radio load balancing.	
	ap-inter-balance enable	Enables inter-radio load balancing.
	(Optional) It is used to configure the load balancing parameters.	
	ap-inter-balance chan-wid-thrd	Configures the bandwidth resource threshold for triggering inter-radio load balancing guidance.
	ap-inter-balance weight-scale	Configures the amplification factor of the bandwidth resource weight of the STA-accessed radio.
	ap-inter-balance low-weight-scale	Configures the amplification factor of the bandwidth resource weight of the non-STA-accessed radio.
	ap-inter-balance hide-limit count	Configures the frequency limit of the AC sending messages to the hidden SSID.
Configuring Inter-Radio Load Balancing (by Bandwidth Resources) **Config**	(Mandatory) It is used to enable association control.	
	package	Configures a package.
	primary-sta	Configures the primary STA in the package.
	secondary-sta	Configures the secondary STA in the package.
	control-zone	Configures an association control domain.
	ap	Configures the AP information.

uration

Effect

Guide STAs to access radios with more bandwidth resources for inter-radio load balancing.

Notes

- When the inter-radio load balancing feature and the 5G first feature are both enabled, and the SSID signal is hidden by the load balancing feature because the 5 GHz radio has fewer resources, new STAs accessing the radio will be rejected by the 5G first feature if they support 5G.
- If the bandwidth resource weight of the radio that STAs access is still lower than other radios after the resource weight is amplified through the amplification factor, the SSID of the radio is hidden to prevent users from viewing it.

Configuring STA Management	(Optional) It is used to configure the time after which the STA is disassociated if no traffic is detected.	
	sta-idle-timeout	Configures the time after which the STA is disassociated if no traffic is detected.
Configuring STA Informational Syslog Suppression	(Optional) It is used to configure the maximum output rate of the STA informational syslogs.	
	sta-logging rate-limit	Configures the maximum output rate of the STA informational syslogs.
Configuring Configuring Intelligent SSID	**hide-ssid sta-reach-limit** [**radio** { **2.4g** | **5g** | **6g** }]	Configures intelligent SSID hiding.
Configuring STA Jitter Prevention	(Optional) It is used to set the jitter prevention time.	
	prevent-jitter enable	Enables STA jitter prevention.
	prevent-jitter time keep-time	Configures the STA jitter prevention time.
Configuring Configuring the Syslog Format upon STA Association STA Association	(Optional) It is used to set the format of the syslog output when a STA obtains an IP address online.	
	sta-logging mac-fmt-line	Configures the format of the syslog output when a STA goes online and obtains an IP address.
Enabling Enabling Fast STA Association	(Optional) It is used to enable fast association for STAs.	
	sta-behaviour fast-assoc	Configures fast association for STAs.
Enabling Enabling IP Address Detection	(Mandatory) It is used to enable or disable IP address detection for STAs.	
	sta-behaviour ip-check enable	Enables or disables IP address detection.
	(Optional) It is used to set the delay for IP address detection for STAs.	
	sta-behaviour ip-check delay *time*	Configures the delay for IP address detection, in seconds.
	(Optional) It is used to set the quiet period for IP address detection for STAs.	
	sta-behaviour ip-check sulk *time*	Configures the quiet period for IP address detection, in seconds.
Enabling Enabling DHCP Proxy	(Optional) It is used to enable DHCP proxy.	
	sta-behaviour dhcp-proxy enable	Enables or disables DHCP proxy.
	(Optional) It is used to configure the delay for DHCP proxy.	
	sta-behaviour dhcp-proxy delay *time*	Configures the delay for DHCP proxy, in seconds.
Configuring Configuring	(Optional) It is used to delete the MAC address of a specified wireless STA.	

Wireless STA Management	**client-kick**	Deletes the MAC address of a specified wireless STA.

1.4.1 Configuring Dynamic Blocklist

Configuration Effect

- When the number of association failures on a STA reaches the threshold within the specified time, this STA is added to the blocklist.

Notes

- The time period is not fixed and is between **detect-time** and (**detect-time** + 5), in seconds. This factor must be considered during configuration.
- If multiple authentication modes are applied, the number of STA association failures increases by 1 when one of the authentication modes fails. Combinations of authentication modes include, but are not limited to, PSK + Web, PSK + MAB + Web, PSK + MAB, MAB + Web, and 802.1X + Web.

Configuration Steps

Enabling Dynamic Blocklist

- (Mandatory) Enable dynamic blocklist on an AC.

Command	**sta-blacklist enable**
Parameter Description	N/A
Defaults	Dynamic blocklist is disabled.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring the Dynamic Blocklist Parameters

- (Optional) Configure the dynamic blocklist parameters on an AC.
- Configure the aging time for the blocklist. If the aging time of blocklist entries is set improperly, you can reconfigure the aging time.
- Run the **sta-blacklist lifetime** command to configure the aging time for the dynamic blocklist. A longer aging time indicates a longer period of time within which blocklisted STAs are not allowed for association.
- Run the **sta-blacklist detect-time** command to configure the detection time. As the detection time decreases, unauthorized STA detection becomes more sensitive and the number of false reports increases.
- Run the **sta-blacklist fail-limit** command to configure the upper limit of association failures. A larger upper limit indicates that a STA can make more association attempts.

Command	**sta-blacklist lifetime** *seconds*
Parameter Description	*seconds:* Indicates the aging time of STAs in the blocklist. The value ranges from 60s to 1200s.
Defaults	300s

Command Mode	AC configuration mode
Usage Guide	N/A

Command	**sta-blacklist detect-time** *seconds*
Parameter Description	*seconds:* Indicates the STA detection time. The value ranges from 5s to 60s.
Defaults	60s
Command Mode	AC configuration mode
Usage Guide	This command is used to configure the STA detection time. When a STA fails upon first association, the STA is listed as a suspected attacker. If the number of association failures on the STA reaches the upper limit (namely, the **fail-limit**) within the detection time, the STA is added to the blocklist.

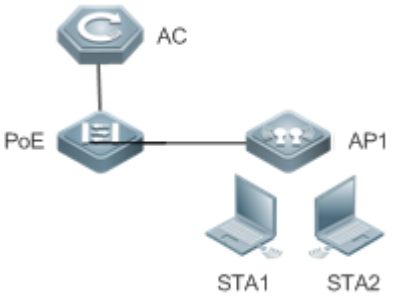
Command	**sta-blacklist fail-limit** *number*
Parameter Description	*number*: Indicates the maximum number of association failures. The value ranges from 1 to 100.
Defaults	The maximum number of association failures is 5.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show sta-blacklist** command to display the STAs in the blocklist.

Configuration Example

↘ Configuring Dynamic Blocklist

Scenario **Figure 1-4**	
Configuration Steps	● Configure the dynamic blocklist function.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-blacklist enable

Verification	● After the CAPWAP tunnel is established between an AP and an AC, enter an incorrect password for several times to verify that the STA can be added to the blocklist.
AC	AC# show sta-blacklist Num STA MAC Add time ---------- -------------- -------------------- 1 0080.1111.1111 2013-07-02 13:56:22 2 0090.2222.3333 2013-07-02 13:56:35 3 0070.1111.2233 2013-07-02 13:57:08

Common Errors

- N/A

1.4.2 Configuring STA Limit

Configuration Effect

- Limit the maximum number of STAs that can be associated with an AC, a WLAN, an AP, or a radio of an AP on the wireless network.

Notes

- The STA limits configured for an AC, a WLAN, an AP, or a radio of an AP take effect simultaneously. That is, a STA can be associated only if all the STA limits are met.
- The STA limit configured on the AC is not under license control.

Configuration Steps

↘ Configuring STA Limit

- (Optional) Configure the STA limit an AC.
- If there a large number of STAs on the wireless network, configure the STA limit to allow more STAs to be associated, but the total bandwidth will decrease.
- Run the **sta-limit** command to configure the STA limit. A large STA limit indicates that more STAs can be associated.
- The default AC-based STA limit is the maximum number of STAs that can be associated with an AC. The default WLAN-based STA limit is not specified. By default, the AP-based STA limit is 32 for a disassociated AP or in AP group configuration mode and varies with models for an associated AP.
- Run the **sta-limit radio** command to configure the radio-based STA limit for an AP. A larger STA limit indicates that more STAs can be associated. No limit is set by default. Radio-based STA limit and AP-based STA limit are independent. The total number of radio-based STA limits cannot be considered as the AP-based STA limit.
- Run the **sta-limit per-ap** command to configure the maximum number of STAs supported on each AP on a WLAN. By default, the number of STAs on an AP is not limited. If the number of configured STAs exceeds the maximum number of STAs supported by an AP, no new STA can be associated with the AP.

Command	**sta-limit** *max-num*

Parameter Description	*max-num*: Indicates the maximum number of STAs. The value varies according to the configuration modes and devices.
Defaults	In AC configuration mode, the default value is the maximum number of STAs supported by an AC, not limited by the license. In AP group configuration mode, the default value is 64. In AP configuration mode, the default value is 64 for a disassociated AP or in the **ap-config all** configuration mode. The default value for an associated AP is determined by the AP model. In WLAN configuration mode, the STA limit is not specified.
Command Mode	AC configuration mode, WLAN configuration mode, AP configuration mode, or AP group configuration mode
Usage Guide	If the maximum number of STAs configured for a disassociated AP exceeds the actual capacity, the STA limit automatically changes to the actual maximum number of STAs supported after the AP is associated.

Command	**sta-limit** *max-num* **radio** *radio-id*
Parameter Description	*max-num*: Indicates the maximum number of STAs. The value ranges from 1 to 4,096. *radio-id*: Indicates the radio ID. The value ranges from 1 to 96.
Defaults	The STA limit is not specified.
Command Mode	AP configuration mode and AP group configuration mode
Usage Guide	If the maximum number of STAs configured for a disassociated AP exceeds the actual capacity of the radio, the STA limit automatically changes to the actual maximum number of STAs supported after the AP is associated.

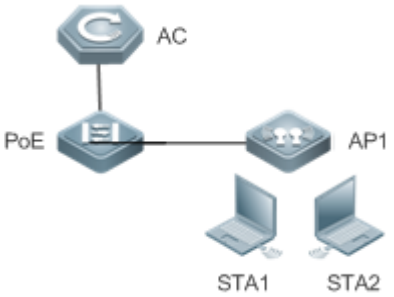
Command	**sta-limit per-ap** *max-num*
Parameter Description	*max-num*: Indicates the maximum number of STAs supported on an AP. The value ranges from 1 to 4,096.
Defaults	The number of STAs supported on an AP is not limited.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Verify that the number of STAs is limited.

Configuration Example

Configuring STA Limit

Scenario **Figure 1-5**	
Configuration Steps	● Configure the STA limit.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ap-config ap1 AC(config-ap)# sta-limit64
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the AC running configuration.
AC	AC# show ap-config running ap-config ap1 sta-limit 64 !

Common Errors

- N/A

1.4.3 Configuring Load Balancing

Configuration Effect

- Enable even distribution of STAs on multiple APs in a load balancing group.

Notes

- Load balancing is applicable only to STAs that are associated, but not to STAs that are disassociated. Therefore, after STAs are disassociated, the traffic difference between APs or the STA quantity difference may exceed the threshold.
- Load balancing takes effect only on the same type of radios (2.4 GHz, 5 GHz, or 6 GHz). If the types of radios are different, load balancing is performed only when the AP reports that the STAs are capable of multi-band operation. Otherwise, the 2.4 GHz STAs may fail to be associated with 2.4 GHz radios when no STA is associated with 5 GHz radio. The same applies to other radios.
- After the traffic-based balancing group is configured to use the traffic information uploaded by APs, APs must upload the traffic information to the AC at a regular interval because the traffic only exists on APs and is not routed to the AC. During this interval, the traffic information on the AC does not change. At this time, if the traffic between APs is not

balanced, STAs cannot be associated with APs with heavy traffic until the APs upload the traffic information to the AC.

Configuration Steps

Creating a Number-based Balancing Group

- (Mandatory) Create a number-based balancing group on the AC.
- APs can be only added to a created load balancing group.

Command	**num-balance-group create** *group-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group.
Defaults	No number-based balancing group is created.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding an AP to the Number-based Balancing Group

- (Mandatory) The configuration is performed on the AC.
- Load balancing only applies to the APs which are added to a load balancing group.

Command	**num-balance-group add** *group-name ap-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	No AP is added to the number-based balancing group.
Command Mode	AC configuration mode
Usage Guide	N/A

Creating a Traffic-based Balancing Group

- (Mandatory) The configuration is performed on the AC.
- Load balancing only applies to the APs which are added to a created load balancing group.

Command	**flow-balance-group create** *group-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group.
Defaults	No traffic-based balancing group is created.
Command Mode	AC configuration mode
Usage Guide	N/A

Adding an AP to the Traffic-based Balancing Group

- (Mandatory) The configuration is performed on the AC.
- Load balancing only applies to the APs which are added to a load balancing group.

Command	**flow-balance-group add** *group-name ap-name*

Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	No AP is added to the traffic-based balancing group.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring Load Balancing Group Parameters

- (Optional) Configure the parameters of a load balancing group on the AC.
- Run the **num-balance-group num** command to configure the threshold of number-based balancing. A larger threshold indicates a greater difference in the number of STAs associated with two APs, and the less balanced load.
- Run the **num-balance-group mode** command to configure radio-based balancing. If radio-based balancing is enabled, the control on the distribution of STAs is more accurate, but the effect of balancing among APs is less satisfying.
- Run the **num-balance-group enable** command to configure the trigger threshold of the number-based balancing group. A higher trigger threshold indicates that load balancing is enabled only when the AP load is heavier.
- Run the **num-balance-group del** command to delete an AP from the number-based balancing group.
- Run the **flow-balance-group flow** command to configure the traffic-based balancing threshold. A higher traffic balancing threshold indicates that the traffic difference between two APs is greater and the traffic is less balanced.
- Run the **flow-balance-group radio-flow** command to enable the traffic balancing group to use the traffic information uploaded by APs. In local forwarding mode, data packets are not routed to the AC, and the AC cannot obtain the traffic information. Therefore, the traffic information uploaded by APs must be used to determine whether to enable load balancing.
- Run the **flow-balance-group enable** command to configure the trigger threshold of the traffic-based balancing group. A higher trigger threshold indicates that load balancing is enabled only when the AP load is heavier.
- Run the **flow-balance-group del** command to delete an AP from the traffic-based balancing group.
- Run the **flow-balance-group base** command to configure the baseline of traffic balancing in global configuration mode.
- Run the **sta-balance num-limit enable** command to configure the maximum number of times for enabling load balancing.

Command	**num-balance-group num** *group-name number*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *number*: Indicates the trigger threshold. The default value is 3. The value ranges from 0 to 20. **0** indicates that number-based balancing is disabled for the load balancing group.
Defaults	3
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group mode** *group-name*{ **radio-mode**| **ap-mode** }

Parameter Description	*group-name:* Indicates the name of a load balancing group.
Defaults	AP-based number balancing
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group enable** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: indicates the trigger threshold. The default value is 3. The value ranges from 0 to 10. **0** indicates that number-based balancing is disabled for the load balancing group.
Defaults	3
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**num-balance-group del** *group-name ap-name*
Parameter Description	*group-name*: Indicates the name of a load balancing group. *ap-name*: Indicates the AP name.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group flow** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: indicates the trigger threshold. The unit is %. The default value is 5%. The value ranges from 0 to 1,000. **0** indicates that load balancing is disabled for the load balancing group. The traffic baseline is 10 Mbps by default.
Defaults	5%
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group radio-flow** *group-name*
Parameter Description	*group-name:* Indicates the name of a specified traffic balancing group that uses the traffic information uploaded by APs.
Defaults	Traffic information on the CAPWAP data channel is used on the AC.
Command Mode	AC configuration mode
Usage Guide	You can enable a traffic balancing group to use the traffic information uploaded by APs. In this way, the traffic

	balancing group can receive the traffic information periodically sent by APs for load balancing.

Command	**flow-balance-group enable** *group-name number*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *number*: Indicates the trigger threshold. The unit is %. The default value is 5%. The value ranges from 0 to 500. **0** indicates that load balancing is disabled for the load balancing group. The traffic baseline is 10 Mbps by default.
Defaults	5%
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group del** *group-name ap-name*
Parameter Description	*group-name:* Indicates the name of a load balancing group. *ap-name:* Indicates the AP name.
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Command	**flow-balance-group base** *number*
Parameter Description	*number*: Indicates that traffic baseline. The default value is 10 Mbps. The value ranges from 1 to 100.
Defaults	10 Mbps
Command Mode	AC configuration mode
Usage Guide	N/A

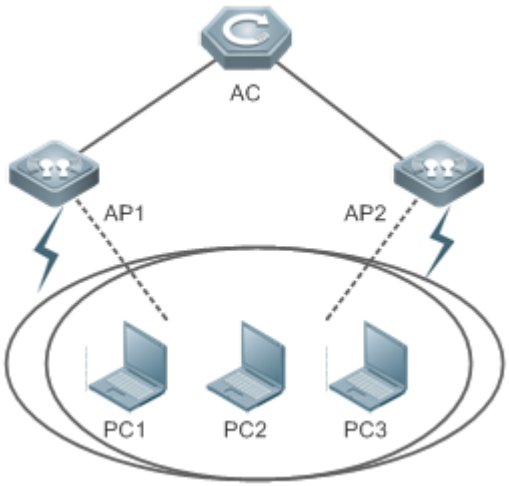
Command	**sta-balance num-limit enable**
Parameter Description	N/A
Defaults	The function is disabled.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Number balancing: Check whether the difference in the number of STAs associated with APs in the load balancing group is within the threshold.
- Traffic balancing: Check whether the difference in the traffic of APs in the load balancing group is within the threshold.

Configuration Example

Configuring Traffic-based Balancing

Scenario **Figure 1-6**	
Configuration Steps	● Create a load balancing group. ● Set the trigger threshold of this load balancing group to 1,000 Kbps. ● Add AP1 and AP2 to the load balancing group named **test-group.** (If two APs are added to the same load balancing group, PCs in this group can search the radio signals of both APs.)
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)#ac-controller AC(config-ac)#flow-balance-group create test-group AC(config-ac)#flow-balance-group flow test-group 10 AC(config-ac)#flow-balance-group add test-group AP1 AC(config-ac)#flow-balance-group add test-group AP2
Verification	● Check the configuration of the load balancing group.
AC	AC# show ac-config flow-balance summary Group State Enable Threshold Base mode AP NAME --- ----- --- --- ---- --- --- test-group UP 5*100kbps 10% 10 ap-mode(0) AP1, AP2

Common Errors

- N/A

1.4.4 Configuring Inter-Radio Load Balancing (by Number of STAs/Traffic/Ratio)

Configuration Effect

- Enable inter-radio load balancing on APs to balance the load among radios.
- Configure the load ratio of radios. Load is balanced among radios according to the ratio.

Notes

- This function is not applicable to the i-Share solution. Signals of different radios cover different areas. A STA may receive signals from one or several radios. In this case, the inter-radio load balancing function cannot be enabled.
- Load balancing is applicable only to STAs that are associated. Therefore, after STAs are disassociated, the traffic difference between APs or the STA quantity difference may exceed the threshold.
- If the radio that a STA attempts to associate with is different from the radio with the lowest load, load balancing is performed only when the AP reports that the STA is capable of multi-band operation. Otherwise, the 2.4 GHz STAs may fail to be associated with 2.4 GHz radios when no STA is associated with 5 GHz radio. The same applies to other radios.
- After the traffic balancing group is configured to use the traffic information uploaded by APs, APs must upload the traffic information to the AC at a regular interval because the traffic only exists on APs in local forwarding mode. During this interval, the traffic information on the AC does not change. At this time, if the traffic among APs is not balanced, STAs cannot be associated with APs with heavy traffic until the APs upload the traffic information to the AC.
- Configuration of load balancing parameters varies according to the inter-frequency and intra-frequency radios. When performing load balancing, the AC determines the load balancing parameter according to the target radio and the type of the radio associated with the STA and determines whether to associate the STA to the target radio
- For a specific AP, when load balancing is enabled in any of the **ap-config**, **ap-group**, and **ap-config** all modes, load balancing is enabled on this AP. If the load balancing configurations in the three modes are different, the configurations take effect in descending order: **ap-config** mode, **ap-group** mode, **ap-config all** mode.
- When inter-radio load balancing is enabled, the association attempt of the same STA will be denied for at most twice within five minutes. If the STA is still associated with a radio with a heavy load for the third time, the association is allowed. Therefore, the effect of inter-radio load balancing is related to the actual STA behaviors.

Configuration Steps

↘ Enabling Inter-radio Traffic Balancing

- (Mandatory). The configuration is performed on the AC. After the function is enabled, traffic is balanced whenever possible among different radios of the same AP.
- This function can be enabled for a single AP, all APs in an AP group, or all APs (configured in **ap-config all** mode).

Command	**inter-radio-balance flow-balance enable**
Parameter Description	N/A
Defaults	Inter-radio traffic balancing is disabled.
Command Mode	AP configuration mode and AP group configuration mode
Usage Guide	N/A

↘ Enabling Inter-radio Number Balancing

- (Mandatory) The configuration is performed on the AC. After the function is enabled, the number of STAs is balanced whenever possible among different radios of the same AP.
- This function can be enabled for a single AP, all APs in an AP group, or all APs (configured **in ap-config all** mode).

Command	**inter-radio-balance num-balance enable**
Parameter Description	N/A
Defaults	Inter-radio number balancing is disabled.
Command Mode	AP configuration mode and AP group configuration mode
Usage Guide	N/A

Configuring Inter-radio Load Balancing Parameters

- (Optional) The configuration is performed on the AC. The configuration of parameters can be changed based on actual requirements of network optimization.
- Run the **inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for traffic balancing among inter-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.
- Run the **inter-radio-balance flow-balance same-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for traffic balancing among intra-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.
- Run the **inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for number balancing among inter-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.
- Run the **inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num* command to configure the trigger threshold and the load threshold for number balancing among intra-frequency radios. A smaller trigger threshold indicates that it is easier to enable load balancing. A smaller load threshold indicates that the load is better balanced.

Command	**inter-radio-balance flow-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	*en-num*: Indicates the trigger threshold. The unit is kbps. The value ranges from 1 to 1,000. *thrs-num*: Indicates the load threshold. The unit is kbps. The value ranges from 1 to 1,000.
Defaults	Both the trigger threshold and the load threshold are 10.
Command Mode	AP configuration mode and AP group configuration mode
Usage Guide	N/A

Command	**inter-radio-balance flow-balance same-band enable-load***e n-num* **threshold** *thrs-num*
Parameter Description	*en-num*: Indicates the trigger threshold. The unit is 100 kbps. The value ranges from 1 to 1,000. *thrs-num*: Indicates the load threshold. The unit is 100 kbps. The value ranges from 1 to 1,000.
Defaults	Both the trigger threshold and the load threshold are 5.

Command Mode	AP configuration mode and AP group configuration mode
Usage Guide	N/A

Command	**inter-radio-balance num-balance dual-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	*en-num*: Indicates the trigger threshold. The value ranges from 1 to100. *thrs-num*: Indicates the load threshold. The value ranges from 1 to 100.
Defaults	The trigger threshold value is 20 and the load threshold is 8.
Command Mode	AP configuration mode and AP group configuration mode
Usage Guide	N/A

Command	**inter-radio-balance num-balance same-band enable-load** *en-num* **threshold** *thrs-num*
Parameter Description	*en-num*: Indicates the trigger threshold. The value ranges from 1 to 100. *thrs-num*: Indicates the load threshold. The value ranges from 1 to 100.
Defaults	The trigger threshold and the load threshold are 20 and 6 respectively.
Command Mode	AP configuration mode and AP group configuration mode
Usage Guide	N/A

Configuring the Load Ratio of Radios

- (Optional) The configuration is performed on the AC. After the load ratio is configured, load is balanced to different radios of the same AP based on the ratio.
- The load ratio can be configured for a single AP, all APs in an AP group, or all APs (configured in **ap-configure all** mode).

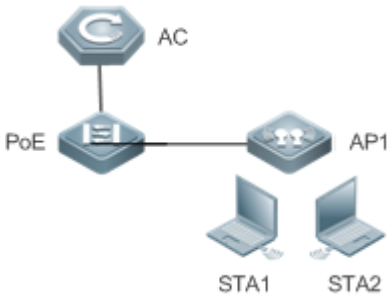
Command	**inter-radio-balance radio** *radio-id* **weight** *weight-num*
Parameter Description	N/A
Defaults	The radio weight is 100, and load is balanced between radios based on the 1:1 ratio by default.
Command Mode	AP configuration mode and AP group configuration mode
Usage Guide	N/A

Verification

- Number balancing: Run the **show ap-config summary** command to check whether the difference in the number of STAs between radios of the AP where load balancing is within the threshold.
- Traffic balancing: Run the **show ac-config client** command to check whether the traffic difference between radios of the AP where load balancing is enabled is within the threshold.

Configuration Example

Enabling Inter-radio Number Balancing on All APs in the Default AP Group

Scenario **Figure 1-7**	
Configuration Steps	● Enter the default AP group configuration mode. ● Enable inter-radio number balancing.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)#ap-group default AC(config-group)#inter-radio-balance num-balance enable
Verification	● Run the **show run** command to display the configuration.
AC	AC# show run | begin ap-group default ap-group default inter-radio-balance num-balance enable

Common Errors

- N/A

1.4.5 Configuring Inter-Radio Load Balancing (by Bandwidth Resources)

Configuration Effect

Guide STAs to access radios with more bandwidth resources for inter-radio load balancing.

Notes

- When the inter-radio load balancing feature and the 5G first feature are both enabled, and the SSID signal is hidden by the load balancing feature because the 5 GHz radio has fewer resources, new STAs accessing the radio will be rejected by the 5G first feature if they support 5G.
- If the bandwidth resource weight of the radio that STAs access is still lower than other radios after the resource weight is amplified through the amplification factor, the SSID of the radio is hidden to prevent users from viewing it.
- Only resource weights of radios on one AP can be compared.
- An SSID can be hidden based on the bandwidth resource weight only when the same SSID is configured on different radios, so that user services are not affected. For example, if SSID4 exists on radio 1 and not on radio 2, SSID4 will not be hidden even if the resource weight of radio 1 is far lower than that of radio 2, ensuring that users can always access SSID4 in the wireless environment.

Configuration Steps

Enabling Inter-Radio Load Balancing

- Optional

Command	**ap-inter-balance enable**
Parameter Description	N/A
Defaults	The feature is disabled.
Command Mode	AP group configuration mode, AP configuration mode, and all AP configuration mode
Usage Guide	N/A

Configuring the Bandwidth Resource Threshold for Triggering Inter-Radio Load Balancing Guidance

- Optional

Command	**ap-inter-balance chan-wid-thrd** { **20** | **40** | **80** | **160** } **thrd-hold** *thrd-num*
Parameter Description	**20**: Indicates the lower limit of average STA bandwidth resources if the radio bandwidth is 20 MHz. **40**: Indicates the lower limit of average STA bandwidth resources if the radio bandwidth is 40 MHz. **80**: Indicates the lower limit of average STA bandwidth resources if the radio bandwidth is 80 MHz. **160**: Indicates the lower limit of average STA bandwidth resources if the radio bandwidth is 160 MHz. *thrd-num*: Indicates the lower limit of average bandwidth resources occupied by each STA accessing the radio. If the occupied resources are lower than this threshold, inter-radio load balancing guidance is triggered. The value range is from 1 to 320.
Defaults	Default lower limit of average STA bandwidth resources, *thrd-num*, depends on the bandwidth configuration of the radio. ● If the default bandwidth is 20 MHz, the default lower limit of average STA bandwidth resources is 4. ● If the default bandwidth is 40 MHz, the default lower limit of average STA bandwidth resources is 8. ● If the default bandwidth is 80 MHz, the default lower limit of average STA bandwidth resources is 8. ● If the default bandwidth is 160 MHz, the default lower limit of average STA bandwidth resources is 16.
Command Mode	AP group configuration mode, AP configuration mode, and all AP configuration mode
Usage Guide	N/A

Configuring the Bandwidth Resource Weight Amplification Factor of the STA-Accessed Radio

- Optional
- When a STA accesses the AP, the radio where the SSID that the STA connects to is located is the STA-accessed radio, while other radios on the AP are non-STA-accessed radios.

Command	**ap-inter-balance weight-scale** *scale-num*
Parameter Description	*scale-num*: Indicates the factor based on which the resource weight of the STA-accessed radio is amplified during resource weight calculation. For example, 50 indicates that the weight is amplified by 50%. The value range is from 1 to 1000.
Defaults	The default value is 50, that is, weight × 1.5.
Command	AP group configuration mode, AP configuration mode, and all AP configuration mode

Mode	
Usage Guide	• Calculated resource weights of different radios may differ greatly. Therefore, resource weights of STA-accessed radios are amplified based on a specific ratio to reduce the differences, preventing frequent SSID hiding before the resource lower limit is reached. • The larger resource weight amplification factor, the less chance of SSID hiding and load balancing guidance.

Configuring the Bandwidth Resource Weight Amplification Factor of Non-STA-Accessed Radios

- Optional
- When a STA accesses the AP, the radio where the SSID that the STA connects to is located is the STA-accessed radio, while other radios on the AP are non-STA-accessed radios.

Command	**ap-inter-balance low-weight-scale** *scale-num*
Parameter Description	*scale-num*: Indicates the factor based on which the resource weight of the non-STA-accessed radio is amplified during resource weight calculation. For example, 50 indicates that the weight is amplified by 50%. The value range is from 1 to 1000.
Defaults	The default value is 0.
Command Mode	AP group configuration mode, AP configuration mode, and all AP configuration mode
Usage Guide	Resource weights of radios are amplified based on this factor to reduce resource weight differences among radios, preventing frequent SSID hiding. If this factor is larger, hidden SSIDs are unhidden and wireless service is restored earlier.

Configuring the Frequency Limit of the AC Sending Messages to the Hidden SSID

- Optional
- Compare the resource weights of different radios on the AP. If the resource weight of the STA-accessed radio is still lower than those of other radios after the weight is amplified based on the amplification factor, the SSID is hidden.

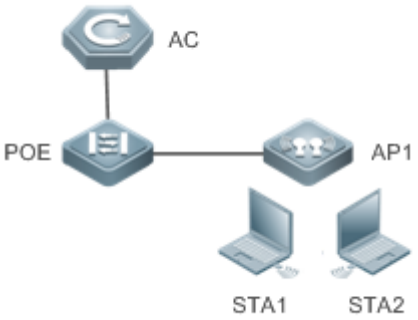
Command	**ap-inter-balance hide-limit count** *count-num* **lifetime** *time*
Parameter Description	*count-num*: Indicates the maximum number of times that the AC sends messages to the hidden SSID within one cycle. The value range is from 1 to 300. *time*: Indicates the duration of one cycle, in seconds. The value range is from 3 to 300.
Defaults	The default value of *count-num* is 30, and the default value of *time* is 120.
Command Mode	AP group configuration mode, AP configuration mode, and all AP configuration mode
Usage Guide	N/A

Verification

Run the **show ap-config running** *ap-name* command to check whether the configuration is successful.

Configuration Example

Configuring Load Balancing

Scenario **Figure 1-1**	
Configuration Steps	5. Enable inter-radio load balancing for AP1. 6. Set the bandwidth of the radio to 80 MHz and the lower limit of average STA bandwidth resources to 10 MHz. 7. Set the resource weight amplification factor to 30 for STA-accessed radios and non-STA-accessed radios. 8. Configure the AC to send messages to the hidden SSID 30 times at maximum within 150s.

AC	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# ap-inter-balance enable`
	`Hostname(config-ap)# ap-inter-balance chan-wid-thrd 80 thrd-hold 10`
	`Hostname(config-ap)# ap-inter-balance weight-scale 30`
	`Hostname(config-ap)# ap-inter-balance low-weight-scale 30`
	`Hostname(config-ap)# ap-inter-balance hide-limit count 30 lifetime 150`

Verification	View the configuration.

AC	`Hostname# show ap-config running`
	` ap-inter-balance enable`
	` ap-inter-balance chan-wid-thrd 80 thrd-hold 10`
	` ap-inter-balance weight-scale 30`
	` ap-inter-balance low-weight-scale 30`
	` ap-inter-balance hide-limit count 30 lifetime 150`
	`!`

Common Errors

- N/A

1.4.6 Configuring Association Control

Configuration Effect

- Secondary STAs must be associated with APs in the same group as the primary STA when being associated.

Notes

- When a package is deleted, all its related configurations are deleted as well. If some STAs in this package are currently associated, all these STAs will be disassociated.
- A package can only be configured with one primary STA. If the information about the primary STA in the package is configured for multiple times, the latest configuration prevails.
- When a primary STA is deleted from a package, the primary STA and all secondary STAs in this package may be disassociated.
- When a secondary STA is deleted from a package, this secondary STA may be disassociated.
- The association control domain name cannot be duplicated. Otherwise, an error will be prompted. In addition, if an association control domain is deleted, all configurations related to this domain will be deleted. Consequently, STAs in the package associated with this control domain may be disassociated.
- When the AP information in an association control domain is deleted, STAs in the package associated with this AP be disassociated.

Configuration Steps

Configuring a Package

- (Mandatory) The configuration is performed on an AC.
- The primary and secondary STA information can be configured only after a package is configured.

Command	**package** *pkg-name*
Parameter Description	*pkg-name*: Indicates the name of a package. The package name is a string of 1 to 32 characters.
Defaults	No package is configured.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Primary and Secondary STAs in a Package

- (Mandatory) The configuration is performed on an AC.
- Run the **primary-sta** command to configure the primary STA. Only one primary STA can be configured. The secondary STAs will be associated with APs in the same group as the primary STA.
- Run the **secondary-sta** command to configure a secondary STA. After the secondary STA is configured, the secondary STA will be associated with an AP in the same group as the primary STA.

Command	**primary-sta** *mac-address*
Parameter Description	*mac-address*: Indicates the MAC address of the STA.
Defaults	No primary STA is configured.
Command Mode	Package configuration mode
Usage Guide	N/A

Command	**secondary-sta** *mac-address*

Parameter Description	*mac-address*: indicates the MAC address of the STA.
Defaults	No secondary STA is configured.
Command Mode	Package configuration mode
Usage Guide	N/A

Configuring an Association Control Domain

- (Mandatory) The configuration is performed on an AC.
- Configure an association control domain.
- APs can be added to an association control domain only after this association control domain is configured.

Command	**control-zone** *czone-name*
Parameter Description	*czone-name*: Indicates the name of an association control domain. The name is a string of 1 to 64 characters.
Defaults	No association control domain is configured.
Command Mode	Global configuration mode
Usage Guide	N/A

Adding an AP to an Association Control Domain

- (Mandatory) The configuration is performed on an AC.
- Add an AP to an association control domain.
- Association control can be performed on only APs that are added to the association control domain.

Command	**ap** *WORD*
Parameter Description	*WORD*: Indicates the name of an AP. The name is a string of 1 to 64 characters.
Defaults	No AP is added to an association control domain.
Command Mode	Association control domain configuration mode
Usage Guide	N/A

Enabling Association Control

- (Mandatory) The configuration is performed on an AC. The **assoc-control** command must be used to enable association control.
- Enable association control.

Command	**assoc-control**
Parameter Description	N/A
Defaults	Association control is disabled.

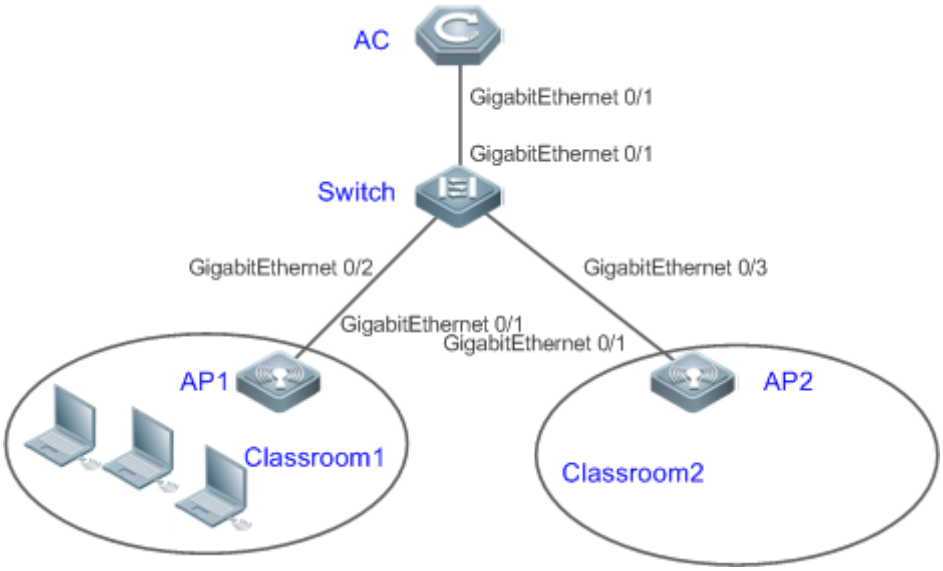
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Verify that secondary STAs can be associated with APs in the same group as the primary STA.

Configuration Example

Configuring the E-bag in Fit AP Architecture.

Scenario **Figure 1-8**	
Configuration Steps	● Configure packages and related primary STAs and secondary STAs. ● Configure association control domains and related APs. ● Enable association control.
AC	AC#configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# package Cart 1 AC(config-package)#primary-sta 00d0.f800.0001 AC(config-package)#secondary-sta 00d0.f800.0002 AC(config-package)#secondary-sta 00d0.f800.0003 AC(config-package)#exit AC(config)# control-zone Classroom 1 AC(config-czone)#apAP1 AC(config-czone)#exit AC(config)# control-zone Classroom 2 AC(config-czone)# apAP2 AC(config-czone)#exit

	AC(config)#assoc-control
Verification	● Display the association control running state. ● Display the package configuration. ● Display the association control domain configuration.
AC	AC#show assoc-control Association control is enabled. AC# show package total package num : 1 ========= Cart 1 ========= primary STA : 00d0.f800.0001 secondary STA num : 2 00d0.f800.0002 00d0.f800.0003 AC# show control-zone control zone num : 2 control-zoneAP ------------ ---------- Classroom 1 AP1 00d0.f800.889e Classroom 2 AP2 00d0.f800.889f

Common Errors

- N/A

1.4.7 Configuring STA Management

Configuration Effect

- STAs are disassociated if no traffic is detected on the STAs within the specified time.

Notes

- N/A

Configuration Steps

↘ Configuring the STA Aging Time

- (Optional) The configuration is performed on an AC.
- A shorter aging time indicates that a STA without traffic can be detected and disassociated in a faster manner.

Command	**sta-idle-timeout** *timer-num*
Parameter Description	*timer-num*: Indicates the aging time, in seconds. The value ranges from 60 to 64,000.

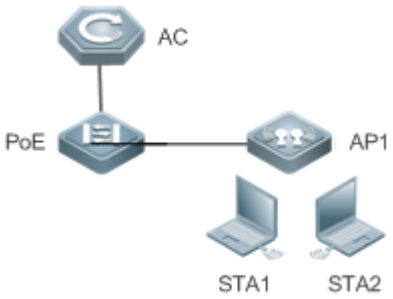
Defaults	300s
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Check whether the STA aging time is successfully configured.

Configuration Example

Configuring the STA Aging Time

Scenario **Figure 1-9**	
Configuration Steps	● Configure the STA aging time.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ap-config ap1 AC(config-ap)# sta-idle-timeout 15
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the configuration.
AC	AC# show ap-config running ap-config ap1 sta-idle-timeout 15 !

Common Errors

- N/A

1.4.8 Configuring STA Informational Syslog Suppression

Configuration Effect

- Even though STAs are frequently associated or disassociated, the number of informational syslogs output per second does not exceed the limit.

Notes

- N/A

Configuration Steps

Configuring the Syslog Suppression Rate

- (Optional) The configuration is performed on the AC.
- Configure the syslog suppression rate. A larger rate indicates that more syslogs can be output per second.

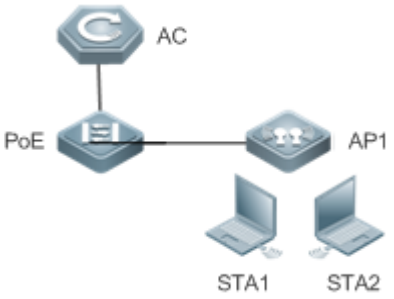
Command	**sta-logging rate-limit** *limit-num*
Parameter Description	*limit-num*: Indicates the rate, in entries per seconds. The value ranges from 0 to 10,000.
Defaults	Less than five syslogs are output per second, that is, the maximum syslog output rate is 5 entries per second.
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

- Run the **show running** command to check whether the syslog suppression rate is successfully configured.

Configuration Example

Configuring STA Informational Syslog Suppression

Scenario **Figure 1-10**	
Configuration Steps	● Configure STA informational syslog suppression.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-logging rate-limit 50
Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the configuration.
AC	AC# show running ac-controller sta-logging rate-limit 50 !

Common Errors

- N/A

1.4.9 Configuring Intelligent SSID Hiding

Configuration Effect

- When the number of STAs on an AP or a radio reaches the upper limit, new STAs cannot detect the SSID.

Notes

- This function takes effect only when both the AC and AP versions support this function.

Configuration Steps

↘ Enabling Intelligent SSID Hiding

- (Optional) The configuration is performed on an AC.
- Enable intelligent SSID hiding.

Command	**hide-ssid sta-reach-limit** [**radio** { **2.4g** | **5g** | **6g** }]
Parameter Description	**radio**: Indicates a specific radio on which intelligent SSID hiding is enabled. If this parameter is not specified, intelligent SSID hiding is enabled on all radios. **2.4g**: Indicates that intelligent SSID hiding is enabled on the 2.4 GHz radio.

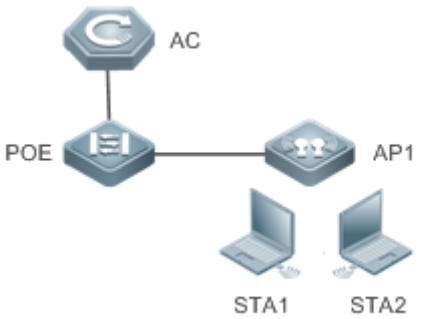
	5g: Indicates that intelligent SSID hiding is enabled on the 5 GHz radio. **6g**: Indicates that intelligent SSID hiding is enabled on the 6 GHz radio.
Defaults	Intelligent SSID hiding is disabled.
Command Mode	AP configuration mode
Usage Guide	After intelligent SSID hiding is enabled and the numbers of STAs on all APs in an area reach the upper limit, new STAs cannot detect the SSID in this area. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Verification

- Run the **show running or show ap-config running** command to check the configuration.

Configuration Example

Enabling the Intelligent SSID Hiding Function

Scenario **Figure 1-2**	
Configuration Steps	● Enable intelligent SSID hiding.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# ap-config AP1`
	`AC(config-ap)# hide-ssid sta-reach-limit`

Verification	● After the CAPWAP tunnel is established between an AP and an AC, check the configuration.

AC	`AC# show ap-config running AP1`
	`ac-config AP1`
	` hide-ssid sta-reach-limit`
	`!`

Common Errors

The AC version supports the intelligent SSID hiding function but the AP version does not.

1.4.10 Configuring STA Jitter Prevention

Configuration Effect

- When STA jitter prevention is enabled for a WLAN and a STA is disassociated from the WLAN, the AC retains a STA entry for a period of time before forcing the STA to go offline.

Notes

- When an AC or authentication server proactively forces a STA to go offline, the STA jitter prevention function does not take effect.

Configuration Steps

↘ Enabling STA Jitter Prevention

- (Mandatory) Enable STA jitter prevention on the AC.

Command	**prevent-jitter enable**
Parameter Description	N/A
Defaults	STA jitter prevention is disabled.
Command Mode	WLAN configuration mode
Usage Guide	When STA jitter prevention is enabled for a WLAN and a STA is disassociated from the WLAN, the AC retains a STA entry for a period of time (60s by default) before forcing the STA to go offline.

↘ Configuring the STA Jitter Prevention Time

- (Optional) Configure the STA jitter prevention time on the AC.

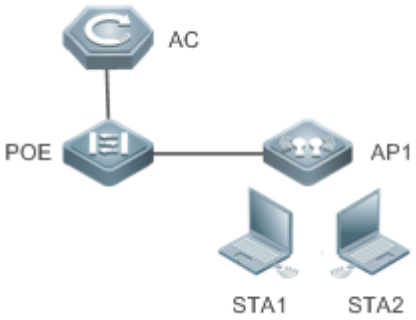
Command	**prevent-jitter time** *keep-time*
Parameter Description	*keep-time*: indicates the STA jitter prevention time, in seconds. The value ranges from 1 to 8,6400.
Defaults	60s
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run the **show running** or **show ap-config running** command to check the configuration.

Configuration Example

↘ Enabling STA Jitter Prevention

Scenario **Figure 1-11**	
Configuration Steps	● Enable STA jitter prevention.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# wlan-config 1`
	`AC(config-wlan)# prevent-jitter enable`

Verification	● Check the configuration.

AC	`AC# show running-config`
	`wlan-config 1 SSID`
	` prevent-jitter enable`
	`!`

Common Errors

- N/A

1.4.11 Configuring the Syslog Format upon STA Association

Configuration Effect

- When this command is configured, the syslog output will be in the configured format when a STA goes online and obtains an IP address.

Notes

- N/A

Configuration Steps

↘ Configuring the Syslog Format

- (Mandatory) The configuration is performed on an AC.

Command	**sta-logging mac-fmt-line**

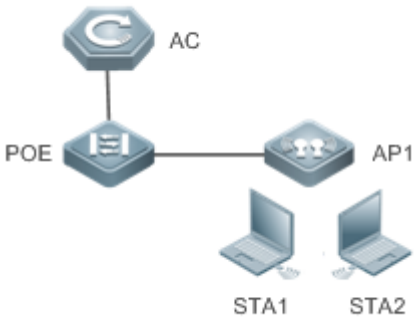
Parameter Description	N/A
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	The default syslog format for obtaining IP address when a STA comes online is: User Online, MAC Address 0001.2fe1.5022, AP Name *name,* base radio MAC: 0074.9c5b.288a, IP address 192.168.1.1, SSID: test. The syslog format after the command is configured is: CLIENT_ONLINE: UserIP=192.168.1.1, UserMAC=00-01-2F-E1-50-22, APMAC=00-74-9C-5B-28-85.

Verification

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

Configuration Example

Configuring the Syslog Format upon STA Association

Scenario Figure 1-3	
Configuration Steps	● Configure the syslog format when a STA goes online.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-logging mac-fmt-line
Verification	● Display the configuration.
AC	AC# show running ac-controller sta-logging mac-fmt-line !

Common Errors

- N/A

1.4.12 Enabling Fast STA Association

Configuration Effect

- When the fast association feature is enabled for a STA, the AC does not need to wait for the AP to add the STA response and can directly process the next association request when the STA goes online.

Notes

- N/A

Configuration Steps

Configuring Fast Association

- (Optional) The configuration is performed on the AC.

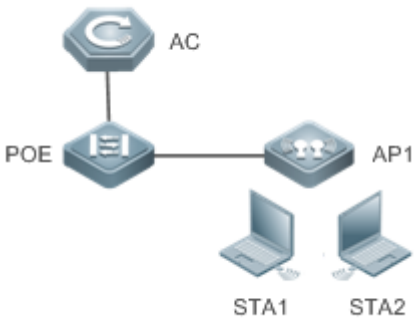
Command	**sta-behaviour fast-assoc**
Parameter Description	N/A
Defaults	Disabled
Command Mode	AC configuration mode
Usage Guide	By default, when STA goes online, the AC will wait for the response packet from AP before processing the next STA's association request packet. After this command is configured, there is no need to wait, avoiding message blocking in high-concurrency situations.

Verification

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

Configuration Example

Enabling Fast Association

Scenario **Figure 1-4**	
Configuration Steps	● Enable fast association.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z.

	AC(config)# ac-controller AC(config-ac)# sta-behaviour fast-assoc
Verification	● Display the configuration.
AC	AC# show running ac-controller sta-behaviour fast-assoc !

Common Errors

- N/A

1.4.13 Enabling IP Address Detection

Configuration Effect

- When IP address detection is enabled, a STA will be disconnected if it fails to obtain an IP address.

Notes

- N/A

Configuration Steps

↘ Configuring IP Address Detection

- (Mandatory) The configuration is performed on an AC.

Command	**sta-behaviour ip-check enable**
Parameter Description	N/A
Defaults	Enabled
Command Mode	AC configuration mode
Usage Guide	After configuration, IP address detection will be enabled. A STA will be disconnected if it doesn't have an IP address.

- (Optional) The configuration is performed on an AC.

Command	**sta-behaviour ip-check delay** *time*
Parameter Description	*time*: Indicates the delay, in seconds. The minimum value is 1s and the maximum value is 60s.
Defaults	30s
Command Mode	AC configuration mode
Usage Guide	After configuration, IP address detection will be delayed for the specified time. If the delay for IP address detection is set to 0, IP address detection is disabled.

- (Optional) The configuration is performed on an AC.

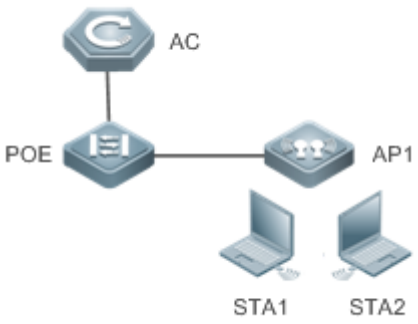
Command	**sta-behaviour ip-check sulk** *time*
Parameter Description	*time*: Indicates the quiet period, in seconds. The minimum value is 0s and the maximum value is 86,400s.
Defaults	600s
Command Mode	AC configuration mode
Usage Guide	If a STA is disconnected due to IP address detection, IP address detection will not be performed during the quiet period.

Verification

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

Configuration Example

Enabling IP Address Detection

Scenario **Figure 1-5**	
Configuration Steps	● Enable IP address detection. Set the delay for IP address detection of STAs to 20s and the quiet period to 300s within which IP address detection is not performed for a STA after it is disconnected due to IP address detection.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-behaviour ip-check enable AC(config-ac)# sta-behaviour ip-check delay 20 AC(config-ac)# sta-behaviour ip-check sulk 300
Verification	● Display the configuration.
AC	AC# show running sta-behaviour ip-check delay 20 sta-behaviour ip-check sulk 300 !

Common Errors

- N/A

1.4.14 Enabling DHCP Proxy

Configuration Effect

- After this command is configured, the AC will initiate DHCP Discover packets, interact with the server, and generate snooping entries on the AC on behalf of a STA, eliminating the need for the STA to participate in this process.

Notes

- N/A

Configuration Steps

↘ Enabling DHCP Proxy

- (Optional) The configuration is performed on an AC.

Command	**sta-behaviour dhcp-proxy enable**
Parameter Description	N/A
Defaults	Disabled
Command Mode	AC configuration mode
Usage Guide	After this command is configured, DHCP proxy will be enabled.

- (Optional) The configuration is performed on an AC.

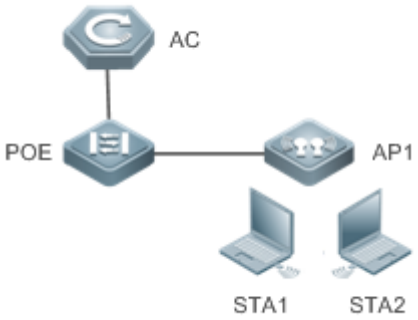
Command	**sta-behaviour dhcp-proxy delay** *time*
Parameter Description	*time*: Indicates the delay, in seconds. The minimum value is 1s and the maximum value is 60s.
Defaults	5s
Command Mode	AC configuration mode
Usage Guide	After this command is configured, DHCP proxy will be delayed for the specified time.

Verification

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

Configuration Example

↘ Enabling DHCP Proxy

Scenario **Figure 1-6**	
Configuration Steps	● Enable DHCP proxy and set the delay to 20s.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# ac-controller AC(config-ac)# sta-behaviour dhcp-proxy enable AC(config-ac)# sta-behaviour dhcp-proxy delay 20
Verification	● Display the configuration.
AC	AC# show running sta-behaviour dhcp-proxy enable sta-behaviour dhcp-proxy delay 20 !

Common Errors

- N/A

1.4.15 Configuring Wireless STA Management

Configuration Effect

- Delete the MAC address of a specified wireless STA.

Notes

- N/A

Configuration Steps

↘ Deleting the MAC Address of a Specified Wireless STA

- (Optional) The configuration is performed on an AC.

Command	**client-kick** *sta-mac*
Parameter	*sta-mac*: Indicates the MAC address of a wireless STA.

Description	
Defaults	N/A
Command Mode	AC configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

Deleting the MAC Address of a Specified Wireless STA

Configuration Steps	The following example deletes the wireless STA with the MAC address aaaa.bbbb.cccc.
	`Hostname(config)# ac-controller` `Hostname(config-ac)# client-kick aaaaa.bbbbb.ccccc`

Common Errors

- N/A

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show ac-config client [**by-ap-name** | **802.11a** | **802.11b** | **802.11n** | **802.11g** | **802.11ac** | **802.11ax** | **other**]	Displays the information about all STAs connected to the AC.
show ac-config client detail *mac-address*	Displays the detailed information about a specified STA.
show ac-config client statistic	Displays the statistics of all STAs.
show ac-config flow-balance summary	Displays the detailed configuration of the traffic-based balancing group.
show ac-config num-balance summary	Displays the detailed configuration of the number-based balancing group.
show assoc-control	Displays the status of the association control function.
show control-zone [**summary** | *czone-name*]	Displays the association control domain configuration.
show package [*pkt-name*]	Displays the package configuration.
show sta-blacklist	Displays the STAs in the blocklist.
show ac-config client hot-backup	Displays the backup information of a STA.

Debugging

N/A

1 Configuring VIP-FIRST

1.1 Overview

VIP-FIRST is a function used to improve the wireless user experience, including preferred access and independent rate limiting for VIP users.

Preferred access for VIP users ensures that VIP users can access the network at any time without being affected by the STA-LIMIT function. When a wireless user accesses the network, the MAC address of the wireless user is used to determine whether it is a VIP user.

Independent rate limiting for VIP users indicates that an independent rate limit can be configured for VIP users to prevent them being affected by the global rate limit.

1.2 Applications

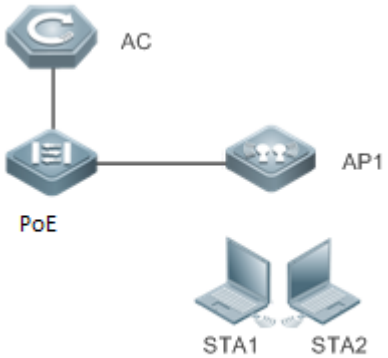
Application	Description
VIP-FIRST in Fit AP Networking	Fit AP networking is adopted, including at least one AC and one AP.

1.2.1 VIP-FIRST in Fit AP Networking

Scenarios

On a wireless network, an AC is deployed with preferred access and independent rate limiting enabled for VIP users. The VIP user list is uploaded to a specific directory on the AC, and the **import** command is run to advertise the AC to parse the VIP user list.

Figure 1-1



Remarks	AC: Indicates a wireless access controller. PoE: Indicates a switch used as the gateway of the AP. AP: Indicates a wireless access point. STA1 and STA2: Indicates two wireless clients.

Deployment

- Enable the VIP-FIRST function on the AC.

1.3 Features

Basic Concepts

Preferred Access for VIP Users

In scenarios where a large number of users access the network, good user experience cannot be guaranteed for each user. If the number of users on the AC, WLAN, AP, or radio exceeds the limit specified by the STA-LIMIT function, preferred access for VIP users allows VIP users to access the network and disconnects non-VIP users with poor communication quality.

Independent Rate Limiting for VIP Users

In scenarios where a large number of users access the network, good user experience cannot be guaranteed for each user. In addition to the global rate limit, an independent rate limit is configured for VIP users to ensure that the bandwidth of VIP users is higher than that of non-AP users.

Overview

Feature	Description
Preferred Access for VIP Users	Ensures that VIP users can access the network at any time.
Independent Rate Limiting for VIP Users	Ensures that the bandwidth of VIP users is higher than that of non-VIP users.

1.3.1 Preferred Access for VIP Users

Preferred access for VIP users ensures that VIP users can access the network anytime without being affected by the STA-LIMIT function.

Working Principle

If the number of users on the AC, WLAN, AP, or radio exceeds the limit specified by the STA-LIMIT function, non-VIP users with poor communication quality will be disconnected to ensure that VIP users can access the network.

1.3.2 Independent Rate Limiting for VIP Users

In addition to the global rate limit, an independent rate limit is configured for VIP users to ensure that the bandwidth of VIP users is higher than that of non-VIP users.

Working Principle

When the global rate limit is configured, a higher independent rate limit is configured for VIP users.

1.4 Configuration

Configuration	Description and Command	
Configuring VIP User Parsing or Deletion	⚠ (Mandatory) It is used to advertise the AC to parse the VIP user list.	
	vip-first import	Advertises the AC to parse the VIP user list.
	⚠ (Optional) It is used to advertise the AC to delete the VIP user list.	
	vip-first clear	Clears the VIP user list from the AC.
Configuring Preferred Access for VIP Users	⚠ (Mandatory) It is used to enable preferred access for VIP users.	
	vip-first prior-assoc	Enables preferred access for VIP users on the AC.
Common Errors N/A	⚠ (Mandatory) It is used to enable independent rate limiting for VIP users.	
Configuring Independent Rate Limiting for VIP Users	**vip-first rate-limit**	Configures the uplink and downlink rate limits for VIP users on the AC.

1.4.1 Configuring VIP User Parsing or Deletion

Configuration Effect

- Advertise the AC to parse or delete the VIP user list.

Notes

- Upload the VIP user list file to the **flash** directory and then run the **import** command to advertise the AC to parse the VIP user list. It takes several to dozens of seconds for the AC to parse the VIP user list.
- The VIP user list file is named **vip_user_list.txt**.
- The **clear** command will delete VIP users and the VIP user list file cached on the AC.
- The VIP user parsing or deletion command is not saved.

Configuration Steps

↘ **Advertising the AC to Parse the VIP User List**

- Mandatory.

- Run the **vip-first import** command in global configuration mode on the AC.

Command	vip-first import
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show vip-first user** command to check whether a user is a VIP user.

↘ Advertising the AC to Delete the VIP User List

- Optional.
- Run the **vip-first clear** command in global configuration mode on the AC.

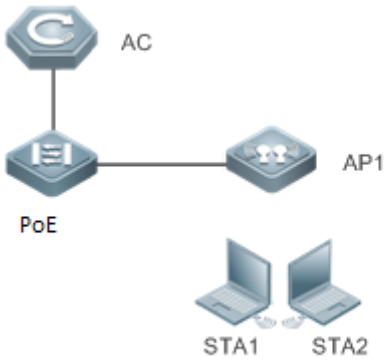
Command	vip-first clear
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **dir** command to check whether the **vip_user_list.txt** file exists.

Configuration Example

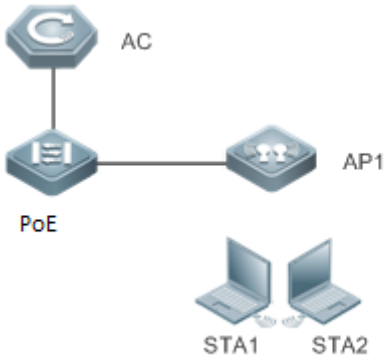
↘ Advertising the AC to Parse the VIP User List

Scenario **Figure 1-2**	
Configuration Steps	● Advertise the AC to parse the VIP user list in global configuration mode.
AC	`Hostname#configure terminal` `Hostname(config)# vip-first import`
Verification	Run the **show vip-first user** command to display configuration.

AC	`AC_20_3F#show vip-first user 0000.0000.0001`
	`STA_MAC YES/NO`
	`------------ ------`
	`0000.0000.0001 YES`

Configuration Example

Deleting the VIP User List

Scenario **Figure 1-3**	
Configuration Steps	● Advertise the AC to delete the VIP user list in global configuration mode.
AC	`Hostname#configure terminal` `Hostname(config)# vip-first clear`
Verification	Check whether the **vip_user_list.txt** file exists in the **flash** directory.

AC	AC_20_3F# dir Number Properties Size Time Name ------ ---------- ------ ------------------------ -------------------- 1 drwx 160B Tue Apr 25 08:39:38 2017 dev 2 drwx 160B Thu Nov 24 18:06:41 2016 rep 3 drwx 224B Thu Nov 24 18:06:42 2016 var

Common Errors

- The **vip-first import** command is run to advertise the AC to parse the VIP user list before the **vip_user_list.txt** file is uploaded to the AC.

1.4.2 Configuring Preferred Access for VIP Users

Configuration Effect

- Enable VIP users to access the network anytime without being affected by the STA-LIMIT function.

Notes

- The function can be configured only in global configuration mode on the AC.

Configuration Steps

↘ Enabling Preferred Access for VIP Users

- Mandatory.
- Run the **vip-first prior-assoc** command in global configuration mode on the AC.
- Enable preferred access for VIP users to ensure that VIP users can access the network anytime without being affected by the STA-LIMIT function.

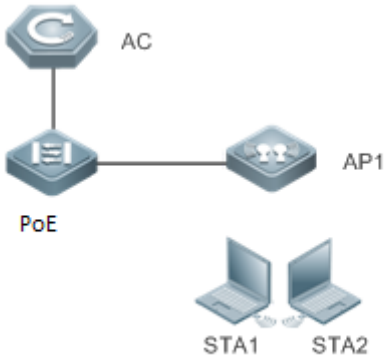
Command	**vip-first prior-assoc**
Parameter Description	N/A
Defaults	Preferred access for VIP users is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Enabling Preferred Access for VIP Users

Scenario **Figure 1-4**	
Configuration Steps	• Enable preferred access for VIP users in global configuration mode on the AC.
AC	Hostname#configure terminal Hostname(config)# vip-first prior-assoc
Verification	Run the **show running-config** command to display configuration.
AC	Hostname# show ap-config running ! vip-first prior-assoc!

Common Errors

- N/A

1.4.3 Configuring Independent Rate Limiting for VIP Users

Configuration Effect

- Ensure that the bandwidth of VIP users is higher than that of non-VIP users.

Notes

- An independent rate limit can be configured for VIP users only after a global rate limit is configured. The VIP user rate limit must be greater than the global rate limit. The global rate limit takes effect for all users on the AC.

Configuration Steps

↘ Enabling Independent Rate Limiting for VIP Users

- Mandatory.
- Enable independent rate limiting in the global configuration mode on the AC.
- Enable independent rate limiting for VIP users to increase the bandwidth of VIP users.

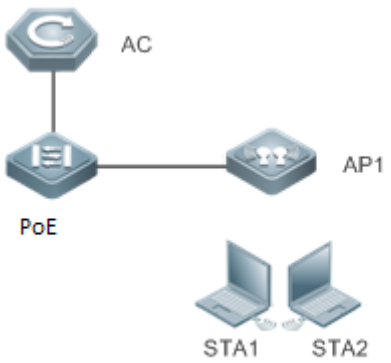
Command	**vip-first rate-limit** { **down-stream** | **up-stream** } **average-rate** *average-rate* **burst-rate** *burst-rate*
Parameter Description	**down-streams**: Sets the downlink rate limit of an AP. **up-streams**: Sets the uplink rate limit of an AP. *average-rate*: Sets the average rate limit. The unit is 8 kbps. The value range is **8** to **261,120**. *burst-rate*: Sets the burst rate limit. The unit is 8 kbps. The value range is **8** to **261,120**.
Defaults	Independent rate limiting for VIP users is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

↘ Enabling Independent Rate Limiting for VIP Users

Scenario **Figure 1-5**	
Configuration Steps	• Enable independent rate limiting for VIP users in global configuration mode on the AC.

AC	Hostname#configure terminal Hostname(config)# vip-first rate-limit up-stream average-rate 8 burst-rate 8 Hostname(config)# vip-first rate-limit down-stream average-rate 8 burst-rate 8
Verification	Run the **show ap-config running** command to display configuration.
AC	Hostname# showap-config running ! vip-first rate-limit up-stream average-rate 8 burst-rate 8 vip-first rate-limit down-stream average-rate 8 burst-rate 8 !

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show vip-first user { *mac* | **all** }	Checks whether a user is a VIP user.

Debugging

N/A

1 Configuring Hotspot 2.0

1.1 Overview

To implement automatic association and authentication on wireless local area networks (WLANs), automatic offloading of cellular network data, STA roaming between networks of different service providers, and effective management of authentication information, Wi-Fi Alliance releases the Hotspot 2.0 technical standard. Built on IEEE 802.11u standards, Hotspot 2.0 allows wireless STAs to perform automatic Wi-Fi identification and seamless handover without additional identity authentication, providing wireless users with cellular-like mobile experience.

Protocols and Standards

- IEEE 802.11u-2011
- Hotspot_2-0_(R2)_Technical_Specification_v1-1-0

1.2 Applications

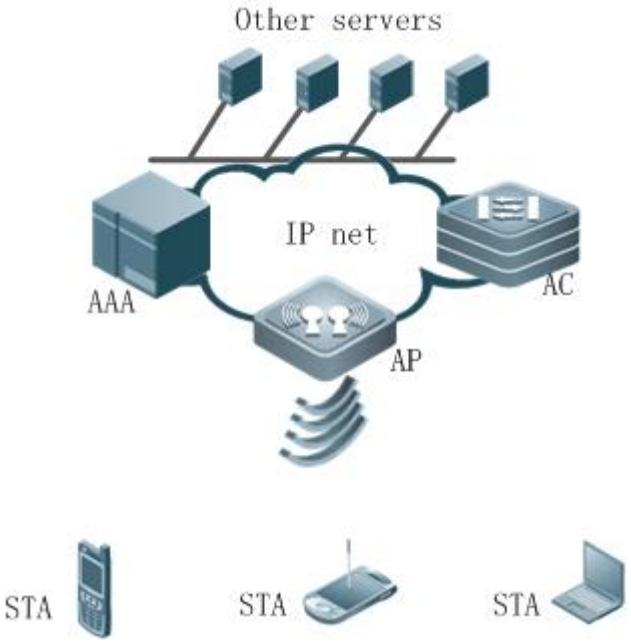
Application	Description
Self-Built Hotspot 2.0 Network	The service scope of a Hotspot 2.0 network that is not deployed by a service provider is small.
Hotspot 2.0 Network Built by a Service Provider	The service scope of a Hotspot 2.0 network deployed by a service provider is limited to the network.
Roaming Hotspot 2.0 Network	The service scope of Hotspot 2.0 networks deployed by multiple service providers can be extended across the Hotspot 2.0 networks.

1.2.1 Self-Built Hotspot 2.0 Network

Scenario

Entities other than service providers (such as shopping malls, train stations, and airports) deploy Hotspot 2.0 access networks to provide the Hotspot 2.0 service for STAs. The Hotspot 2.0 authentication service is available only on the Hotspot 2.0 access network.

Figure 1-1 Topology of a Self-Built Hotspot 2.0 Network



Remarks	AAA: Indicates an authentication, authorization, and accounting (AAA) server. AC: Indicates a wireless access controller. AP: Indicates a wireless access point. STA: Indicates a wireless access client. Other servers: Indicates other servers, such as email server and domain name system (DNS) server.

Deployment

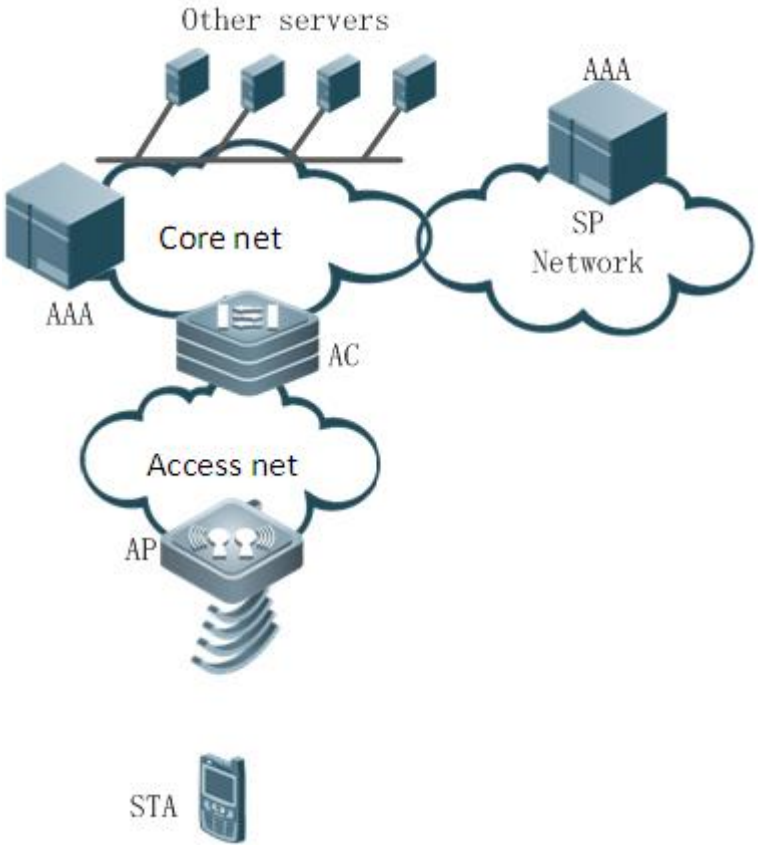
- Configure Hotspot 2.0 for the AP on the AC.
- Configure 802.1X authentication for the AP on the AC and configure the network-attached storage (NAS) device.
- Configure AAA authentication on the AAA server.
- Enable Hotspot 2.0 on STAs.

1.2.2 Hotspot 2.0 Network Built by a Service Provider

Scenario

A service provider deploys a Hotspot 2.0 network in a site to provide WLAN services. On the network, the access STAs are subscribers of the service provider and access authentication needs to be implemented by the service provider. In general, an internal AAA server is deployed in a site to simplify and implement hierarchical deployment. The internal AAA server is interconnected with the AAA server of a service provider for authentication.

Figure 1-2 Topology of a Hotspot 2.0 Network Deployed by a Service Provider



Remarks	AAA: Indicates an AAA server. AC: Indicates a wireless access controller. AP: Indicates a wireless access point. STA: Indicates a wireless access client. Other servers: Indicates other servers, such as email server and DNS server. SP Network: Indicates the network of a service provider.

Deployment

- Configure Hotspot 2.0 for the AP on the AC.
- Configure 802.1X authentication for the AP on the AC and configure the NAS device.
- Configure proxy authentication on the local AAA server and local authentication on the service provider's AAA server.
- Enable Hotspot 2.0 on STAs.

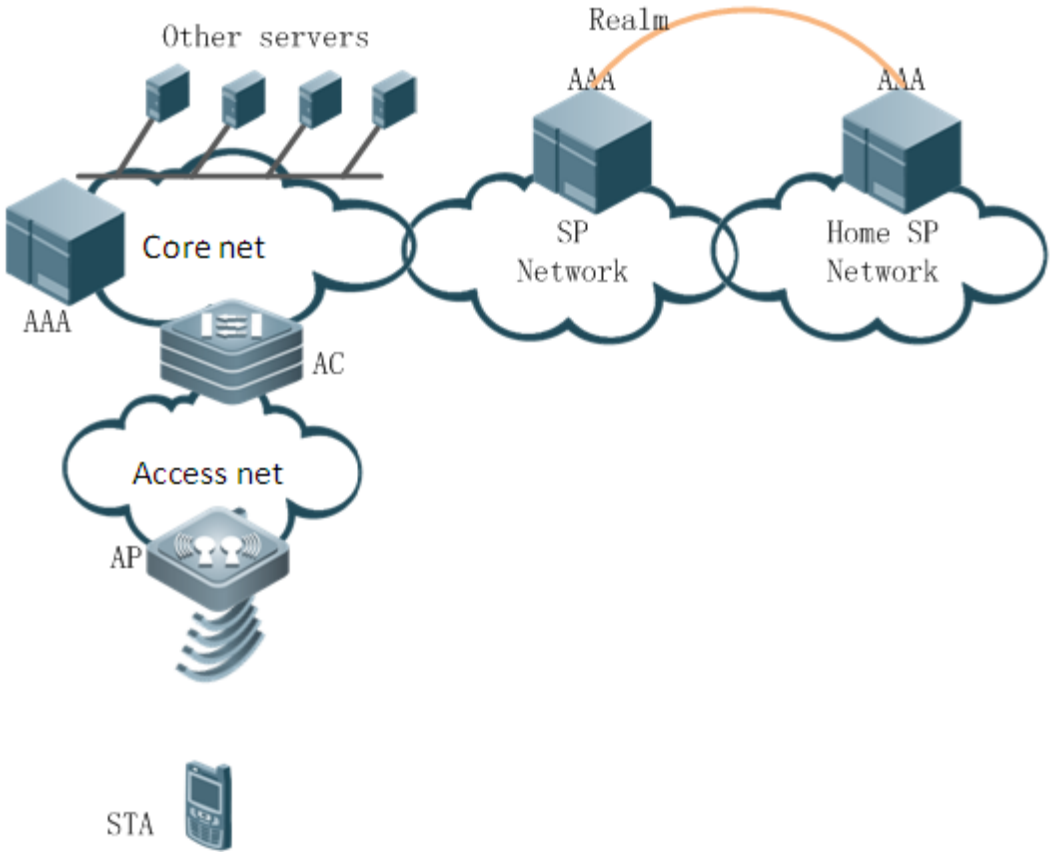
1.2.3 Roaming Hotspot 2.0 Network

Scenario

Multiple service providers deploy Hotspot 2.0 networks in some sites to provide WLAN services. The subscribers of different service providers can access the Internet on the Hotspot 2.0 networks of different service providers. To achieve this goal, different service providers need to enable wireless clients to roam between networks. The service providers'

AAA servers are used for subscriber authentication as a proxy, and routing and proxy authentication are performed through the realm.

Figure 1-3 Topology of a Roaming Hotspot 2.0 Network



Remarks	AAA: Indicates AAA servers, including the local AAA server, the AAA server of a service provider, and the AAA server of the home service provider. AC: Indicates a wireless access controller. AP: Indicates a wireless access point. STA: Indicates a wireless access client. Other servers: Indicates other servers, such as email server and DNS server. SP Network: Indicates the network of a service provider. Home SP Network: Indicates the network of the home service provider, that is, the service provider network to which a user subscribes.

Deployment

- Configure Hotspot 2.0 for the AP on the AC.
- Configure 802.1X authentication for the AP on the AC and configure the NAS device.
- Configure proxy authentication on the local AAA server, local authentication and proxy authentication on the service provider's AAA server, and local authentication on the home service provider's AAA server.
- Enable Hotspot 2.0 on STAs.

1.3 Features

Basic Concepts

Network Entity

STA: Indicates wireless stations with wireless network interface cards (NICs) such as laptops and mobile phones.

AP: Indicates a wireless access point that provides wireless signals for STA access.

AC: Indicates a wireless access controller that provides wireless connection and relevant services.

AAA: Indicates an AAA server.

OSUS: Indicates an online sign-up server that provides online sign-up service for Hotspot 2.0 STAs.

HLR: Indicates the home location register.

CA: (Optional) indicates the digital certificate authentication center server used to issue certificates to servers.

GAS, ANQP, and OSU

Generic Advertisement Service (GAS) is a mechanism defined by 802.11u through which the STA obtains network information by exchanging Request and Response packets with the network side.

Access Network Query Protocol (ANQP) is a network information query protocol encapsulated in GAS packets. ANQP defines the network parameters that are used to identify networks.

Online sign-up (OSU) provides a mechanism for STAs with no authentication information available on the AAA server to sign up online and obtain authentication information.

Overview

Feature	Description
Features of Hotspot 2.0	Hotspot 2.0 implements automatic WLAN association, online sign-up of users, automatic offloading of cellular traffic, and STA roaming between networks of different service providers.
Hotspot 2.0 Principle	Hotspot 2.0 network discovery, selection, and access process
GAS Principle	GAS principle and use
ANQP Principle	ANQP principle and use
Common Protocol Dictionary	Definitions of common dictionary used by protocols

1.3.1 Features of Hotspot 2.0

Hotspot 2.0 implements automatic STA access, online sign-up of users, automatic offloading of cellular traffic, and STA roaming between networks of different service providers.

Automatic Access

After the WLAN function is enabled on a STA, the STA automatically discovers and selects a Hotspot 2.0 network, connects to the network, and performs authentication for Internet access. Automatic access authentication eliminates the need for manual intervention, achieving cellular-like network access.

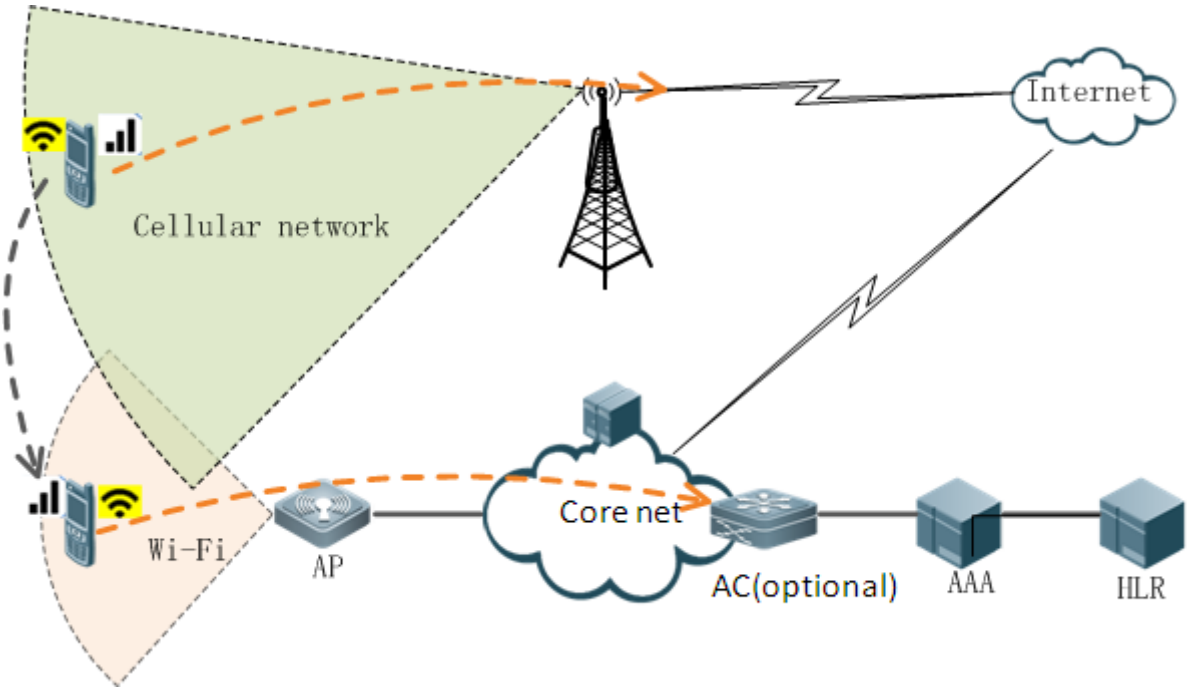
Online Sign-up

After a STA selects a Hotspot 2.0 WLAN, if the AAA server does not have the STA's access authentication information, you can choose online sign-up to submit identity information, obtain authentication information, and install identity information. After completion, the STA can be automatically authenticated for Internet access based on the installed identity information. The identity information sign-up and installation are completed by users independently and the process is simple.

Automatic Offloading of Cellular Traffic

A user initially accesses the Internet by using mobile data within the coverage of a cellular network. As the user moves to the coverage area of a Hotspot 2.0 WLAN, a STA automatically connects to the Hotspot 2.0 WLAN and accesses the Internet through the WLAN. If both mobile data and WLAN functions are enabled, the STA automatically selects WLAN first. You can also manually disable mobile data.

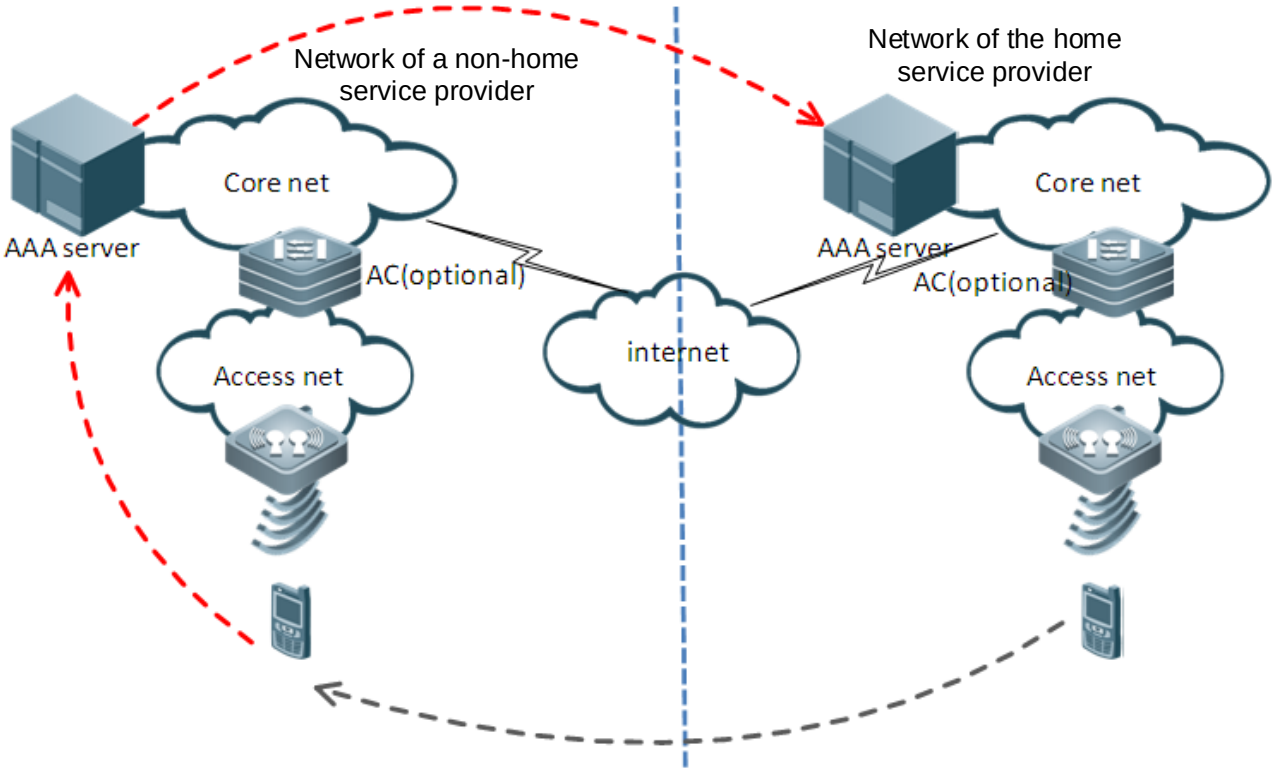
Figure 1-4 Automatic Offloading of Cellular Traffic



STA Roaming Between Networks of Different Service Providers

A user registers user information on the network of the home service provider and subscribes to the Hotspot 2.0 WLAN service. The user can connect to the Hotspot 2.0 WLAN for Internet access by using the registered authentication information. When the user moves to the Hotspot 2.0 WLAN of a non-home service provider, the user can still connect to the network for Internet access, eliminating the need to register identity information and obtain authentication credential.

Figure 1-5 STA Roaming Between Networks of Different Service Providers

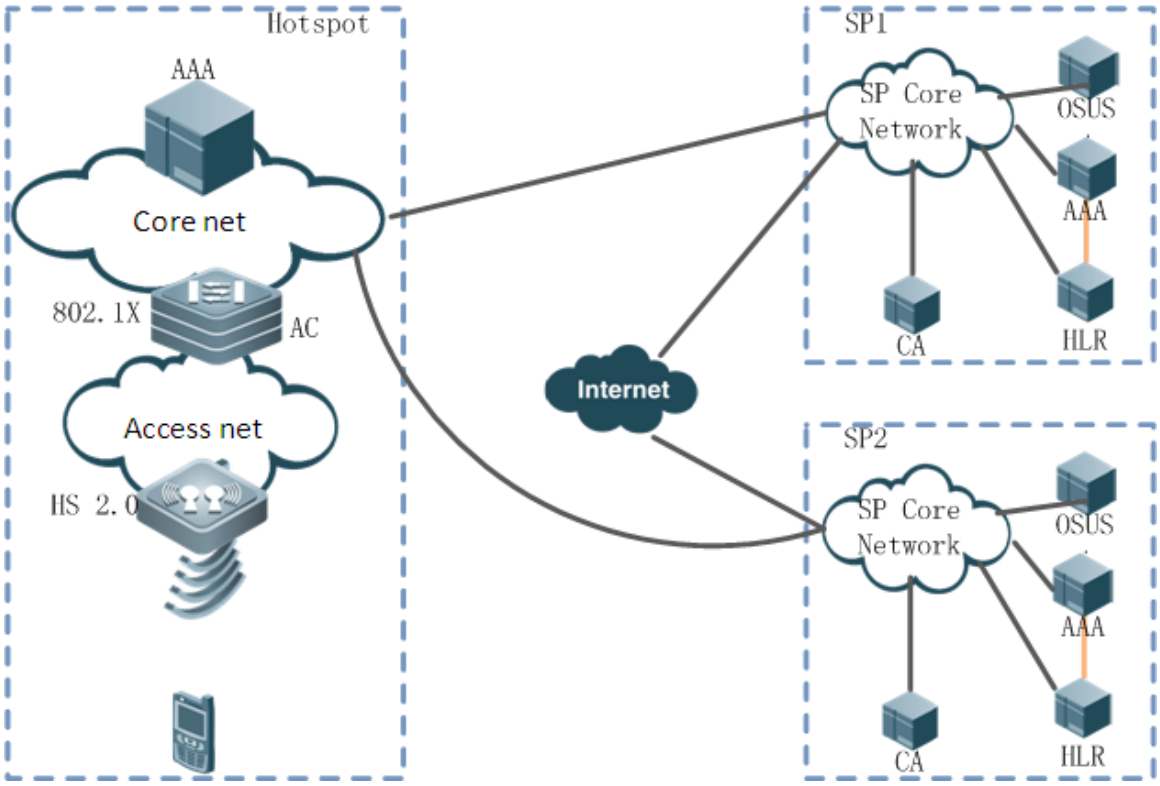


1.3.2 Hotspot 2.0 Principle

Network Architecture

The Hotspot 2.0 WLAN architecture can be divided into the Hotspot 2.0 WLAN access network and server cluster of service providers.

Figure 1-6 Hotspot 2.0 Network Architecture



Access Network of a Hotspot 2.0 WLAN

The AC manages APs in a unified manner and APs run Hotspot 2.0 for user access. The AC supports 802.1X authentication and interconnects with the AAA server on the Hotspot 2.0 network to implement user access authentication. The AAA server on the Hotspot 2.0 network serves as a proxy and interworks with service providers' AAA servers to complete the authentication. In the fat mode, APs are associated directly with the local AAA server for authentication.

Service Cluster of a Service Provider

Authentication on a service provider's network is managed by the service provider in a unified manner. After receiving authentication requests from a service provider's users, the AAA server on a Hotspot 2.0 network forwards the requests to the service provider's AAA server, and the service provider's AAA server returns authentication results to the AAA server on the Hotspot 2.0 network, which finally returns the results to access users to complete authentication.

If a user adopts SIM authentication, the service provider's AAA server interconnects with the service provider's HLR server to complete SIM authentication.

If an access user is not a subscriber of the current service provider but a subscriber of another service provider, roaming between networks of the service providers is required for authentication. The AAA server on the current network sends the authentication request of a user to the AAA server on the user's home network to implement authentication on the user. The AAA server on the user's home network returns the authentication result. If a user employs SIM authentication, the AAA server on the home network needs to interconnect with the HLR server on the home network to complete authentication.

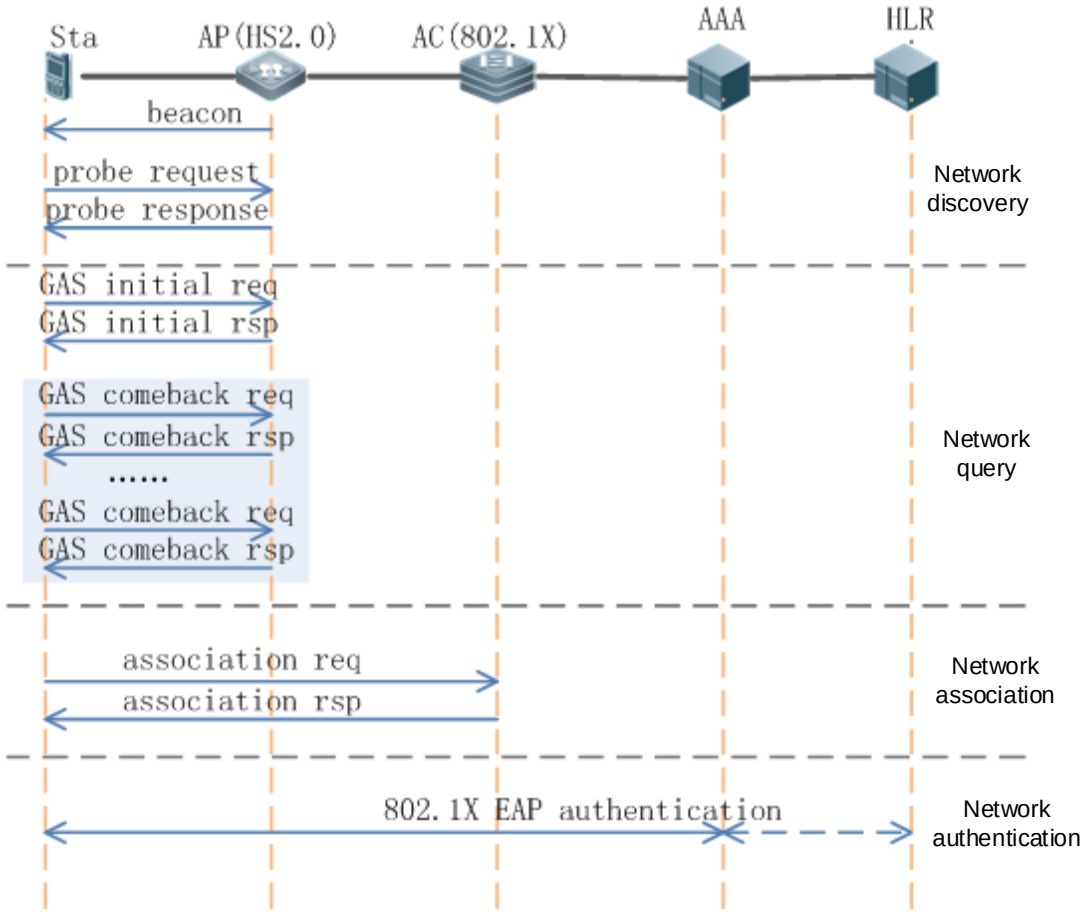
For STAs that have no authentication information on the AAA server upon first access, service providers offer OSU service for online sign-up as well as authentication information downloading and installation. Then, the STAs can access the Hotspot 2.0 network by using the registered authentication information.

Network Access Process

Hotspot 2.0 is implemented based on IEEE 802.11u standards. IEEE 802.11u defines a mechanism for STAs to obtain WLAN information. In roaming or non-roaming scenarios, STAs can discover a Hotspot 2.0 WLAN through Beacon or Probe frames and obtain detailed WLAN information through GAS frames. Based on the received WLAN information, the STAs automatically select the optimal WLAN network to access, where the STAs will be automatically authenticated.

Network information exchange is achieved through GAS and ANQP packets on a Hotspot 2.0 WLAN.

Figure 1-7 Hotspot 2.0 Network Access



In general, the process of Hotspot 2.0 network access involves four phases: network discovery, network query, network association, and network authentication.

Network Discovery

A Hotspot 2.0 network can be discovered through passive or active scan, that is, by using Beacon frames and Probe frames. The principle is as follows: An AP sends a Beacon or Probe frame which contains the Hotspot 2.0 network

information elements to a STA. The STA parses information elements related to Hotspot 2.0 and then discovers a Hotspot 2.0 network.

Network Query

This phase is unique to Hotspot 2.0. After a STA discovers a Hotspot 2.0 network, it needs to obtain further information related to Hotspot 2.0 through GAS query. GAS Initial Request frame and GAS Initial Response frame are mandatory for GAS exchange between an AP and a STA. However, GAS Comeback Request and GAS Initial Response frame exchange are optional, which occur only when the requested response data needs to be fragmented or a response delay is set.

Network Association

The association process of a Hotspot 2.0 network is exactly the same as that of a traditional WLAN, except that the QoS MAP advertisement is added to the Association Response frame.

Network Authentication

Hotspot 2.0 networks adopt IEEE 802.1X authentication and the standard Extensible Authentication Protocol (EAP) method for STA authentication. Remote Authentication Dial-In User Service (RADIUS) options need to be extended to support Hotspot 2.0.

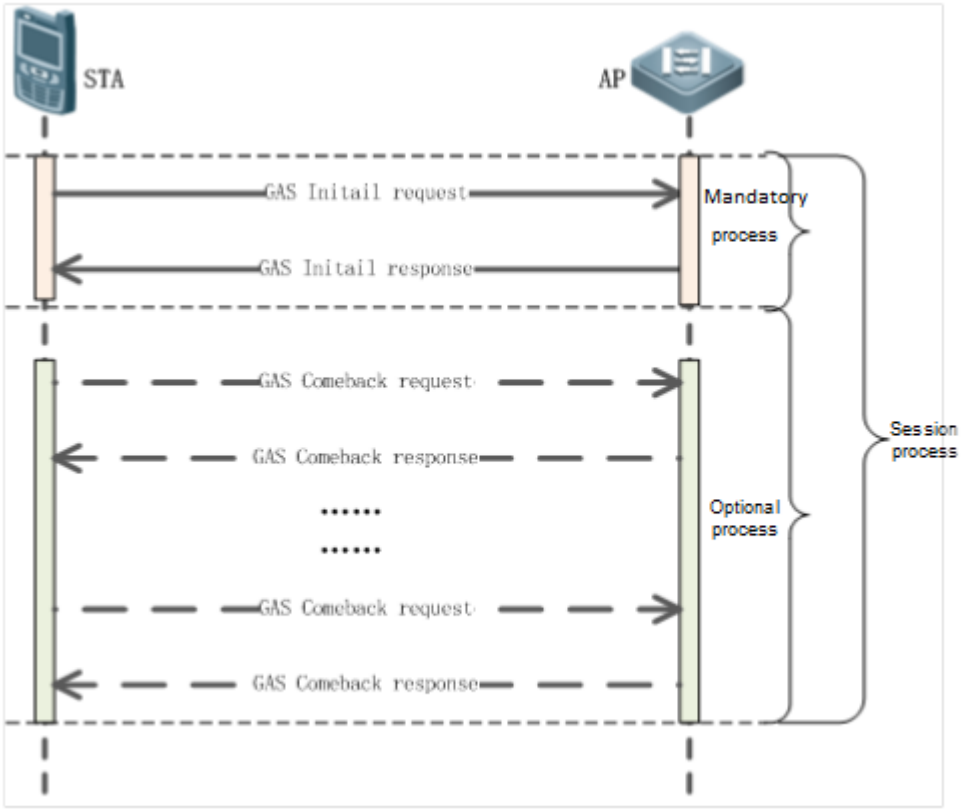
1.3.3 GAS Principle

Generic Advertisement Service (GAS) is a mechanism defined by 802.11u through which the STA obtains network information by exchanging Request and Response packets with the network side.

Protocol Exchange Process

GAS adopts the standard client/server mode, in which STAs serve as clients, an AP serves as the server, and the AP responds to STAs' requests. One GAS session exchange process includes the mandatory process and the optional process that is executed only when conditions are met. The mandatory process means the exchange between a STA and an AP through GAS Initial Request and GAS Initial Response frames, and this process is executed only once. The optional process is one or more exchanges using GAS Comeback Request and GAS Comeback Response frames. It is the continuation of the mandatory process. This process starts when the AP is required to delay obtaining response data or the response data exceeds the maximum data length of one-time response.

Figure 1-8 GAS Exchange Process



GAS Session Management

GAS session management includes session generation, session processing, and session termination.

Session Generation

A GAS session is identified by a STA + Dialog Token. The STA refers to the STA's MAC address, and Dialog Token is the Dialog Token in a GAS Initial Request frame.

A GAS session is generated upon the receiving of a GAS Initial Request frame. There are transient sessions and persistent sessions.

A transient session refers to a session that ends after a GAS Initial Request frame is received, the request is parsed, and all the response data is encapsulated into the GAS Initial Response frame at a time. The transient session adopts the mode of only one response to one request with simple logic.

The difference between a persistent session and a transient session lies in whether response data is encapsulated into one GAS Initial Response frame. If it is impossible to encapsulate response data into one response frame, the session becomes a persistent session. It can be said that a persistent session includes the transient session process. The only difference is that the GAS Initial Response frame of a transient session contains complete response data while a persistent session responds with an empty GAS Initial Response frame, and the valid data is captured in subsequent GAS Comeback exchange.

A GAS session enters the persistent session state when either of the following conditions is met:

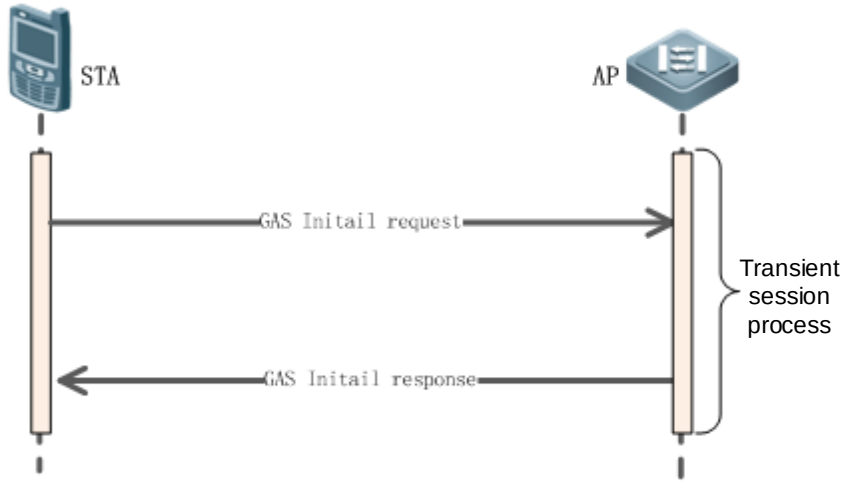
- GAS response delay is configured.

- The response content exceeds the maximum data length of a one-time response.

Session Processing

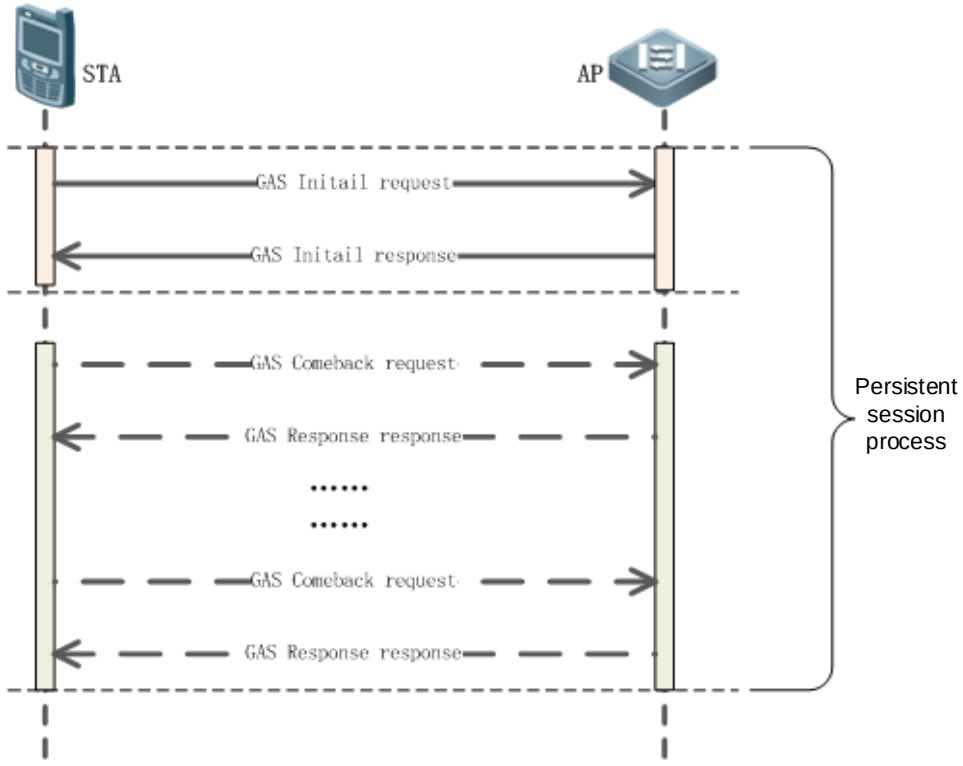
A transient session is very simple. One GAS Initial Request frame maps to one GAS Initial Response frame, and the whole session ends after one response is returned to one request.

Figure 1-9 GAS Transient Session



Compared with transient sessions, persistent sessions have the GAS Comeback exchange process. Data is only generated in the GAS Initial process, and the valid data exchange occurs in the GAS Comeback process.

Figure 1-10 GAS Persistent Session



Session Termination

A transient session is terminated after an AP replies a GAS Initial Response.

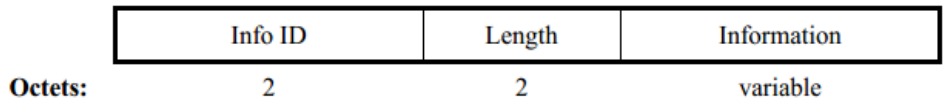
A persistent session may be terminated in the event of the following cases:

- The session ends normally, that is, all data is exchanged. The session ends after the last GAS Comeback exchange is completed.
- The session ends due to timeout. If no GAS Comeback Request is received within the timeout duration of a session (5 seconds by default), the session is terminated. If a GAS Comeback Request is received within the timeout duration, the timeout countdown is re-counted.
- A session ends due to other exceptions, for example, a session is released due to insufficient resources.

1.3.4 ANQP Principle

ANQP is carried over GAS and GAS uses ANQP for information encapsulation. The GAS service is usually called the ANQP service and the GAS server is also called the ANQP server. ANQP encapsulates messages in the TLV (ID, length, and value) format.

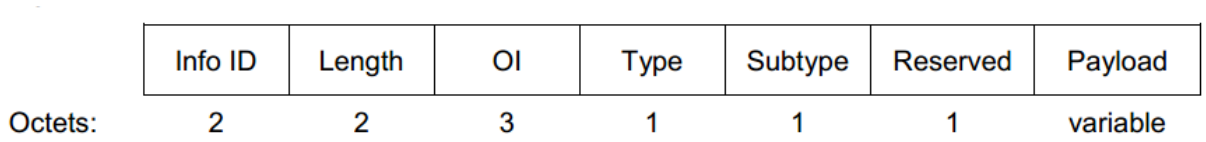
Figure 1-11 Standard Message Format of ANQP



	Info ID	Length	Information
Octets:	2	2	variable

The information element with info ID 56797 is an extended ANQP information element, which is used by Hotspot 2.0.

Figure 1-12 Extended ANQP Message Format of Hotspot 2.0



	Info ID	Length	OI	Type	Subtype	Reserved	Payload
Octets:	2	2	3	1	1	1	variable

The value of **Info ID** is fixed at **56797**. **Length** indicates the length of all data behind the element. **OI** indicates the organization ID and Wi-Fi Alliance uses 0x 506F9A. **Type** indicates the OI type and is set to **0x11**. **SubType** indicates the type of an extended information element. **Reserved** is a reserved field and the value is **0**. **Payload** indicates the content of the information element. It may contain sub-elements, which is also encapsulated in the TLV (ID, length, value) format.

Standard ANQP Options

Information Element	Info ID	Generated by	Description
ANQP Query list	256	STA	ANQP query list. A STA specifies the information to be queried in this information element and specifies the info ID to be queried in the request body.
ANQP Capability list	257	AP	ANQP capability list. It is a response to **ANQP Query list** and specifies the capability set of ANQP. It involves no specific parameter values.

Information Element	Info ID	Generated by	Description
Venue Name information	258	AP	Venue name. It is a response to **ANQP Query list**. There are zero or multiple names of BSS-related venues. If there is more than one venue name, they refer to the same venue name in different languages and the venue name information contains venue type information (venue group and venue type).
Network Authentication Type information	260	AP	Network authentication type. It is a response to **ANQP Query list**. The network authentication type here is actually the additional action required for users to access the network and can be set to the following: **0**: accepting the terms of use **1**: online registration **2**: HTTP/HTTPS redirection **3**: DNS redirection
Roaming Consortium list	261	AP	Roaming consortium list. It is a response to **ANQP Query list**. Each roaming member is represented by OI, which is arranged in the format of length, value.
IP Address Type Availability Information	262	AP	IP address type availability information. It is a response to **ANQP Query list** and indicates the availability of the IP service after a STA is associated with a WLAN. For IPv6 addresses, the values are as follows: **0**: unavailable; **1**: available; **2**: unknown. For IPv4 addresses, the values are as follows: **0**: unavailable; **1**: Public IPv4 addresses are available. **2**: Port-restricted IPv4 addresses are available. **3**: Single-NATed private IPv4 addresses are available. **4**: Double-NATed private IPv4 addresses are available. **5**: Single-NATed and port-restricted IPv4 addresses are available. **6**: Double-NATed and port-restricted IP addresses are available. **7**: unknown.
NAI Realm list	263	AP	NAI realm list. It is a response to **ANQP Query list** and contains the realm name and authentication mode.
3GPP Cellular Network information	264	AP	3GPP cellular network information. It is a response to **ANQP Query list**. It contains the cellular network ID to assist STAs in selecting an AP to access 3GPP networks. Cellular network information also includes a 3-bit mobile country code (MCC) and a 2-bit or 3-bit mobile network code (MNC).
Domain Name list element	268	AP	Operator domain name list. It is a response to **ANQP Query list**. It contains the domain name of a hotspot operator to assist STAs with network selection. A STA can obtain this information through ANQP query.

Extended ANQP Options of Hotspot 2.0

Information Element	Subtype	Generated by	Description
HS Query List element	1	STA	HS request list. A STA specifies the information to be queried in this information element and specifies the subtype ID to be queried in the request body.
NAI Home Realm Query element	6	STA	NAI home realm query. Through this information element, a STA requests an AP to query information about the home service provider network that has the STA's authentication information, to find out whether the STA has permission to access the local network. Multiple home service provider networks can be specified.
Icon Request element	10	STA	Sign-up icon request. Hotspot 2.0 supports the OSU service provider icon query by file name.
HS Capability List element	2	AP	HS capability list. It is a response to **HS Query List** and indicates the capability support. It involves no specific capability values.
Operator Friendly Name element	3	AP	Operator's friendly name. It is a response to **HS Query List**. If there are multiple pieces of operator information, it is information about the same operator in different languages.
WAN Metrics element	4	AP	WAN link status. It is a response to **HS Query List** and contains the following information: Status: down/up/test; symmetric or not; rate: uplink/downlink, symmetric link rate.
Connection Capability element	5	AP	IP protocol connection control. It is a response to **HS Query List**. It controls service ports and specifies whether to disallow or allow users to use IP services after access, including TCP, UDP, and ICMP.
OSU Providers List element	8	AP	OSU provider list. It is a response to **HS Query List** and provides online sign-up service for STAs, including OSU SSIDs. It can provide a list of OSU service providers and information about each provider includes the OSU provider name, description, OSU server URI, OSU method, OSU network access ID, and available icon file information.
Icon Binary File element	11	AP	Icon binary file content. It is a response to **Icon Request**.

1.3.5 Common Protocol Dictionary

Venue Type

Group	Group Description	Type	Type Description
0	Unspecified	0	Unspecified
1	Assembly	0	Unspecified
		1	Arena
		2	Stadium

		3	Passenger Terminal
		4	Amphitheater
		5	Amusement Park
		6	Place of Worship
		7	Convention Center
		8	Library
		9	Museum
		10	Restaurant
		11	Theater
		12	Bar
		13	Coffee Shop
		14	Zoo or Aquarium
		15	Emergency Coordination Center
2	Business	0	Unspecified
		1	Doctor or Dentist office
		2	Bank
		3	Fire Station
		4	Police Station
		6	Post Office
		7	Professional Office
		8	Research and Development Facility
		9	Attorney Office
3	Educational	0	Unspecified
		1	School, Primary
		2	School, Secondary
		3	University or College
4	Factory and Industrial	0	Unspecified
		1	Factory
5	Institutional	0	Unspecified
		1	Hospital
		2	Long-Term Care Facility
		3	Alcohol and Drug Rehabilitation Center
		4	Group Home
		5	Prison or Jail
6	Mercantile	0	Unspecified
		1	Retail Store
		2	Grocery Market
		3	Automotive Service Station
		4	Shopping Mall
		5	Gas Station
7	Residential	0	Unspecified
		1	Private Residence
		2	Hotel or Motel
		3	Dormitory

		4	Boarding House
8	Storage	0	Unspecified
9	Utility and Miscellaneous	0	Unspecified
10	Vehicular	0	Unspecified
		1	Automobile or Truck
		2	Airplane
		3	Bus
		4	Ferry
		5	Ship or Boat
		6	Train
		7	Motor Bike
11	Outdoor	0	Unspecified
		1	Muni-mesh Network
		2	City Park
		3	Rest Area
		4	Traffic Control
		5	Bus Stop
		6	Kiosk

1.4 Configuration

Configuration	Description and Command	
Configuring a Hotspot 2.0	(Mandatory) It is used to configure a Hotspot 2.0 profile.	
	hotspot2 template *template-name*	(Mandatory) Creates a Hotspot 2.0 profile.
	3gpp-cellular-network mcc *mcc* **mnc** *mnc*	(Optional) Configures a cellular network ID.
	network-auth-type {acceptance | online-enroll| http-https-redirection [redirect-url *url***] | dns-redirection }**	(Optional) Configures the network authentication type.
	osu-ssid *ssid*	(Optional) Configures an OSU SSID.
	venue-group *venue-group* **type** *venue-type*	(Optional) Configures the venue type.
	venue-name language-code *language-code* **name** *name*	(Optional) Configures the venue name.
	roam-consortium oi *oi* **[in-beacon]**	(Optional) Configures a roaming consortium.
	hessid *mac-address*	(Optional) Configures a homogeneous extended service set identifier (HESSID).
	domain-name *domain-name*	(Optional) Configures a hotspot operator domain name.
	network-type { emergency-service | personal-device | private | private-guest | public-chargeable | public-free | test | wildcard } [internet-access]	(Optional) Configures the network type.

	ipv4-address-available {not-available | public-available | port-restricted | single-nat | double-nat | port-restricted-single-nat | port-restricted-double–nat | unknown }	(Optional) Configures available IPv4 address types.
	ipv6-address-available { not-available | available | unknown }	(Optional) Configures available IPv6 address types.
	nai-realm realm-name *realm-name* **[eap-method-type [eap-ttls [auth-method** *auth-method-id* **auth-para** *auth-para-value* **] | eap-tls [auth-method** *auth-method-id* **auth-para** *auth-para-value* **] | eap-sim [auth-method** *auth-method-id* **auth-para** *auth-para-value* **] | eap-aka [auth-method** *auth-method-id* **auth-para** *auth-para-value* **] | eap-aka' [auth-method** *auth-method-id* **auth-para** *auth-para-value* **]]]**	(Optional) Configures a NAI realm member.
	connection-capability { esp | icmp | tcp-ftp | tcp-http | tcp-pptp-vpn | tcp-ssh | tcp-tls-vpn | tcp-voip | udp-ike2-4500 | udp-ike2-500| udp-voip } { enable | disable }	(Optional) Configures the IP protocol and port connection capability.
	dgaf {enable | disable }	(Optional) Enables or disables downstream group-addressed forwarding (DGAF).
	operator-name language-code *language-code* **name** *name*	(Optional) Configures an operator name.
	dls-tdls {enable | disable}	(Optional) Configures DLS connection control.
	osu-provider *template-name*	(Optional) Configures an OSU provider profile to be applied.
	gas-response delay {enable | disable}	(Optional) Enables GAS response delay.
	wan-metrics link-status {up | down | test} [asymmetric downlink-speed *downlink-speed* **uplink-speed** *uplink-speed* **| symmetric link-speed** *link-speed* **]**	(Optional) Configures the WAN port status.
Configuring an OSU Provider	⚠ (Optional) It is used to configure an OSU provider profile.	
	Hotspot2 osu-provider template *template-name*	(Mandatory) Creates an OSU provider profile.

	friendly-name language-code *language-code* **name** *name*	(Optional) Configures an OSU provider name.
	service-description language-code *language-code* **description** *description*	(Optional) Configures the OSU service description.
	server-uri *uri*	(Mandatory) Configures the OSU server URI.
	method {oma-dm | soap-xml-spp}	(Mandatory) Configures the OSU method.
	nai *nai*	(Optional) Configures the OSU network access ID.
	icon-name *name* **type {png | jpg | bmp | gif} language-code** *code* [**width** *width* **height** *height*]	(Optional) Configures an OSU icon.
Applying a Hotspot 2.0 Profile to a WLAN	⚠ (Mandatory) It is used to apply a Hotspot 2.0 profile to a WLAN.	
	Hotspot2 template *template-name*	Applies Hotspot 2.0 configuration in WLAN configuration mode of an AC.

1.4.1 Configuring a Hotspot 2.0 Profile

Configuration Effect

- Create a Hotspot profile and configure parameters in the profile. The configured Hotspot 2.0 profile can be applied and bound to a WLAN so that the WLAN supports the Hotspot 2.0 functions.

Notes

- Only existing Hotspot 2.0 profiles can be bound to a WLAN.

Configuration Steps

↘ Creating a Hotspot 2.0 Profile

- Mandatory.
- Create a Hotspot 2.0 profile and enter the Hotspot 2.0 configuration mode.

Command	**hotspot2 template** *template-name*
Parameter Description	*template-name*: Indicates the name of a profile. The value is a string of up to 32 case-sensitive visible characters excluding question marks (?) and spaces.
Defaults	No Hotspot 2.0 profile is configured.
Command Mode	Global configuration mode
Usage Guide	A maximum of 16 Hotspot 2.0 profiles can be configured and the profile names must be unique.

↘ Configuring a Cellular Network ID

- Optional.
- Configure a cellular network ID in the Hotspot 2.0 profile.

- A STA needs to obtain the 3GPP cellular public land mobile network (PLMN) ID from an AP so as to select the network for access. The cellular network ID is used to identify a cellular network and the cellular network information includes the 3-bit mobile country code (MCC) and 2-bit or 3-bit mobile network code (MNC).

Command	**3gpp-cellular-network mcc** *mcc* **mnc** *mnc*
Parameter Description	*mcc*: Indicates the 3-bit mobile country code. The value is a number in the range of 0 to 9. *mnc*: Indicates the 2-bit or 3-bit mobile network code. The value is a number in the range of 0 to 9.
Defaults	No cellular network ID is configured.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	A maximum of 16 cellular network IDs can be configured.

Configuring the Network Authentication Type

- Optional.
- Configure the network authentication type in the Hotspot 2.0 profile.
- A Hotspot 2.0-supported AP carries parameter information (additional steps required for access (ASRA)) in Beacon frames and Probe response frames to help STAs discover and select appropriate networks. If a network operator expects STAs to perform specified actions such as opening the specified web page for Portal authentication, the ASRA field needs to be set to **1** in the frames, indicating that additional authentication is required when STAs access the network. Then you can use this command to specify the network authentication mode. The network authentication type parameter exists only when ASRA is set to **1** in the **Interworking** field. The parameter must be set to **0** if RSNA is enabled.

Command	**network-auth-type {acceptance [redirect-url** *url***] | online-enroll | http-https-redirection [redirect-url** *url***] | dns-redirection }**
Parameter Description	*url*: Indicates the authentication redirection URL.
Defaults	No network authentication type is configured.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	A maximum of four authentication types can be configured.

Configuring an OSU SSID

- Optional.
- Configure an OSU SSID in the Hotspot 2.0 profile.
- When an OSU network access identifier (NAI) is provided, the OSU access network uses the OSEN mode. Otherwise, the OPEN mode is adopted. You are advised to hide OSU SSIDs to ensure security.

Command	**osu-ssid** *ssid*
Parameter Description	*ssid*: Indicates the OSU SSID. The value is a string of 1 to 32 characters.
Defaults	No OSU SSID is configured.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	Up to one OSU SSID can be configured. The repeated configuration will overwrite the previous

	configuration. Another WLAN needs to be deployed to implement access to the OSU network. The SSID of the WLAN must be the same as the configured OSU SSID. If an OSU NAI is configured, the OSEN access mode needs to be configured for the WLAN. Otherwise, the OPEN access mode needs to be configured.

Configuring the Venue Type

- Optional.
- Configure the venue type in the Hotspot 2.0 profile.
- Specify venue information to indicate the site information of the Hotspot 2.0 network.

Command	**venue-group** *venue-group* **type** *venue-type*
Parameter Description	*venue-group*: See Section 1.3.5 Common Protocol Dictionary. *venue-type*: See Sections 1.3.5 Common Protocol Dictionary.
Defaults	The group is not specified (the value is **0**) and the type is not specified (the value is **0**).
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	One venue group and one venue type can be configured at most.

Configuring the Venue Name

- Optional.
- Configure the venue name in the Hotspot 2.0 profile.
- If there are multiple venue names, they refer to the same venue name in different languages.

Command	**venue-name language-code** *language-code* **name** *name*
Parameter Description	*language-code*: The value is a string of 2 to 3 characters. It supports both ISO-639-1 and ISO-639-2 standards. If ISO-639-1 is adopted, **0** is added to ensure that the value contains three characters. *name*: The value is a string of 1 to 252 case-sensitive visible characters excluding question marks (?) and spaces.
Defaults	No venue name is configured.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	A maximum of eight venue names can be configured.

Configuring a Roaming Consortium

- Optional.
- Configure a roaming consortium in the Hotspot 2.0 profile.
- An operator identifier (OI) uniquely identifies a roaming member. It consists of six or ten characters in hexadecimal notation. **in-beacon** indicates that the OI needs to be added to the Beacon frame. A maximum of three OIs can be added to the Beacon frame. If this parameter is not specified, the OI is not added to the Beacon frame.

Command	**roam-consortium oi** *oi* **[in-beacon]**
Parameter Description	*oi*: Indicates the OI. The value is in the format of HH-HH-HH or HH-HH-HH-HH-HH. **H** is a 1-bit character in hexadecimal notation.
Defaults	No roaming consortium is configured.

Command Mode	Hotspot 2.0 configuration mode
Usage Guide	A maximum of 16 roaming consortium OIs can be configured.

(Optional) Configuring an HESSID

- Optional.
- Configure an HESSID in the Hotspot 2.0 profile.
- When multiple Hotspot 2.0 services exist on the network, a STA needs to identify the access service providers but SSIDs are not unique. Therefore, unique HESSIDs are used to identify APs of the same service provider. The HESSID is consistent with the BSSID of an AP. HESSID is an optional parameter in the Hotspot 2.0 profile. A Hotspot 2.0-supported AP carries parameter information in Beacon frames and Probe response frames to help STAs determine whether to obtain network parameters again.

Command	**hessid** *mac-address*
Parameter Description	*mac-address*: Indicates the HESSID in the format of HHHH.HHHH.HHHH. **H** is a 1-bit character in hexadecimal notation.
Defaults	No HESSID is configured.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	Up to one HESSID can be configured

Configuring a Hotspot Operator Domain Name

- Optional.
- Configure a hotspot operator domain name in the Hotspot 2.0 profile.
- After a hotspot operator domain name is configured, a STA can obtain the information through ANQP query to facilitate network selection.

Command	**domain-name** *domain-name*
Parameter Description	*domain-name*: Indicates a hotspot operator domain name. The value is a string of 1–255 characters and complies with RFC1035. It cannot contain question marks (?) and spaces. The string cannot end with double quotation marks (").
Defaults	No hotspot operator domain name is configured.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	A maximum of eight hotspot operator domain names can be configured.

Configuring the Network Type

- Optional.
- Configure the network type in the Hotspot 2.0 profile.
- When multiple Hotspot 2.0 services exist on a network, a STA needs to obtain information about the Hotspot 2.0 networks to select a network for access. A Hotspot 2.0-supported AP carries parameter information in Beacon frames and Probe response frames to help STAs discover and select appropriate networks.

Command	**network-type { emergency-service | personal-device | private | private-guest | public-chargeable |**

	public-free | test | wildcard } [internet-access]
Parameter Description	N/A
Defaults	The **network-type wildcard internet-access** command is configured and STAs can access the Internet.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	Up to one network type can be configured.

Configuring an Available IPv4 Address Type

- Optional.
- Configure an available IPv4 address type in the Hotspot 2.0 profile.
- When a STA accesses the Hotspot 2.0 service, Hotspot 2.0 can transfer the available IPv4 address type on the network as an ANQP parameter to the STA through an AP. In this way, the STA can know the type of an IP address that can be obtained after accessing the network.

Command	**ipv4-address-available** { **not-available** | **public-available** | **port-restricted** | **single-nat** | **double-nat** | **port-restricted-single-nat** | **port-restricted-double–nat** | **unknown** }
Parameter Description	N/A
Defaults	The available type of IPv4 addresses is set to **unknown**.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	Up to one available IPv4 address type can be configured.

Configuring an Available IPv6 Address Type

- Optional.
- Configure an available IPv6 address type in the Hotspot 2.0 profile.
- When a STA accesses the Hotspot 2.0 network, Hotspot 2.0 can transfer the available IPv6 address type on the network as an ANQP parameter to the STA through an AP. In this way, the STA can know the type of an IP address that can be obtained after accessing the network.

Command	**ipv6-address-available { not-available | available | unknown }**
Parameter Description	N/A
Defaults	The available type of IPv6 addresses is set to **unknown**.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	Up to one available IPv6 address type can be configured at most.

Configuring a NAI Realm Member

- Optional.
- Configure a NAI realm member in the Hotspot 2.0 profile.
- After a NAI realm member is configured, a STA can access the configured operator network.

Command	**nai-realm realm-name** *realm-name* [**eap-method-type** [**eap-ttls** [**auth-method** *auth-method-id* **auth-para** *auth-para-value*] | **eap-tls** [**auth-method** *auth-method-id* **auth-para** *auth-para-value*] | **eap-sim** [**auth-method** *auth-method-id* **auth-para** *auth-para-value*] | **eap-aka** [**auth-method** *auth-method-id* **auth-para** *auth-para-value*] | **eap-aka'** [**auth-method** *auth-method-id* **auth-para** *auth-para-value*]]]
Parameter Description	*realm-name*: Indicates the realm name of a NAI realm member. The value is a string of 1–252 visible characters and complies with RFC4282. It cannot contain question marks (?) and spaces, and the string cannot end with double quotation marks ("). *auth-method-id*: Indicates the authentication method. 2: **Non-EAP Inner Authentication Type**; 5: **Credential Type**; 6: **Tunneled EAP Method Credential Type** *auth-para*: Indicates authentication parameters. When **auth-method-id** is set to **2**, authentication parameters that can be configured are as follows: 1: **PAP**; 2: **CHAP**; 3: **MSCHAP**; 4: **MSCHAPV2** When **auth-method-id** is set to **5**, authentication parameters that can be configured are as follows: 1: **SIM**; 2: **USIM**; 3: **NFC Secure Element**; 4: **Hardware Token**; 5: **Softoken**; 6: **Certificate**; 7: **Username/password**; 8: **None***(server-side authentication only) When **auth-method-id** is set to **6**, authentication parameters that can be configured are as follows: 1: **SIM**; 2: **USIM**; 3: **NFC Secure Element**; 4: **Hardware Token**; 5: **Softoken**; 6: **Certificate**; 7: **Username/password**; 9: **Anonymous**
Defaults	No NAI realm member is configured.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	A maximum of 16 NAI realm members can be configured. Authentication parameters need to be configured based on the current user scenario to ensure that the configuration is consistent with the authentication environment. If the authentication environment is not specified, you can skip the authentication parameter configuration.

Configuring the IP Protocol and Port Connection Capability

- Optional.
- Configure the connection capability in the Hotspot 2.0 profile, including allowed IP protocols and ports of the network.
- Configure whether a Hotspot 2.0 network supports common IP protocols and ports.

Command	**connection-capability** { **esp** | **icmp** | **tcp-ftp** | **tcp-http** | **tcp-pptp-vpn** | **tcp-ssh** | **tcp-tls-vpn** | **tcp-voip** | **udp-ike2-4500** | **udp-ike2-500** | **udp-voip** } { **enable** | **disable** }
Parameter Description	N/A
Defaults	A Hotspot 2.0 network supports all IP protocols and ports.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	N/A

Configuring DGAF

- Optional.

- Configure DGAF in the Hotspot 2.0 profile.
- After the DGAF function is enabled on an AP, the AP forwards all downstream wireless broadcast ARP packets and wireless multicast packets. After the DGAF function is disabled, the AP discards all downstream wireless broadcast ARP packets and wireless multicast packets. Disabling DGAF can prevent attackers from forging group address frames and attacking clients by utilizing the vulnerability that all clients in the same BSS use the same group temporal key (GTK). If wireless broadcast ARP packets or wireless multicast packets need to be forwarded, you can enable proxy ARP before disabling DGAF.

Command	**dgaf {enable | disable }**
Parameter Description	N/A
Defaults	DGAF is enabled.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	N/A

Configuring the Operator Name

- Optional.
- Configure the operator name in the Hotspot 2.0 profile.
- If there are multiple operator names, they refer to the same operator name in different languages.

Command	**operator-name language-code** *language-code* **name** *name*
Parameter Description	*language-code*: The value is a string of 2 to 3 characters. It supports both ISO-639-1 and ISO-639-2 standards. If ISO-639-1 is adopted, **0** is added to ensure that the value contains three characters. *name*: The value is a string of 1 to 252 case-sensitive visible characters excluding question marks (?) and spaces.
Defaults	No operator name is configured.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	A maximum of eight operator names can be configured.

Configuring DLS Connection Control

- Optional.
- Configure DLS connection control in the Hotspot 2.0 profile.
- STAs in the same BSS cannot directly perform Layer 2 communication with each other, and Layer 2 packet detection and filtering are required for the communication. Hotspot 2.0 supports only DLS control and TDLS control.

Command	**dls-tdls {enable | disable}**
Parameter Description	N/A
Defaults	DLS and TDLS connections can be established between STAs.
Command Mode	Hotspot 2.0 configuration mode

Usage Guide	N/A

Configuring an OSU Provider Profile to Be Applied

- Optional.
- Configure an OSU provider profile to be applied in the Hotspot 2.0 profile.
- An OSU provider profile must be configured during online sign-up, and the OSU provider profile to be applied must exist.

Command	**osu-provider** *template-name*
Parameter Description	*template-name*: Indicates the name of a profile. The value is a string of up to 32 case-sensitive visible characters excluding question marks (?) and spaces.
Defaults	No OSU provider profile is applied.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	A maximum of 16 OSU provider profiles can be applied.

Enabling GAS Response Delay

- Optional.
- Enable GAS response delay in the Hotspot 2.0 profile.
- Enable GAS response delay to delay responding to GAS requests. You are advised not to enable this function.

Command	**gas-response delay** { **enable** | **disable** }
Parameter Description	N/A
Defaults	GAS response delay is disabled.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	N/A

Configuring the WAN Port Status

- Optional.
- Configure the WAN port status of an AP in the Hotspot 2.0 profile.
- Perform the configuration to advertise the WAN port status of an AP to STAs so as to help STAs select appropriate Hotspot 2.0 networks.

Command	**wan-metrics link-status** { **up** | **down** | **test** } [**asymmetric downlink-speed** *downlink-speed* **uplink-speed** *uplink-speed* | **symmetric link-speed** *link-speed*]
Parameter Description	*down-speed*: Indicates the downlink speed, in kbps. The value range is from 1 to 4,194,304. *up-speed*: Indicates the uplink speed, in kbps. The value range is from 1 to 4,194,304.
Defaults	No WAN port status is configured. If no link speed is configured, the link speed is **0**, indicating unknown.
Command Mode	Hotspot 2.0 configuration mode
Usage Guide	The WAN port status includes the link work status, uplink speed, downlink speed, uplink usage, downlink usage, metrics period, whether upstream and downstream rates are the same, and whether user access

	is denied when the upper limit is reached. Currently, the uplink and downlink usage remains **0**, indicating unknown. The metrics period is set to **0**, indicating that the uplink and downlink loads cannot be calculated and are unknown. The parameter indicating whether user access is denied when the upper limit is reached is set to **0**, and whether access upper limit is reached is not detected here.

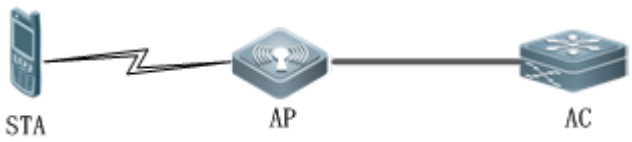
Verification

- Display the configuration of the Hotspot 2.0 profile to ensure the configuration correctness.

Configuration Example

Configuring a Hotspot 2.0 Profile in Fit AP Environment

- The configuration in the fat AP environment is completely the same as that in the fit AP environment.

Scenario **Figure 1-13**	

Configuration Steps	● Create and configure a Hotspot 2.0 profile.
	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# hotspot2 template test`
	`Hostname(config-hs20-tmplt)# 3gpp-cellular-network mcc 461 mnc 03`
	`Hostname(config-hs20-tmplt)# network-auth-type acceptance`
	`Hostname(config-hs20-tmplt)# osu-ssid osussid`
	`Hostname(config-hs20-tmplt)# vune-group 1 type 1`
	`Hostname(config-hs20-tmplt)# venue-name language-code eng name testvenue`
	`Hostname(config-hs20-tmplt)# roam-consortium oi 00-11-11 in-beacon`
	`Hostname(config-hs20-tmplt)# hessid 0141.1241.1124`
	`Hostname(config-hs20-tmplt)# domain-name www.org.com`
	`Hostname(config-hs20-tmplt)# network-type test`
	`Hostname(config-hs20-tmplt)# ipv4-address-availabe public-available`
	`Hostname(config-hs20-tmplt)# ipv6-address-availabe not-available`
	`Hostname(config-hs20-tmplt)# nai-realm realm-name testgg`
	`Hostname(config-hs20-tmplt)# connection-capability icmp enable`
	`Hostname(config-hs20-tmplt)# dgaf enable`
	`Hostname(config-hs20-tmplt)# operator-name language-code eng name mywifi`
	`Hostname(config-hs20-tmplt)# dls-tdls enable`
	`Hostname(config-hs20-tmplt)# osu-provider osu-test`
	`Hostname(config-hs20-tmplt)# gas-response delay enable`
	`Hostname(config-hs20-tmplt)# wan-metrics link-status up asymmetric`
	`downlink-speed 34 uplink-speed 56`

```
Hostname(config-hs20-tmplt)#exist
Hostname(config)#
```

Verification

Display the configuration of the Hotspot 2.0 profile.

```
Hostname#
Hostname#show hotspot2 template test
OSU SSID                : osussid
HESSID                  : 0141.1241.1124
Network type             : test
     Internet access     : enable
IPv4 address availability  : public-available
IPv6 address availability  : not-available
DGAF                    : enable
DLS/TDLS                : enable
Venue group              : 1(Assembly)
Venue type               : 1(Arena)
GAS response delay        : enable

Wan Metrics information:
  Link Status Symmetric Link downlink-speed(Kbps) Uplink-speed(Kbps)
  ----------- -------------- --------------------- ------------------
  test       asymmetric    34                56

Operator name information:
Index Language name
----- -------- -----------------------------------------
1    eng     mywifi

Venue name information:
Index Language name
----- -------- -----------------------------------------
1    eng     testvenue

Domain name information:
Index Domain name
----- ----------------------------------------------
1    www.org.com

Roaming consortium information:
Index OI                In beacon
----- -------------------- --------------------------
1    00-11-11           On

3GPP cellular network information:
```

```
Index MCC MNC
----- --- ----
1     460 03

Network authentication type information:
Index Authentication type redirection URL
----- ------------------ ------------------------------------
1     Acceptance

NAI realm information:
Index Auth method            Auth ID Auth Parameter Realm name
----- ------------------------ ------- --------------
-------------------------------------
1     --                    --      --           testgg


Osu-provider information:
  Index Template Name
  ----- -----------------
  1     osu-test

Connection capability information:
Index Protocol     Status
----- -----------   -------
1     ESP          on
2     ICMP         on
3     TCP-FTP       on
4     TCP-HTTP      on
5     TCP-SSH       on
6     TCP-VOIP      on
7     TCP-TLS-VPN   on
8     TCP-PPTP-VPN  on
9     UDP-VOIP      on
10    UDP-IKE2-500  on
11    UDP-IKE2-4500 on

Hostname#
```

Common Errors

- N/A

1.4.2 Configuring an OSU Provider Profile

Configuration Effect

- Create a Hotspot 2.0 OSU provider profile and configure parameters in the profile. The configured Hotspot 2.0 OSU provider profile can be applied and bound to a Hotspot 2.0 profile and bound to the Hotspot 2.0 profile so that the Hotspot 2.0 profile supports the Hotspot 2.0 OSU function.

Notes

- N/A

Configuration Steps

Creating an OSU Provider Profile

- Mandatory.
- Create an OSU provider profile.
- An OSU provider profile must be configured during online sign-up.

Command	**hotspot2 osu-provider template** *template-name*
Parameter Description	*template-name*: Indicates the name of a profile. The value is a string of up to 32 case-sensitive visible characters excluding question marks (?) and spaces.
Defaults	No OSU provider profile is configured.
Command Mode	Global configuration mode
Usage Guide	A maximum of 16 OSU provider profiles can be configured.

Configuring an OSU Provider Name

- Optional.
- Configure an OSU provider name.
- If a provider has multiple names, they refer to the same provider in different languages.

Command	**friendly-name language-code** *language-code* **name** *name*
Parameter Description	*language-code*: The value is a string of 2 to 3 characters. It supports both ISO-639-1 and ISO-639-2 standards. If ISO-639-1 is adopted, **0**is added to ensure that the value contains three characters. *name*: The value is a string of 1 to 252 case-sensitive visible characters excluding question marks (?) and spaces.
Defaults	No OSU provider name is configured.
Command Mode	OSU configuration mode
Usage Guide	A maximum of eight OSU provider names can be configured.

Configuring the OSU Service Description

- Optional.
- Configure the OSU service description.
- If a provider has multiple descriptions, they refer to the same service description in different languages.

Command	**service-description language-code** *language-code* **description** *description*
Parameter Description	*language-code*: The value is a string of 2 to 3 characters. It supports both ISO-639-1 and ISO-639-2 standards. If ISO-639-1 is adopted, **0** is added to ensure that the value contains three characters.

	description: The value is a string of 1 to 252 case-sensitive visible characters excluding question marks (?).
Defaults	No OSU provider description is configured.
Command Mode	OSU configuration mode
Usage Guide	A maximum of eight OSU provider descriptions can be configured.

Configuring the OSU Server URI

- Mandatory.
- Configure the OSU server URI.
- A client accesses an OSU server through the URI of the OSU server and performs the OSU process.

Command	**server-uri** *uri*
Parameter Description	*uri*: The value is a string of 1–255 visible characters and complies with RFC4282. It cannot contain question marks (?) and spaces, and the string cannot end with double quotation marks (").
Defaults	No OSU server URI is configured.
Command Mode	OSU configuration mode
Usage Guide	Up to one OSU server URI can be configured. Repeated configuration will overwrite the previous configuration.

Configuring an OSU Method

- Mandatory.
- Configure an OSU method.
- OSU methods include the OMA DM method and SOAP XML SPP method.

Command	**method** { **oma-dm** | **soap-xml-spp** }
Parameter Description	**oma-dm**: Indicates the OMA DM method. See section 8.3 in the Hotspot 2.0 protocol. **soap-xml-spp**: Indicates the SOAP XML SPP method. See section 8.4 in the Hotspot 2.0 protocol.
Defaults	No OSU method is configured.
Command Mode	OSU configuration mode
Usage Guide	A maximum of two OSU methods can be configured at the same time.

Configuring the OSU Network Access ID

- Optional.
- Configure the OSU network access ID.
- An OSU network access ID serves as an identity for EAP authentication when a client accesses the encrypted OSU wireless service. When an encrypted OSU wireless service is provided for a client, an OSU network access ID (OSU_NAI) needs to be configured.

Command	**nai** *nai*
Parameter Description	*nai*: Indicates the network access ID of an OSU server. The value is a string of 1–252 case-sensitive characters.

Defaults	No network access identifier is configured for an OSU server.
Command Mode	OSU configuration mode
Usage Guide	Up to one network access identifier can be configured for an OSU server.

Configuring an OSU Icon

- Optional.
- Configure an OSU icon.
- This command only loads images to an OSU provider profile and specifies the attributes of the images. To upload and store images, you need to use other means such as FTP or TFTP. Icon images are stored in the **wlan_bs/hotspot2/icons** path.

Command	**icon-name** *name* **type** { **png| jpg**	**bmp**	**gif** } **language-code** *code* [**width** *width* **height** *height*]
Parameter Description	*name*: Indicates the name of an icon file. The value is a string of 1 to 64 case-sensitive visible characters excluding question marks (?) and spaces. *code*: The value contains 2–3 characters. It supports both ISO-639-1 and ISO-639-2 standards. If ISO-639-1 is adopted, **0** is added to ensure that the value contains three characters. *width:* Indicates the pixel width of the icon file. The value range is from 1 to 65,536. The actual value should be consistent with the real image. If it is not set, the pixel width is automatically calculated. *height***:** Indicates the pixel height of the icon file. The value range is from 1 to 65,536. The actual value should be consistent with the real image. If it is not set, the pixel height is automatically calculated.
Defaults	No OSU icon is configured.
Command Mode	OSU configuration mode
Usage Guide	A maximum of eight OSU icons can be configured and the size of each icon image cannot exceed 64 KB. One icon image can be configured only once in the same OSU provider profile, and one image cannot be used for more than one language.

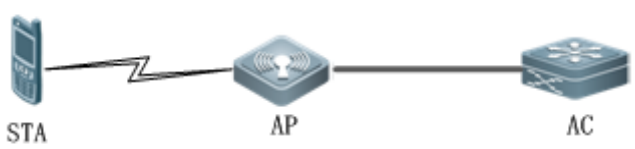
Verification

- Display the configuration of the OSU provider profile to ensure the configuration correctness.

Configuration Example

Configuring an OSU Provider Profile in Fit AP Environment

- The configuration in the fat AP environment is completely the same as that in the fit AP environment.

Scenario **Figure 1-14**	
Configuration	● Create and configure an OSU provider profile.

steps	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# hotspot2 osu-provider template test Hostname(config-hs20-osu-tmplt)# friendly-name language-code eng name test service provider Hostname(config-hs20-osu-tmplt)# service-description language-code eng description free test service Hostname(config-hs20-osu-tmplt)# server-uri https://test.oui.com Hostname(config-hs20-osu-tmplt)# method oma-dm Hostname(config-hs20-osu-tmplt)# nai myprovider Hostname(config-hs20-osu-tmplt)# icon-name test.png type png language-code eng width 400 height 200 Hostname(config-hs20-osu-tmplt)# exist Hostname(config)#
Verification	Display the configuration of the OSU provider profile.
	Hostname# show hotspot2 osu-provider template test NAI : myprovider URI : https://test.oui.com OSU methods : OMA-DM Friendly names information: Index Language Name ----- -------- ---------- 1 eng test service provider Service descriptions information: Index Language Description ----- -------- ---------- 1 eng free test service Icons information: Index Width Height Type language name ----- ----- ------ ----- -------- ---------- 1 400 200 png eng test.png Hostname#

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

Common Errors

- N/A

1.4.3 Applying a Hotspot 2.0 Profile to a WLAN on an AC

Configuration Effect

- Apply Hotspot 2.0 configuration to a WLAN so that the WLAN can run the Hotspot 2.0 functions.

Notes

- N/A

Configuration Steps

Applying a Hotspot 2.0 Profile to a WLAN on an AC

- Mandatory.
- Apply a Hotspot 2.0 profile to a WLAN on an AP.
- Apply Hotspot 2.0 configuration to a WLAN.

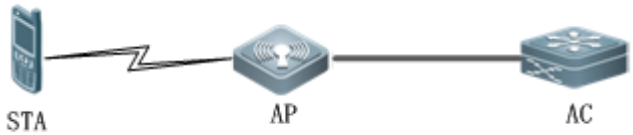
Command	**hotspot2 template** *template-name*
Parameter Description	**template** *template-name*: Uses the WLAN as the Hotspot 2.0 WLAN and specifies the Hotspot 2.0 profile. The name of a Hotspot 2.0 profile is a string of up to 32 case-sensitive visible characters excluding question masks (?) and spaces.
Defaults	No Hotspot 2.0 profile is applied to a WLAN.
Command Mode	WLAN configuration mode
Usage Guide	The specified Hotspot 2.0 profile must exist. Only one Hotspot 2.0 profile can be applied to a WLAN. If Hotspot 2.0 profiles are configured for the same WLAN multiple times, the later configuration will overwrite the previous configuration.

Verification

- Display the configuration of the Hotspot 2.0 profile applied to a WLAN to ensure the configuration correctness.

Configuration Example

Applying a Hotspot 2.0 Profile to a WLAN in the AC Environment

Scenario **Figure 1-15**	
Configuration Steps	• Apply a Hotspot 2.0 profile to a WLAN.
AC	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#wlan-config 1 test Hostname(config-wlan)#hotspot2 template testtmplt

	Hostname(config)#
Verification	Run the **show running-config** command to display the configuration.

Common Errors

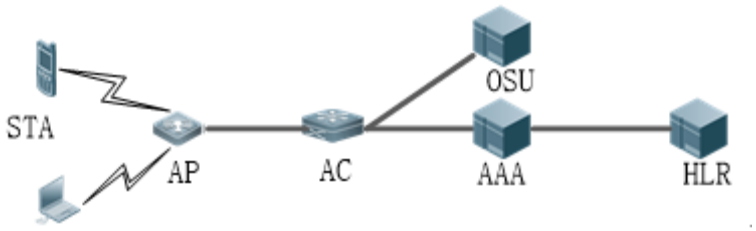
N/A

1.4.4 Configuration Examples

Configuration Effect

- An operator deploys a Hotspot 2.0 network where mobile phones can automatically access the Hotspot 2.0 network through SIM authentication and non-mobile terminals (without SIM cards) such as PADs and laptops can access the network.

Scenario

Scenario **Figure 1-17**	

Configuration Steps

- Create a Hotspot 2.0 network.

AC	Hostname(config)#wlan-config 2 Hotspot2 Hostname(config-wlan)#exit Hostname(config)#ap-group Hotspot2 Hostname(config-group)#interface-mapping 2 2

- Create a WLAN for OSU.

AC	Hostname(config)#wlan-config 3 osu Hostname(config-wlan)#exit Hostname(config)#ap-group osu Hostname(config-group)#interface-mapping 3 3

- Configure an OSU profile.

AC	Hostname(config)# hotspot2 osu-provider template osu Hostname(config-hs20-osu-tmplt)#friendly-name language-code eng name "SP Orange Test Only" Hostname(config-hs20-osu-tmplt)#server-uri

	https://osu-server.r2-testbed-rks/OnlineSignup/ Hostname(config-hs20-osu-tmplt)#method soap-xml-spp Hostname(config-hs20-osu-tmplt)#icon-name test1.png type png language-code eng

- Configure a Hotspot 2.0 profile.

AC	Hostname(config)# hotspot2 template Hotspot2 Hostname(config-hs20-tmplt)#3gpp-cellular-network mcc 460 mnc 00 Hostname(config-hs20-tmplt)#3gpp-cellular-network mcc 460 mnc 01 Hostname(config-hs20-tmplt)#3gpp-cellular-network mcc 460 mnc 03 Hostname(config-hs20-tmplt)#osu-ssid osu Hostname(config-hs20-tmplt)#venue-group 2 type 8 Hostname(config-hs20-tmplt)#roam-consortium oi 50-6F-9A in-beacon Hostname(config-hs20-tmplt)#roam-consortium oi 00-1B-C5-04-BD in-beacon Hostname(config-hs20-tmplt)#hessid 0a69.6cb9.7918 Hostname(config-hs20-tmplt)#domain-name wi-fi.org Hostname(config-hs20-tmplt)#network-type public-chargeable Hostname(config-hs20-tmplt)#nai-realm realm-name wi-fi.org eap-method-type eap-ttls auth-method 5 auth-para 7 Hostname(config-hs20-tmplt)#operator-name language-code eng name "Wi-Fi Alliance" Hostname(config-hs20-tmplt)#osu-provider osu

- Enable Hotspot 2.0 on the WLAN.

AC	Hostname(config)#wlan-config 2 Hotspot2 Hostname(config-wlan)#hotspot2 template Hotspot2

- Configure AAA authentication.

AC	Hostname(config)#aaa new-model Hostname(config)#aaa accounting update Hostname(config)#aaa authentication dot1x Hotspot2 method Hotspot2 group Hostname(config)# aaa group server Hotspot2 group Hostname(config-gs-radius)#server 172.18.33.114 Hostname(config)#radius-server host 172.18.33.114 key testing123

- Configure 802.1X authentication for secure access on the Hotspot 2.0 network.

AC	Hostname(config)#wlansec 2 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)#dot1x authentication Hotspot2 method

Verification

- Check the Hotspot 2.0 configuration on the WLAN.

AC	Hostname(config)#wlan-config 2 Hotspot2 Hostname(config-wlan)#show this Building configuration... ! hotspot2 template Hotspot2 ! End Hostname(config-wlan)#exit Hostname(config)#ap-group Hotspot2 Hostname(config-group)# show this Building configuration... ! interface-mapping 2 2 ! end

- Check the OSU configuration.

AC	Hostname(config)#wlan-config 3 osu Hostname(config-wlan)#show this Building configuration... ! End Hostname(config-wlan)#exit Hostname(config)#ap-group osu Hostname(config-group)# show this

```
Building configuration...
!
 interface-mapping 3 3
!
end
```

- Check the OSU profile.

AC

```
Hostname(config)#show hotspot2 osu-provider template osu
Hotspot2 OSU provider template osu settings:
------------------------------------------------------------------
  NAI...........:
  URI....:https://osu-server.r2-testbed-rks/OnlineSignup/
  OSU methods........:,soap-xml-spp

  Friendly names information:
  Index Language Name
  ----- -------- -------------------------------------------
  1     eng      SP Orange Test Only

  Service descriptions information:
  Index Language Description
  ----- -------- -----------------------------------------

  Icons information:
  Index Width  Height Type  Language Name
  ----- ------ ------ ----- -------- ------------------------
  1     1000   971    jpg   zxx      test1.jpg
```

- Check the Hotspot 2.0 profile.

AC

```
Hostname(config)#show hotspot2 template Hotspot2
Hotspot2 template Hotspot2 settings:
------------------------------------------------------------------
  OSU SSID.............:osu
  Hessid..............:0a69.6cb9.7918
```

```
Network type.............:public-chargeable
       Internet access..:disable
IPv4 address available..:unknown
IPv6 address available..:unknown
DGAF....................:enable
DLS/TDLS................:enable
GAS response delay......:disable
Venue Group.............:2(Business)
Venue Type..............:8(Research and Development Facility)

Wan metrics information:
Link Status Symmetric Link downlink-speed(Kbps) Uplink-speed(Kbps)
----------- -------------- -------------------- ------------------

Operator name information:
Index Language Name
----- -------- ------------------------------------------
1     eng      Wi-Fi Alliance

Venue name information:
Index Language Name
----- -------- ------------------------------------------

Domain name information:
Index Name
----- ------------------------------------------
1     wi-fi.org

Roam consortium information:
Index OI               In Beacon
----- ---------------- ---------
1     50-6F-9A         On
2     00-1B-C5-04-BD   On
```

```
3GPP cellular network information:
Index MCC   MNC
----- ----- -----
1     460   00
2     460   01
3     460   03

Network authentication type information:
Index Authentication type     Redirection URL
----- ----------------------- ----------------------------

Osu-provider information:
Index Template Name
----- -----------------

NAI realm information:
Index Auth method Auth ID Auth Parameter Realm name
----- ----------- ------- -------------- --------------------
1     eap-ttls    5       7              wi-fi.org

Connection capability information:
Index Protocol       Status
----- -------------- ------
1     esp            On
2     icmp           On
3     tcp-ftp        On
4     tcp-http       On
5     tcp-pptp-vpn   On
6     tcp-ssh        On
7     tcp-tls-vpn    On
8     tcp-voip       On
9     udp-ike2-4500  On
10    udp-ike2-500   On
11    udp-voip       On
```

- Display the configuration of AAA authentication.

AC	Hostname#show running-config | inc aaa aaa new-model aaa accounting update aaa authentication dot1x Hotspot2 group Hotspot2 group aaa group server Hotspot2 group Hostname#show running-config | inc server aaa group server radius sim_group_wlan_2 server 172.18.33.114 radius-server host 172.18.33.114 key testing123

- Display the configuration of 802.1X authentication on the Hotspot 2.0 network.

AC	Hostname(config)#wlansec 2 Hostname(config-wlansec)#show this Building configuration... ! security rsn enable security rsn ciphers aes enable security rsn akm 802.1x enable dot1x authentication Hotspot2 method ! end

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show hotspot2 template [*template-name*]	Displays the configuration of a Hotspot 2.0 profile.
show hotspot2 osu-provider template [*template-name*]	Displays the configuration of an OSU provider profile.

Debugging

N/A

1 Configuring STA Identification

1.1 Overview

As the electronic industry develops, STAs are becoming increasingly diversified, requiring a method to identify and manage various STAs. Traditional STA management are inefficient and cannot meet the demands of modern network management.

The STA identification function analyzes and classifies STA information to identify STAs of different types. By comparing the STA information carried in different packets with the STA information feature library, it can identify the hardware information and software versions of the STAs. This method enables network administrators to perform efficient operation and maintenance (O&M), including visualized STA information, STA classification management, and authentication and accounting management.

1.2 Applications

Application	Description
Basic Scenarios of STA Identification	Users are connected to wireless devices over Layer 2 networks.

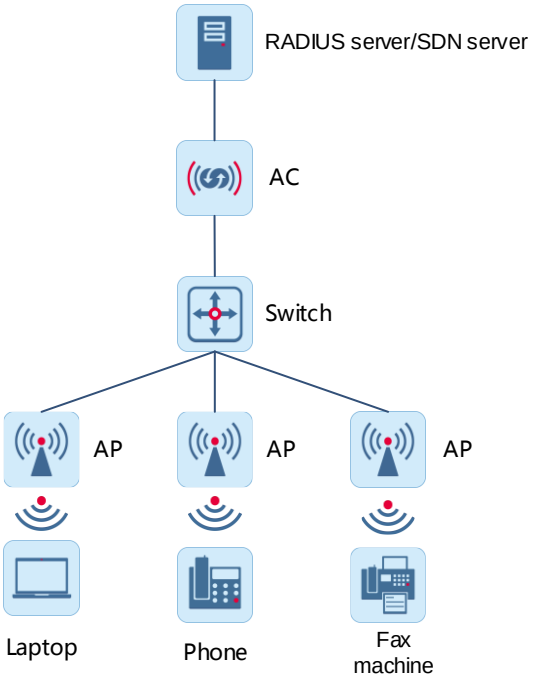
1.2.1 Basic Scenarios of STA Identification

Scenario

To facilitate monitoring and O&M, users require that wireless STAs accessing the network can be identified, and different management policies can be configured based on the STA type. In this case, a wireless access controller (AC) and an SDN controller or RADIUS server can work together to achieve effective management on STAs of different types.

- Enable STA identification on the AC or SDN controller. The AC can directly identify original data and report the identification result to the RADIUS server. Alternatively, the AC can send original data to the SDN controller for identification.
- The RADIUS server or SDN controller implements authentication control based on the identification result and delivers authorization information.

Figure 1-1 STA Identification



Deployment

- Enable global STA identification on the AC.

1.3 Features

Basic Concepts

STA Identification by an AC

The STA identification function is enabled on an AC to collect the packets of STAs and then identify the STA information, including STA types, operating systems, vendors, and models.

STA Identification by an SDN Controller

An AC collects original packets from STAs and send the packets to an SDN controller. Then the SDN controller identifies the STA information, including STA types, operating systems, vendors, and models.

Overview

Feature	Description
STA Identification by an AC	The STA identification function is enabled on an AC to collect the packets of STAs and then identify the STA information, including STA types, operating systems, vendors, and models.

STA Identification by an SDN Controller	A Ruijie SDN controller needs to be deployed on the network to identify the STA information, including STA types, operating systems, vendors, and models.

1.3.1 STA Identification by an AC

The STA identification function is enabled on an AC to collect the packets of STAs and then identify the STA information, including STA types, operating systems, vendors, and models.

Working Principle

- In a scenario where the IP address of a STA is automatically allocated by the DHCP server and the DHCP snooping function is enabled on the AC, the AC identifies the STA information such as the STA type and operating system based on DHCP options when the STA requests an IP address.
- When a STA adopts web-based authentication, the AC identifies information such as the product model and operating system version based on the User-Agent field sent by the browser.
- On an AC that supports STA identification profile configuration, you can configure the AC to collect specified types of packets such as DHCP, HTTP, DNS, mDNS, and SIP packets, and to extract key characteristics from the collected information for identifying STAs.

1.3.2 STA Identification by an Controller

Working Principle

By collecting specified types of packets such as DHCP, HTTP, DNS, mDNS, and SIP packets and extracting key characteristics from the collected information, the AC reports the characteristics to an SDN controller through gRPC. The SDN controller identifies the STA information, including STA types, operating systems, vendors, and models.

1.4 Configuration

Configuration	Description and Command	
Configuring STA Information Collection	(Mandatory) It is used to enable global STA identification.	
	terminal-identify enable	Enables global STA identification.
	(Mandatory) It is used to create a STA identification profile.	
	terminal-identify-template *template-name*	Creates a STA information collection profile.
	(Optional) It is used to configure basic parameters of a collection profile.	
	dhcp enable	Enables DHCP packet collection.
	dns enable	Enables DNS packet collection.
	mdns enable	Enables mDNS packet collection.
	http enable	Enables HTTP packet collection.

	sip enable *address port*	Configures SIP packet collection.
	notification enable	Enables data reporting through gRPC.
	terminal-identify template *template-name* **global**	Applies a STA identification profile globally
Configuring STA Identification Component UpgradeUpgrade	**terminal-identify upgrade feature flash**:*/url*	Upgrades the STA identification feature library.
	terminal-identify upgrade engine flash:*/url*	Upgrades the STA identification engine model.

1.4.1 Configuring STA Information Collection

Configuration Effect

- The AC collects STA packets of specified types and sends the packets to the SDN controller for identification of STA types, operating systems, vendors, and models.

Notes

- N/A

Configuration Steps

Enabling STA Identification

Command	**terminal-identify enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Creating a STA Information Collection Profile or Entering STA Information Collection Profile Configuration Mode

Command	**terminal-identify-template** *template-name*
Parameter Description	*template-name*: Indicates the profile name.
Command Mode	Global configuration mode
Usage Guide	1. If the profile name does not exist, create a collection profile and enter the collection profile configuration mode. 2. If the profile name already exists, enter the collection profile configuration mode. 3. Up to five templates can be created.

Enabling DHCP Packet Collection

Command	**dhcp enable**

Parameter Description	N/A
Command Mode	STA information collection profile configuration mode
Usage Guide	N/A

Enabling DNS Packet Collection

Command	**dns enable**
Parameter Description	N/A
Command Mode	STA information collection profile configuration mode
Usage Guide	N/A

Enabling mDNS Packet Collection

Command	**mdns enable**
Parameter Description	N/A
Command Mode	STA information collection profile configuration mode
Usage Guide	N/A

Enabling HTTP Packet Collection

Command	**http enable**
Parameter Description	N/A
Command Mode	STA information collection profile configuration mode
Usage Guide	N/A

Configuring SIP Packet Collection

Command	**sip enable** { *ipv4-address* | *ipv6-address* } *port*
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the SIP server. *ipv6-address*: Indicates the IPv6 address of the SIP server. *port*: Indicates the port number of the SIP server.
Command Mode	STA information collection profile configuration mode
Usage Guide	After this function is enabled, SIP packets with specified destination addresses and ports are collected for STA identification. A maximum of five SIP server addresses can be configured in a profile. The SIP packet collection function can be configured only for unicast addresses.

Enabling Data Reporting through gRPC

Command	**notification enable**
Parameter Description	N/A
Command Mode	STA information collection profile configuration mode
Usage Guide	N/A

Applying a STA Information Collection Profile Globally

Command	**terminal-identify template** *template-name* **global**
Parameter Description	*template-name*: Indicates the profile name.
Command Mode	Global configuration mode
Usage Guide	1. Only one STA information collection profile can be applied globally. 2. When a STA information collection profile is applied, it indicates that the STA information collection function is enabled.

Configuring the Uploading Mode of the Collected STA Information

Command	**terminal-identify hw-radius-attr option**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable this function, you need to run the **radius-server authentication vendor hw package** command first to configure the device to encapsulate a Huawei proprietary attribute in RADIUS authentication request packets. For details, see *Configuring RADIUS*.

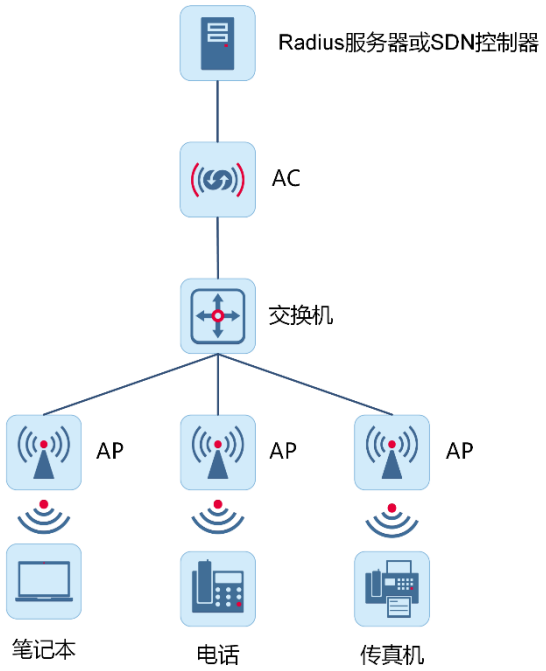
Verification

- Run the **show running-config** command to check whether STA information collection is enabled and display information about the created profile as well as the application status of the global profile.
- Enter the STA information collection profile configuration mode and run the **show this** command to display the configuration of the profile.

Configuration Examples

The following configuration example only describes the configuration related to STA identification.

Configuring STA Identification

Scenario **Figure1-2**	
Configuration Steps	● Enable STA identification on the AC. ● Enter the default STA information collection profile named **default** and disable the collection of DNS and mDNS packets. ● Apply the STA information collection profile named **default** globally.
	Hostname# config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#terminal-identify enable Hostname(config)#terminal-identify-template default Hostname(terminal-identify-template)#no dns enable Hostname(terminal-identify-template)#no mdns enable Hostname(terminal-identify-template)#exit Hostname(config)#terminal-identify template default global
Verification	● Display the configuration of the default STA information collection profile named **default**.
	Hostname#show terminal-identify template Template apply(default) Template default: Type Status -------- -------- DHCP Enable DNS Enable MDNS Enable HTTP Enable ● Display the application status of the STA information collection profile.

	Hostname#show running-config | include terminal-identify terminal-identify template default global

1.4.2 Configuring STA Identification Component Upgrade

Configuration Effect

- Upgrade the STA identification feature library and engine model to the latest version.

Notes

- N/A

Configuration Steps

Upgrading the STA Identification Feature Library

Command	**terminal-identify upgrade feature flash**:*/url*
Parameter Description	*url*: Indicates the path of the feature library file to be upgraded.
Command Mode	Global configuration mode
Usage Guide	The feature library stores the STA identification codes supported by the system. If STA identification codes in the feature library need to be updated, run this command to upgrade the feature library.

Upgrade the STA Identification Engine Model

Command	**terminal-identify upgrade engine flash**:*/url*
Parameter Description	*url*: Indicates the path of the engine model file to be upgraded.
Command Mode	Global configuration mode
Usage Guide	The command is used to upgrade the engine model on products supporting the STA identification engine.

Verification

Run the **show terminal-identify database upgrade history** command to display the upgrade records.

1.5 Monitoring

Displaying

Command	Description
show terminal-identify user	Displays the STA identification result.
show terminal-identify database version	Displays the feature library and engine model version on the device.

show terminal-identify database upgrade history	Displays the update records of the feature library and engine model on the device.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug terminal-identify	Debugs STA identification.

1 Configuring STA Connectivity Test

1.1 Overview

When a fault occurs on a network, it is necessary to quickly and accurately locate the fault and rectify it to restore network services. The connectivity test function is used to detect connectivity between stations (STAs) and different key nodes (such as air interface, gateway, and server). By configuring the target detection node for connectivity test, you can detect the delay and packet loss rate on the link between a STA and the corresponding node.

Protocols and Standards

N/A

1.2 Applications

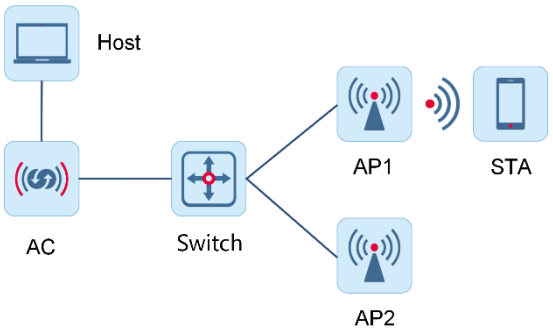
Application	Description
Checking Checking Connectivity Between a STA and the Air Interface of an APthe Air Interface of an AP	In Fit AP mode, a wireless access point (AC) sends a VSP message to an access point (AP) based on the STA's MAC address to trigger link detection on the AP. The AC simulates packet exchange between the AP and STA to obtain the delay and packet loss rate.
Checking Checking Connectivity Between a STA and the Gateway/DHCP Server/DNS Server	In Fit AP mode, the AC sends a VSP message to the AP based on the STA's MAC addresses to trigger link detection on the AP. The AC simulates packet exchange between the AP and the gateway, DHCP server, or DNS server of the STA to obtain the delay and packet loss rate.

1.2.1 Checking Connectivity Between a STA and the Air Interface of an AP

Scenario

In Fit AP mode, the AC sends a VSP message to the AP based on the MAC address of a STA to trigger link detection on the AP. The AC simulates packet exchange between the AP and STA to obtain the delay and packet loss rate.

Figure 1-1 Checking Connectivity Between a STA and the Air Interface of an AP



Remarks	Switch: A switch AC: A wireless access controller. AP1 and AP2: Two wireless access points. Host: A remote host. STA: A wireless access endpoint.

Deployment

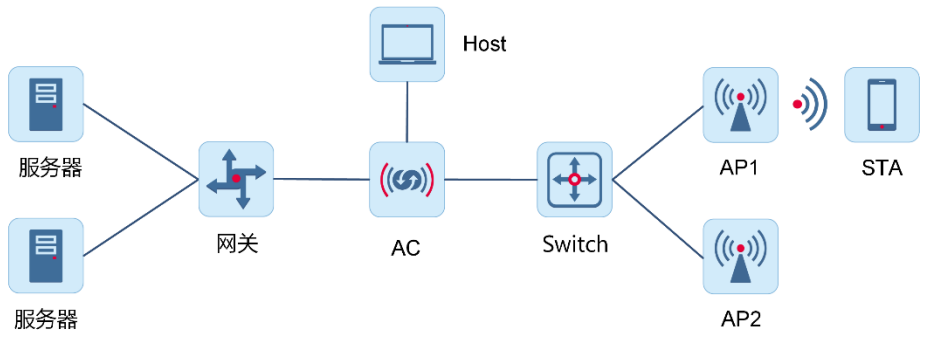
- Enable STA connectivity test on a specified AP connected to the AC.
- Configure the VLAN of the STA to be detected on the AC.
- Configure the MAC address of the STA to be detected on the AC.
- Configure the AC to check the connectivity between the STA and the air interface of the AP.

1.2.2 Checking Connectivity Between a STA and the Gateway/DHCP Server/DNS Server

Scenario

In Fit AP mode, the AC sends a VSP message to the AP based on the MAC address of a STA to trigger link detection on the AP. The AC simulates packet exchange between the AP and the gateway, DHCP server, or DNS server of the STA to obtain the delay and packet loss rate.

Figure 1-2 Checking Connectivity Between a STA and the Gateway/DNS/DHCP Server



Deployment

- Enable STA connectivity test on a specified AP connected to the AC.
- Configure the VLAN of the STA to be detected on the AC.
- Configure the MAC address of the STA to be detected on the AC.
- Configure the AC to check the connectivity between the STA and the gateway, DHCP server, or DNS server.

1.3 Features

Basic Concepts

Packet Loss and Delay Statistics

The AC collects packet loss and delay statistics through Internet Control Message Protocol (ICMP).

CAPWAP Tunnel

In a fit AP network architecture, the AC uniformly manages all APs through a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel, and delivers control policies to APs, eliminating the need to configure APs separately. The CAPWAP tunnel between an AP and the AC consists of a control tunnel and a data tunnel. The AC delivers configurations to the AP and the AP sends event notifications to the AC over the control tunnel, while data packets is transmitted over the data tunnel between the AC and AP.

Overview

Feature	Description
STA Connectivity Test	After the STA connectivity test function is enabled on a specified AP, the AP proactively generates ICMP packets for the STA to be detected and simulates the STA's ICMP communication to detect the link connectivity.

1.3.1 STA Connectivity Test

After the STA connectivity test function is enabled on a specified AP, the AP proactively generates ICMP packets for the STA to be detected and simulates the STA's ICMP communication to detect the link connectivity.

Working Principle

When a connectivity test is performed, the WLAN ID, radio ID, VLAN ID, and forwarding mode of the STA are collected. After link detection is enabled, the AP checks whether the STA is online based on the configuration of the STA connectivity test function. If the STA is online, the AP generates an ICMP packet based on the IP and MAC addresses of the STA. The DATA field in the ICMP packet records information such as the REQ_ID, generation time, and special flag, and stores the packet sending status. The AP simulates a normal STA to send the ICMP request packet, and records the delay and packet loss rate based on the ICMP response packet. Then, the AP sends the information collected at an interval to the AC for storage.

1.4 Configuration

Configuration	Description and Command	
Configuring STA Connectivity	(Mandatory) It is used to enable the STA connectivity test function.	
	sta-cv enable	Enables the STA connectivity test function.
	(Mandatory) It is used to configure the VLAN of the STA.	
	sta-cv vlan	Configures the VLAN of the STA.
	(Optional) It is used to configure the link detection interval for a STA.	
	sta-cv detect interval	Configures the link detection interval for a STA.
	(Mandatory) It is used to configure the MAC address of the STA to be detected.	
	sta-cv mode static	Configures the MAC address of the STA.
	(Mandatory) It is used to configure the target node for link detection.	
	sta-cv target	Configures the detection node type.

1.4.1 Configuring STA Connectivity Test

Configuration Effect

The network connectivity between the STA and the AP's air interface, gateway, DHCP server, or DNS server can be checked.

Notes

N/A

Configuration Steps

Enabling STA Connectivity Test

- Mandatory.
- Enable this function on a specified AP.

Command	**sta-cv enable**
Parameter Description	N/A
Defaults	The function is disabled.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	The configuration priority is listed in descending order: AP configuration mode > AP group configuration mode > all-AP configuration mode. In cases where there are overlapping configurations on the AP, the configuration with the highest priority takes precedence. For example, if connectivity test service is

	configured in both all-AP configuration mode and AP configuration mode, the configuration in AP configuration mode prevails.

Configuring the VLAN of a STA

- Mandatory.

Command	**sta-cv vlan** *vlan-id gateway-ip gateway-mac dns-ip dhcp-ip*
Parameter Description	*vlan-id*: Indicates the VLAN ID. The value range is from 1 to 4094, and the value is unique. *gateway-ip*: Indicates the IP address of the gateway. *dhcp-ip*: Indicates the IP address of the DHCP server. *dns-ip*: Indicates the IP address of the DNS server. *gateway-mac*: Indicates the MAC address of the gateway.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	• When you configure entries with the same VLAN ID but different IP and MAC addresses, the original VLAN configuration is updated. • The STA link detection function simulates a STA to initiate link detection. Therefore, you need to configure the VLAN table associated with the STA (to simulate the forwarding path of a real user, so as to calculate the link delay and packet loss rate).

Configuring the Link Detection Interval

- Optional.

Command	**sta-cv detect interval** *interval-time*
Parameter Description	*interval-time*: Indicates the detection interval, in seconds. The value range is from 2 to 10.
Defaults	2 seconds
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the MAC Address of a STA

- Mandatory.

Command	**sta-cv mode static** *sta-mac*
Parameter Description	*sta-mac*: Configures the MAC address of a STA.
Defaults	N/A
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode

Usage Guide	● If you configure the MAC address of an offline STA, the configuration does not take effect until the STA goes online. ● You can configure multiple static STAs. Up to 16 static STA entries can be configured. If you configure static STA entries with the same MAC address but different IP address, the original configuration is updated.

Configuring the Detection Node Type

- Mandatory.
- To perfom link detection for a specified node, configure the type of the target node on the AC.

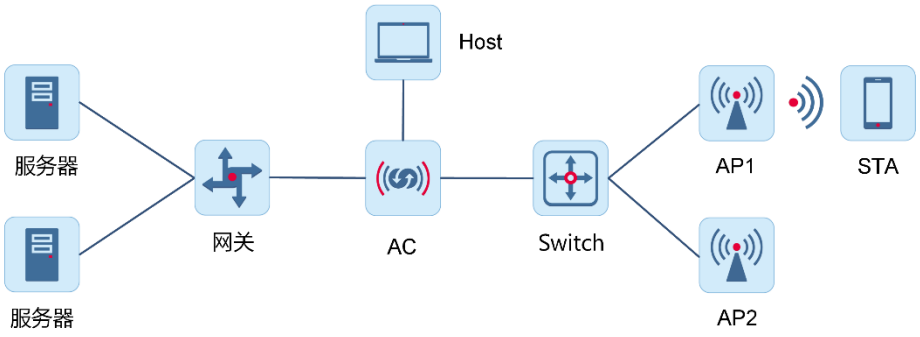
Command	**sta-cv target** { **air** | **gateway** | **server** { **dhcp** | **dns** | *server-ip* } }
Parameter Description	**air**: Configures the detection node as the air interface. **gateway**: Configures the detection node as the gateway. **server**: Configures the detection node as the server. **dhcp**: Specifies the DHCP server.. **dns**: Specifies the DNS server. *server-ip*: Specifies the server with a customized IP address.
Defaults	N/A
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	● If multiple detection node types are configured, the configurations take effect simultaneously. ● Up to 16 detection node entries can be configured (including the air interface, gateway, DHCP server, and DNS server).

Verification

Run the **show running-config** or **show sta-cv cur-cfg** command, or run the **show this** command in the current configuration mode, to display the configuration.

Configuration Examples

Configure STA connectivity Test on a Fit AP Network

Scenario **Figure1 -3**	
Configuration Steps	● Enter the global configuration mode. ● Configuring the VLAN of a STA.

	● Set the link detection interval to 4 seconds. ● Enter the all-AP configuration mode. ● Enable STA connectivity test on all APs. ● Configure the MAC address of a STA. ● Configure the detection nodes as the air interface, gateway, DHCP server, and DNS server.

AC	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# sta-cv vlan 101 192.168.101.1 00D0.F822.35FB 8.8.8.8 10.104.64.125`
	`Hostname(config)# sta-cv detect interval 4`
	`Hostname(config)# ap-config all`
	`Hostname(config-ap)# sta-cv enable`
	`Hostname(ap-config)# sta-cv mode static 448C.000F.B0FD`
	`Hostname(config-ap)# sta-cv target air`
	`Hostname(config-ap)# sta-cv target gateway`
	`Hostname(config-ap)# sta-cv target server dhcp`
	`Hostname(config-ap)# sta-cv target server dns`

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

AC	`Hostname(config-ap)#show this`
	`Building configuration...`
	`!`
	`sta-cv vlan 101 192.168.101.1 00D0.F822.35FB 8.8.8.8 10.104.64.125`
	`sta-cv detect interval 4`
	`ap-config all`
	`sta-cv enable`
	`sta-cv mode static 448C.000F.B0FD`
	`sta-cv target air`
	`sta-cv target gateway`
	`sta-cv target server dhcp`
	`sta-cv target server dns`
	`!`
	`end`

Common Errors

N/A

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show sta-cv log	Displays all connectivity test logs.
show sta-cv cur-cfg	Displays the configurations that take effect on an AP.

Debugging

N/A

Configuring WLAN Roaming

1. Configuring Roaming
2. Configuring MED
3. Configuring SFN

1 Configuring Roaming

Whether this function is supported depends on the actual product version.

1.1 Overview

Roaming allows stations (STAs) to be re-associated with access points (APs) when STAs move in coverage areas of different APs.

Roaming enables STAs to maintain ongoing IP communication and enjoy all application services when they move. The STAs do not detect occurrence of such a behavior during roaming.

Roaming is required when STAs move in different areas in a wireless environment. Roaming is classified into intra-AC and inter-AC roaming:

- Intra-AC roaming is applicable to a network with only one access controller (AC) deployed.
- Inter-AC roaming is applicable to a network with multiple ACs deployed.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Intra-AC Roaming	One STA is associated with AP1 connected to one AC, and then moves to the coverage area of AP2 connected to the same AC and is associated with AP2.
Inter-AC Roaming	One STA is associated with AP1 connected to AC1, and then moves to the coverage area of AP2 connected to AC2 and is associated with AP2.

1.2.1 Intra-AC Roaming

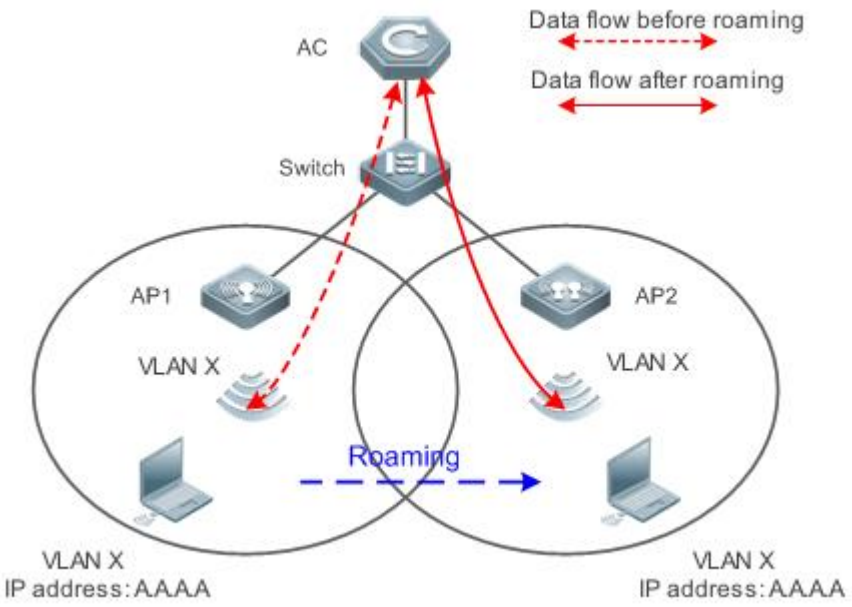
Scenario

One STA is associated with AP1 connected to one AC, and then moves to the coverage area of AP2 connected to the same AC and is associated with AP2. Depending on whether data is forwarded by the AC or AP, intra-AC roaming is further classified into intra-AC Layer 2 or Layer 3 roaming in centralized or local forwarding mode.

1.2.1.1 Intra-AC Layer 2 or Layer 3 Roaming in Centralized Forwarding Mode

Figure 1-1 shows intra-AC Layer 2 or Layer 3 roaming in centralized forwarding mode.

Figure 1-1 Intra-AC Layer 2 or Layer 3 Roaming in Centralized Forwarding Mode



Remarks	VLAN X indicates the VLAN ID associated with the STA. (If VLAN X corresponding to AP2 is changed to VLAN Y, Layer 3 roaming occurs.)

The difference between Layer 2 and Layer 3 roaming depends on whether VLANs associated with a STA are different before and after roaming.

Deployment

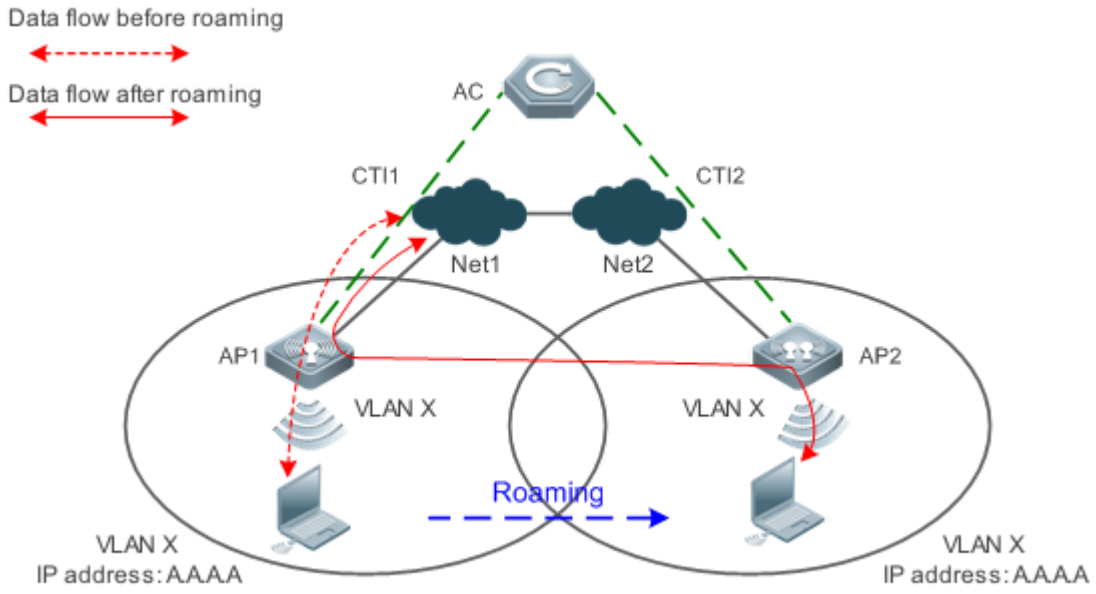
- AP1 and AP2 are associated with the AC through an intermediate device and are assigned to the same WLAN.
- A STA is associated with AP1 and obtains the IP address A.A.A.A.
- Then the STA moves to the coverage area of AP2 and is associated with AP2. During this process, the IP address remains unchanged with service continuity.

A STA can roam only when the wireless service set identifiers (SSIDs) provided by AP1 and AP2 are the same.

1.2.1.2 Intra-AC Layer 2 or Layer 3 Roaming in Local Forwarding Mode

Figure 1-2 shows intra-AC Layer 2 or Layer 3 roaming in local forwarding mode.

Figure 1-2 Intra-AC Layer 2 or Layer 3 Roaming in Local Forwarding Mode



Remarks	The CTI is the communication tunnel between an AP and an AC. VLAN X indicates the VLAN ID associated with a STA.

Deployment

- AP1 and AP2 set up control channels with the AC, and are allocated to VLAN X on the same WLAN.
- AP1 and AP2 work in local forwarding mode. A STA is associated with AP1 and obtains the IP address A.A.A.A.
- Then the STA moves to the coverage area of AP2 and is associated with AP2. During this process, the IP address remains unchanged with service continuity.
- Before roaming, data is directly sent out by AP1. After roaming, data is forwarded from AP2 to AP1, and then sent out by AP1.

⚠ A STA can roam only when the SSIDs provided by AP1 and AP2 are the same.

1.2.2 Inter-AC Roaming

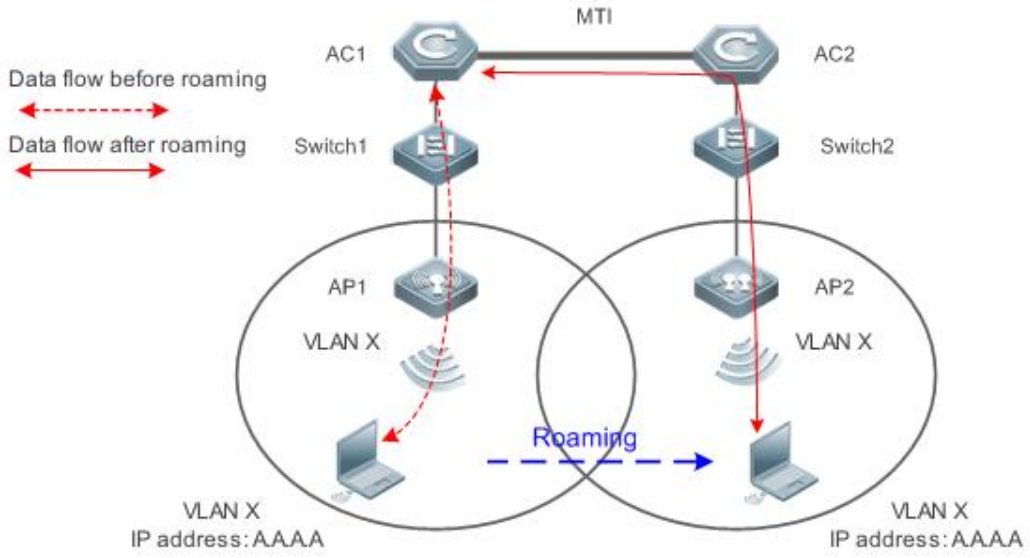
Scenario

One STA is associated with AP1 connected to AC1, and then moves to the coverage area of AP2 connected to AC2 and is associated with AP2. Depending on whether data is forwarded by the AC or AP, inter-AC roaming is further classified into inter-AC roaming in centralized or local forwarding mode.

1.2.2.1 Inter-AC Layer 2 or Layer 3 Roaming in Centralized Forwarding Mode

Figure 1-3 shows inter-AC Layer 2 or Layer 3 roaming in centralized forwarding mode.

Figure 1-3 Inter-AC Layer 2 or Layer 3 Roaming in Centralized Forwarding Mode



Remarks	VLAN X indicates the VLAN ID associated with a STA. MTI is the communication tunnel between ACs.

Deployment

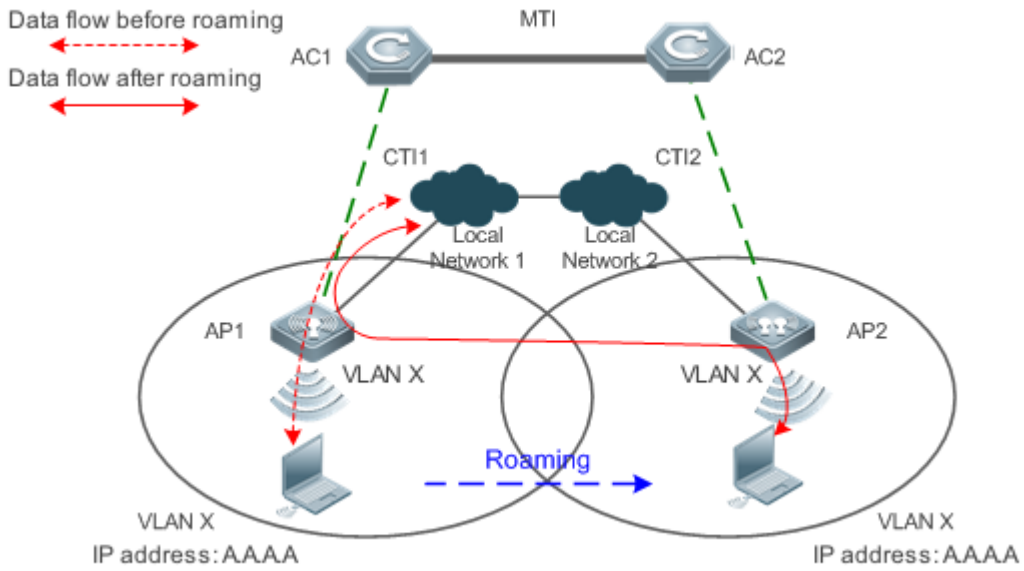
- AC 1 and AC 2 need to be configured as roaming members of each other and can communicate with each other.
- AP1 is connected to AC1 and AP2 is connected to AC2. Both AP1 and AP2 are assigned to VLAN X on the same WLAN.
- A STA is associated with AP1 and obtains the IP address A.A.A.A. Then the STA moves to the coverage area of AP2, and is associated with AP2. During this process, the IP address remains unchanged with service continuity.
- Before roaming, data is directly sent out by AC1. After roaming, data is forwarded from AC2 to AC1 through the MTI, and then sent out by AC1.

A STA can roam only when the SSIDs provided by AP1 and AP2 are the same.

1.2.2.2 Inter-AC Layer 2 or Layer 3 Roaming in Local Forwarding Mode

Figure 1-4 shows inter-AC Layer 2 or Layer 3 roaming in local forwarding mode.

Figure 1-4 Inter-AC Layer 2 or Layer 3 Roaming in Local Forwarding Mode



Remarks	VLAN X indicates the VLAN ID associated with the STA. The MTI is the communication tunnel between ACs, and the CTI is the communication tunnel between an AP and an AC.

Deployment

- AC 1 and AC 2 need to be configured as roaming members of each other in a roaming group.
- AP1 is connected to AC1 and AP2 is connected to AC2. Both AP1 and AP2 are assigned to VLAN X on the same WLAN. Both AP1 and AP2 work in local forwarding mode.
- A STA is associated with AP1 and obtains the IP address A.A.A.A. Then the STA moves to the coverage area of AP2, and is associated with AP2. During this process, the IP address remains unchanged with service continuity.
- Before roaming, data is directly sent out by AP1. After roaming, data is forwarded from AP2 to AP1, and then sent out by AP1.

⚠ A STA can roam only when the SSIDs provided by AP1 and AP2 are the same.

1.3 Features

Basic Concepts

Association and Re-Association

Association: A STA selects an extended service area, and sends the asso frame to set up a connection with this extended service area.

Re-association: A STA moves from a service area of an extended service area to another service area, and is associated with a new AP. In this case, the STA sends the reasso frame.

STA, AP, and AC

STA: Is a wireless workstation that is equipped with the wireless network interface card (NIC), such as a portable computer or a mobile phone.

AP: Is a wireless access point that provides radio signals for the associated STA to access a wireless network.

AC: Is a wireless access controller that provides wireless connections and related service functions.

L2 Roaming and L3 Roaming

L2 roaming: The VLAN to which a STA belongs remains unchanged before and after roaming.

L3 roaming: The VLAN to which a STA belongs changes after roaming.

Centralized Forwarding and Local Forwarding

Centralized forwarding: All packets of a STA are forwarded by an AC.

Local forwarding: Control packets of a STA are processed by an AC, whereas data packets are directly forwarded by an AP.

Intra-AC Roaming and Inter-AC Roaming

Intra-AC roaming: A STA roams from one AP connected to an AC to another AP connected to the same AC.

Inter-AC roaming: A STA roams from an AP connected to an AC to another AP connected to a different AC.

Home AC and Foreign AC

- Home AC (HA): When a STA is associated with an AC in the mobility group for the first time, this AC is called HA of the STA.
- Foreign AC (FA): A STA is connected to an AC that is not the HA. This AC is called FA of the STA.

For intra-AC roaming, the HA and FA are the same.

Overview

Feature	Description
Mobility Group	After a mobility group is configured, a STA can roam to different ACs in the same mobility group.

Mobility List	The mobility list is an extension of the mobility group. The number of AC members in the mobility group is limited. The mobility list is introduced to extend the roaming scope of STAs without affecting roaming of the mobility group.
Checking the STA Roaming Status and Roaming Tracks	The status of all roaming STAs on the local AC and the roaming track of a STA can be displayed.
Suppressing STA Roaming Syslogs	The output rate of STA roaming syslogs is suppressed.
Disabling Roaming Based on WLANs	When multiple WLANs have been planned with the same SSID, roaming can be disabled based on the WLAN ID so that resources on the WLAN can be allocated properly. This ensures that STAs accessing a WLAN ID do not roam to other WLAN IDs with the same SSID.
Disabling Roaming Based on the Device	STAs do not roam when they move between ACs by disabling the inter-AC roaming function.

1.3.1 Mobility Group

The roaming scope of STAs within a WLAN cannot be expanded without limit. To enable a STA to roam among APs connected to different ACs and manage the roaming scope of STAs, configure a mobility group to include a group of ACs within the roaming scope of STAs.

Working Principle

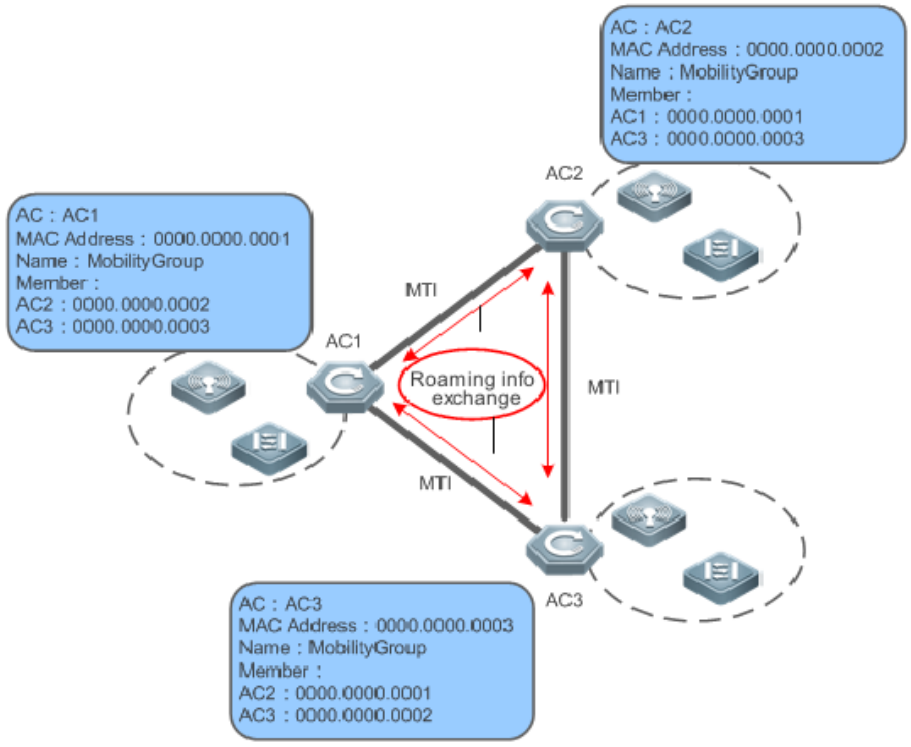
Each AC is configured with a list of other members of a mobility group. When a STA joins an AC, the AC sends out a message to all the other ACs in the mobility group. If it is the first time the STA accesses the mobility group, the initially connected AC (HA) will save information about the STA. When the STA roams to another AC (FA), the HA synchronizes the STA information to the FA. If this STA is roaming, the HA synchronizes the STA information to the FA after receiving a notification message.

Generally, the roaming STA information is exchanged only after roaming occurs. Before roaming occurs, the information synchronization function of the mobility group can be used to proactively share STA information among ACs in the mobility group. This saves time in STA roaming and improves the roaming efficiency.

↘ Topology of the Mobility Group

ACs in a mobility group encapsulate and transfer roaming information through the Controlling and Provisioning of Wireless Access Point (CAPWAP) tunnel. This technology reduces the re-authentication time on the RADIUS server after inter-AC roaming of STAs, and accelerates authentication of roaming STAs, facilitating seamless roaming. **Figure 1-5** shows the topology of the mobility group.

Figure 1-5 Topology of the Mobility Group



Remarks	The MTI is the communication tunnel between ACs. AC1, AC2, and AC3 are in the same mobility group. On each AC, another two ACs are configured as its mobility members.

1.3.2 Mobility List

A mobility list is an extension of a mobility group. The number of AC members in a mobility group is limited, so the mobility list is introduced to extend the roaming scope of STAs without affecting roaming of the mobility group.

Working Principle

↘ Comparison Between a Mobility List and a Mobility Group

Data exchange of roaming STAs in a mobility list is similar to that in a mobility group. The difference is as follows: Intra-group roaming adopts Proactive Key Caching (PKC), while inter-group roaming uses the mobility list that requires a roaming STA to complete the entire authentication process with the AAA/RADIUS server. Compared with intra-group roaming, inter-group roaming has lower efficiency. The similarity between them is that the roaming process is seamless and transparent for STAs.

When an AC is allocated to a specific mobility group, STAs connected to the AC are allowed to roam within the mobility group. If a mobility list is configured on the AC (with member ACs not in the same mobility group as the current AC), STAs on the current AC are allowed to roam across mobility groups.

1.3.3 Checking the STA Roaming Status and Roaming Tracks

To learn the roaming status and mobility of all STAs on an AC, you can check the status and roaming tracks of roaming STAs.

Working Principle

Information about roaming STAs is recorded on the HA, including the roaming type, connected WLAN, as well as VLANs, APs, and radios before and after roaming. Such information is stored, and deleted only when the STAs are deassociated.

The roaming track is recorded by default.

1.3.4 Suppressing STA Roaming Syslogs

STA roaming syslog suppression prevents a high CPU usage caused by a large amount of syslogs output during roaming of a large number of STAs.

Working Principle

The number of output syslogs per second is counted. When the number reaches the upper limit, no more syslog is output within the second. In the next second, the number of syslogs is counted again.

1.3.5 Disabling Roaming Based on WLANs

When multiple WLANs have been planned with the same SSID, roaming can be disabled based on the WLAN ID so that resources can be properly allocated on the WLAN. This ensures that users accessing a particular WLAN ID do not roam to other WLAN IDs with the same SSID.

Working Principle

When an AC receives a roaming request, it checks whether roaming is disabled for the incoming or outgoing WLAN. If so, roaming is not allowed, and the STA goes online normally.

1.3.6 Disabling Roaming Based on the Device

By default, after Layer 3 roaming occurs, a STA still uses the VLAN before roaming for communication on a network to ensure that the STA's IP address remains unchanged after roaming. However, in some special scenarios, STAs may need to use the VLAN assigned after roaming to communicate. This can be achieved by disabling roaming.

After roaming is disabled, moving a STA from one AP to another is referred to as migration. After migration, the STA uses the VLAN assigned after migration to communicate. Migration with the same VLAN before and after migration is called Layer 2 migration, while migration with different VLANs before and after migration is called Layer 3 migration.

For roaming on the entire network, ensure that the STA's IP address can be used for communication in a VLAN before and after roaming. Otherwise, the STA may fail to access the network after roaming.

By disabling the inter-AC roaming function, STAs can be prevented from roaming between ACs.

Working Principle

Roaming can be disabled based on centralized forwarding and local forwarding.

When roaming is disabled based on centralized forwarding, STAs associated with WLANs in centralized forwarding mode will use the VLAN mapped by the AP after Layer 3 roaming for communication.

Local forwarding works in the same manner. When roaming is disabled based on local forwarding, STAs associated with WLANs in local forwarding mode will use the VLAN mapped by the AP after Layer 3 roaming for communication.

For Layer 3 migration, the device checks whether the IP address of a STA is changed by default. If the IP address remains unchanged, the STA does not r-apply for an IP address and cannot access the Internet. The STA is disconnected to trigger the STA to go online and obtain the IP address again. If the IP address of the STA can be used for Internet access before and after Layer 3 migration, detecting IP address changes can be disabled.

Inter-AC roaming requires the use of the roaming tunnel, that is, the MTI tunnel to exchange packets. MTI tunnels fall into data and control channels, which use UDP as the transport-layer protocol. The data channel uses UDP port 5249, and the control channel uses UDP port 5248. The inter-AC roaming function can be used to control whether the roaming module monitors the corresponding port, thereby disabling the inter-AC roaming function.

1.4 Configuration

Configuration	Description and Command	
Configuring a Mobility Group	⚠ (Optional) It is used to implement the inter-AC roaming function.	
	mobility-group	Configures a mobility group.
	member	Adds or deletes a mobility member to or from the mobility group.
Configuring Proactive Information Exchange within the Mobility Group	⚠ (Optional) It is used to exchange STA information within the mobility group.	
	mobility-fast	Enables proactive information exchange within a mobility group.
Configuring a Mobility List	⚠ (Optional) It is used to add members to a mobility list.	
	list	Adds or deletes member ACs to or from the mobility list.
Configuring the Number of Times a Keepalive Packet Can Be Transmitted	⚠ (Optional) It is used to configure the maximum number of times a keepalive packet can be transmitted. If the value is exceeded, the keepalive attempt fails.	
	keepalive-count	Configures the maximum number of times a keepalive packet can be transmitted
Configuring the Interval at Which a Keepalive Packet Is Sent	⚠ (Optional) It is used to configure the interval at which a keepalive packet is sent.	
	keepalive-interval	Configures the interval at which a keepalive packet is sent.
	⚠ (Optional) It is used to test whether ACs in a mobility group are interconnected properly.	

Testing Roaming Connectivity_Starting_a_Roaming	mti-ping	Tests connectivity of tunnels between ACs in a mobility group.
Suppressing STA Roaming Syslogs	(Optional) It is used to suppress the output rate of STA roaming syslogs.	
	roaming logging rate-limit	Sets the output rate of STA roaming syslogs.
Preventing STA Roaming	(Optional) It is used to disable roaming on a specified WLAN.	
	roaming support wlan	Configures whether roaming is allowed within a specified WLAN.
Disabling Roaming Based on the Device	(Optional) It is used to disable roaming in some scenarios.	
	roaming central-unroam	Disables roaming in centralized forwarding.
	roaming local-unroam	Disables roaming in local forwarding.
	roaming disable	Disables inter-AC roaming.
	roaming local-layer2 direct	Configures migration for roaming in local forwarding mode.

1.4.1 Configuring a Mobility Group

Configuration Effect

- Configure a mobility group and add a mobility member to implement inter-AC roaming.
- The centralized forwarding mode is configured in the same way as the local forwarding mode.

Notes

To implement inter-AC roaming, ensure that the two ACs can communicate with each other normally.

Configuration Steps

Creating a Mobility Group

- (Optional) The configuration is mandatory if inter-AC roaming needs to be implemented. Run the **mobility-group** *group-name* command to create a mobility group.
- Configure at least one mobility group on each AC that involves inter-AC roaming.

Up to eight mobility groups can be created on an AC.

Command	**mobility-group** *group-name*
Parameter Description	*group-name*: Specifies the name of a mobility group.
Defaults	No mobility group is configured by default.
Command Mode	Global configuration mode

Usage Guide	N/A

Adding Mobility Members

- (Optional) The configuration is mandatory if inter-AC roaming needs to be implemented.
- Add at least one member to a mobility group on each AC that involves inter-AC roaming.
- After a mobility group is created, there is no mobility member in the group. Therefore, you need to add one or more mobility members.
- To ensure that information is efficiently and reliably synchronized between ACs within a mobility group, you must limit the number of members in the mobility group. A mobility group supports up to 24 mobility members.

Command	**member** {ip-address|ipv6-address}
Parameter Description	*ip-address:* Indicates the IPv4 address of a mobility member. *ipv6-address:* Indicates the IPv6 address of a mobility member.
Defaults	A new mobility group does not contain any member.
Command Mode	Mobility group configuration mode
Usage Guide	N/A

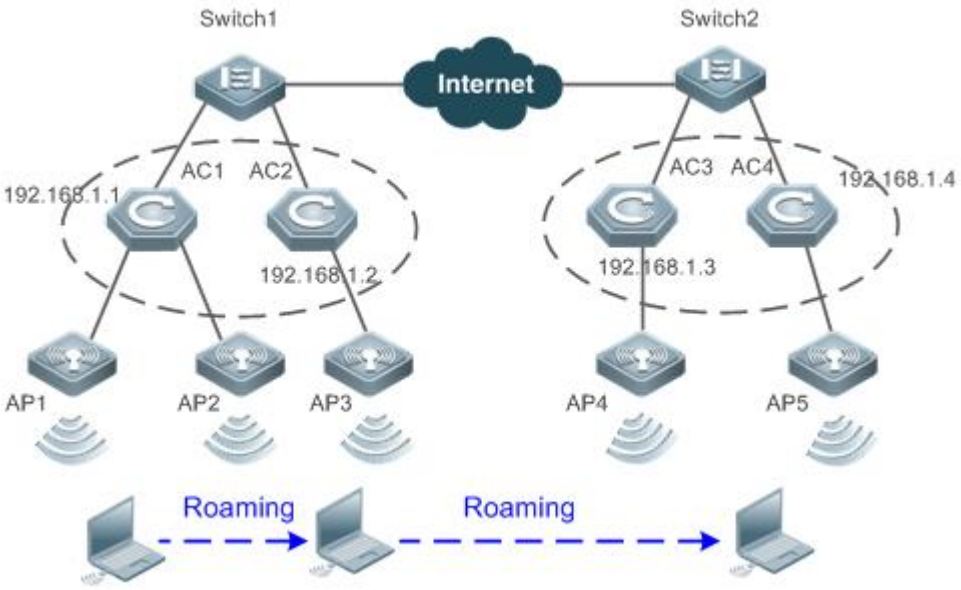
Verification

Check mobility group information to determine whether members are successfully added and whether connections are normal.

Configuration Example

All the configuration examples in this document are provided for the scenario of inter-AC roaming in centralized forwarding mode.

Configuring a Mobility Group and Adding a Member to this Group

Scenario **Figure 1-6**	 ● Inter-AC or intra-AC Roaming Scenario
Configuration Steps	● Set loopback addresses of AC1 and AC2 to 192.168.1.1 and 192.168.1.2 respectively, and ensure that one AC can be pinged successfully from another AC. ● Add a mobility group. ● Add a mobility member.

AC1	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#mobility-groupmgroup_name`
	`Hostname(config-mobility)#member 192.168.1.1`

AC2	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#mobility-groupmgroup_name`
	`Hostname(config-mobility)#member 192.168.1.2`

Verification	● Check mobility group information to determine whether the configurations are successful. ● Run the **show mobility status** *mgroup_name* command on each AC.

AC1	`Hostname# show mobility status mgroup_name`
	`Mobility Group mgroup_name`
	`Mobility Keepalive Interval..... 10`

	Mobility Keepalive Count..... 3 Mobility Group Status..... normal Mobility Members: IP Address Client/Server Data Tunnel Ctrl Tunnel 192.168.1.1Client OK Mobility List Members:
AC2	Hostname# show mobility status mgroup_name Mobility Group mgroup_name Mobility Keepalive Interval..... 10 Mobility Keepalive Count..... 3 Mobility Group Status..... normal Mobility Members: IP Address Client/Server Data Tunnel Ctrl Tunnel 192.168.1.2Client OK Mobility List Members:

Common Errors

- Mobility AC members fail to ping each other.
- The mobility group or members are not configured on an AC.
- The mobility group names are inconsistent.

1.4.2 Configuring Proactive Information Exchange within the Mobility Group

Configuration Effect

When roaming does not occur, an AC also shares STA information with other AC members in the mobility group.

Notes

A mobility group must be configured.

Configuration Steps

- (Optional) After configuring a mobility group on ACs, enter the mobility group configuration mode and enable proactive information exchange.
- (Optional) Configure fast roaming as required.

Command	mobility-fast
Parameter Description	N/A
Defaults	Proactive information exchange is disabled by default.
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

Check mobility group information. If the mobility group status is Fast Mode, the configuration is successful.

Configuration Example

Configuring Proactive Information Exchange within the Mobility Group

Configuration Steps	• Configure a mobility group. The configurations are omitted here. • Enable proactive information exchange within the mobility group.

AC	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#mobility-groupmgroup_name`
	`Hostname(config-mobility)# mobility-fast`

Verification	Check mobility group information.

AC	`Hostname# show mobility status mgroup_name`
	`Mobility Group mgroup_name`
	`Mobility Keepalive Interval..... 10`
	`Mobility Keepalive Count..... 3`
	`Mobility Group Status..... Fast Mode`
	`……b`

Common Errors

N/A

1.4.3 Configuring a Mobility List

Configuration Effect

When no more members can be added to a mobility group, configure a mobility list to implement roaming.

Notes

A mobility group must be configured.

Configuration Steps

- (Optional) Add members to the mobility list after a mobility group is configured on the AC. Run the **list** { *ip-address* | *ipv6-address* } command to add a member to the mobility list.
- If the number of mobility members exceeds the maximum value of the mobility group, you can add members to the mobility list as an alternative.

A mobility list supports up to 72 members.

Command	**list** {ip-address| ipv6-address}
Parameter Description	*ip-address*: Indicates the IPv4 address of a mobility member. *ipv6-address:* Indicates the IPv6 address of a mobility member.
Defaults	No mobility list is configured by default.
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

Check mobility group information to determine whether added members exist.

Configuration Example

Configuring a Mobility List

Configuration Steps	● Configure a mobility group. The configurations are omitted here. ● Add members to the mobility list.

AC	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#mobility-groupmgroup_name`
	`Hostname(config-mobility)# list 192.168.1.1`
	`Hostname(config-mobility)# list 192.168.1.2`

Verification	Check mobility list information.

AC	Hostname# show mobility status mgroup_name Mobility Group mgroup_name Mobility Keepalive Interval..... 10 Mobility Keepalive Count..... 3 Mobility Group Status..... Fast Mode Mobility Members: IP Address Client/Server Data Tunnel Ctrl Tunnel Mobility List Members: IP Address Client/Server Data Tunnel Ctrl Tunnel 192.168.1.2 Client OK OK 192.168.1.1 Client OK OK

Common Errors

N/A

1.4.4 Configuring the Number of Times a Keepalive Packet Can Be Transmitted

Configuration Effect

(Optional) Configure the number of times a keepalive packet can be transmitted. If the value is exceeded, the keepalive attempt fails.

Notes

A mobility group must be configured and has at least one mobility member.

Configuration Steps

- (Optional) Configure a mobility group on the AC and enter the mobility group configuration mode.
- The maximum number of times a keepalive packet can be transmitted does not need to be changed by default. If the network is unstable, you can increase this value.

Command	**keepalive-count** *counts*
Parameter Description	*counts*: Indicates the number of times a keepalive packet can be transmitted. The value ranges from 2 to 30.
Defaults	The default value is 4 after a mobility group is created.
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

Check mobility group information. The maximum number of times a keepalive packet can be transmitted should be displayed.

Configuration Example

Configuring the Number of Times a Keepalive Packet Can Be Transmitted

Configuration Steps	● Configure a mobility group. The configurations are omitted here. ● Set the number of times a keepalive packet can be transmitted to 5.
AC	`Hostname(config)#mobility-group mgroup_name` `Hostname(config-mobility)# keepalive-count 5`
Verification	Check the mobility group configuration.

AC	`Hostname# show mobility status mgroup_name`
	`Mobility Group mgroup_name`
	`Mobility Keepalive Interval..... 10`
	`Mobility Keepalive Count..... 5`
	`Mobility Group Status..... normal`

Common Errors

N/A

1.4.5 Configuring the Interval at Which a Keepalive Packet Is Sent

Configuration Effect

(Optional) Configure the interval at which a keepalive packet is sent.

Notes

A mobility group must be configured and has at least one mobility member.

Configuration Steps

- (Optional) Configure a mobility group on the AC and enter the mobility group configuration mode.
- The interval at which a keepalive packet is sent is 10s by default. If the network is unstable, you can increase the interval.

Command	**keepalive-interval** *seconds*

Parameter Description	*seconds*: Indicates the interval at which a keepalive packet is sent, in seconds. The value ranges from 1 to 30.
Defaults	The default value is 10s after a mobility group is created.
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

Check mobility group information. The interval at which a keepalive packet is sent should be displayed.

Configuration Example

Configuring the Interval at Which a Keepalive Packet Is Sent

Configuration Steps	● Configure a mobility group. The configurations are omitted here. ● Set the interval at which a keepalive packet is sent to 20s.
AC	`Hostname(config)#mobility-group mgroup_name` `Hostname(config-mobility)# keepalive-interval20`
Verification	Check the mobility group configuration.

AC	`Hostname# show mobility status mgroup_name`
	`Mobility Group mgroup_name`
	`Mobility Keepalive Interval..... 20`
	`Mobility Keepalive Count..... 4`
	`Mobility Group Status..... normal`

Common Errors

N/A

1.4.6 Testing Roaming Connectivity

Configuration Effect

(Optional) Start a connectivity test to check whether member ACs are connected to each other normally.

Notes

A mobility group must be configured and has at least one mobility member.

Configuration Steps

- (Optional) After configuring a mobility group on an AC, enter the mobility group configuration mode to start a connectivity test.
- Start a connectivity test to check whether member ACs in the mobility group communicate with each other normally.

Command	**mti-ping** {ip-address|ipv6-address}
Parameter Description	*ip-address*: Indicates the IPv4 address of a mobility member. *ipv6-address:* Indicates the IPv6 address of a mobility member.
Defaults	N/A
Command Mode	Mobility group configuration mode
Usage Guide	N/A

Verification

Check the test result.

Configuration Example

Starting a Roaming Connectivity Test

Configuration Steps	• Configure a mobility group and add mobility members. The configurations are omitted here. • Start a roaming connectivity test.

AC	`Hostname(config)#mobility-group my_group_name`
	`Hostname(config-mobility)#mti-ping 192.168.1.2`
	`Sending 4, MTI packet to  192.168.1.1, timeout is 2 seconds:`
	`!!!!`
	`Success rate is 100 percent (4/4)`

Verification	Check the test result.

AC	`Sending 4, MTI packet to  192.168.1.1, timeout is 2 seconds:`
	`!!!!`
	`Success rate is 100 percent (4/4)`

Common Errors

The **mti-ping** command is different from the **ping** command, that is, successful execution of the **ping** command does not mean that execution of the **mti-ping** command is also successful. The **mti-ping** command is applicable to mobility group members.

1.4.7 Suppressing STA Roaming Syslogs

Configuration Effect

Even if STAs roam frequently, the number of roaming syslogs output per second does not exceed the limit.

Notes

N/A

Configuration Steps

Configuring the Syslog Suppression Rate

- (Optional) The configuration is performed on an AC. Run the **roaming logging rate-limit** command to configure the syslog suppression rate.
- Configure the syslog suppression rate. A larger rate configured indicates that more syslogs can be output per second.

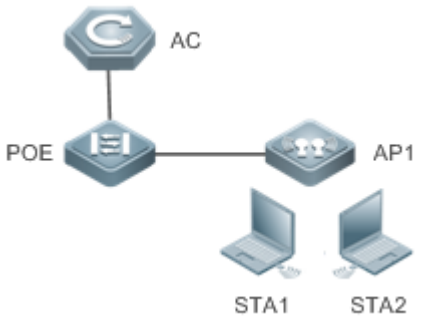
Command	**roaming logging rate-limit** *limit-num*
Parameter Description	*limit-num*: Indicates the syslog suppression rate, which is expressed in records per seconds. The value range is from 1 to 10000.
Defaults	Less than five syslog records are output per second by default, that is, the maximum syslog output rate is 5 records per second.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Run the **show running** command to check whether the syslog suppression rate is successfully configured.

Configuration Example

Suppressing STA Roaming Syslogs

Scenario **Figure 1-7**	
Configuration Steps	Configure the STA syslog suppression rate.

AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# roaming logging rate-limit 30
Verification	After the CAPWAP tunnel is established between an AP and an AC, check the configuration.
AC	AC# show running roaming logging rate-limit 30 !

Common Errors

N/A

1.4.8 Preventing STA Roaming

Configuration Effect

STAs are prevented from roaming within a WLAN.

Notes

N/A

Configuration Steps

↘ Preventing STA Roaming within a WLAN

- (Optional) The configuration is performed on an AC. Run the **roaming support wlan** command to configure the device to permit STA roaming within a specified WLAN.
- Roaming is permitted by default. Run the **no roaming support wlan** command to prevent STA roaming.

Command	**roaming support wlan** *wlan-id*
Parameter Description	*wlan-id*: Specifies the ID a WLAN where roaming is disabled.
Defaults	Roaming is permitted by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Run the **show running** command to check whether roaming is prevented.

Configuration Example

Preventing STA Roaming

Configuration Steps	Configure roaming prevention within WLAN 100.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# no roaming support wlan 100`

Verification	After the CAPWAP tunnel is established between an AP and an AC, check the configuration.

AC	`AC# show running`
	`no roaming support wlan 100`
	`!`

Common Errors

N/A

1.4.9 Disabling Roaming Based on the Device

Configuration Effect

STAs can communicate using the VLAN mapped to the AP after Layer 3 roaming.

Notes

Some STAs do not initiate a new DHCP process after roaming and directly use the IP address before roaming for communication, so the STA's IP address needs to be used for forwarding in both VLANs before and after roaming, which requires collaboration on the entire network. If the STA's IP address cannot be used for forwarding in the VLAN after roaming, the STA will fail to access the network after roaming.

Configuration Steps

Disabling Roaming in Centralized Forwarding Mode

- (Optional) This configuration does not affect the STAs who have already roamed, and new STAs who experience roaming in centralized forwarding mode will communicate using the VLAN after roaming.
- The device does not check whether the IP address of the STA is changed during Layer 3 migration.
- If there are no special requirements, this configuration is not required.

Command	**roaming central-unroam**

Parameter Description	N/A
Defaults	In centralized forwarding mode, STAs still communicate using the VLAN before roaming.
Command Mode	Global configuration mode
Usage Guide	N/A

Disabling Inter-AC Roaming

- If there are no special requirements, this configuration is not required.

Command	**roaming disable**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Disabling Roaming in Local Forwarding Mode

- (Optional) This configuration does not affect the STAs who have already roamed, and new STAs who experience roaming in local forwarding mode will communicate using the VLAN after roaming.
- The device does not check whether the IP address of the STA is changed during Layer 3 migration.
- If there are no special requirements, this configuration is not required.

Command	**roaming local-unroam**
Parameter Description	N/A
Defaults	In local forwarding mode, STAs still communicate using the VLAN before roaming.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Migration for Roaming in Local Forwarding Mode

Whether this configuration is supported depends on the actual product version.

- (Optional) This configuration does not affect the STAs who have already roamed, and new STAs who experience roaming in local forwarding mode adopt migration.
- This function is the same as the function of the **roaming local-unroam** command. The difference is that the device checks whether the STA's IP address is changed after roaming by default.

- If there are no special requirements, this configuration is not required.

Command	roaming local-layer2 direct
Parameter Description	N/A
Defaults	In local forwarding mode, Layer 2 roaming uses migration and Layer 3 roaming does not use migration.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Run the **show running** command to check whether the configuration is successful.

Configuration Example

Disabling Roaming in Local Forwarding Mode

Configuration Steps	Disable roaming in local forwarding mode.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# roaming local-unroam
Verification	Run the **show run** command to check the configuration.
AC	AC# show running roaming local-unroam !

Disabling Inter-AC Roaming

Configuration Steps	Disable the inter-AC roaming function.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# roaming disable
Verification	Run the **show run** command to display the configuration.
AC	AC# show running roaming disable

	!

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show mobility summary	Displays the configuration of all mobility groups.
show mobility status *group-name*	Displays the configuration of a specified mobility group.
show mobility statistics	Displays roaming statistics.
show mobility user [*mac-address*]	Displays roaming STA information.
show mobility user roam-track *mac-address*	Displays roaming tracks of roaming STAs.

1 Configuring Zero Roaming

Whether this function is supported depends on the actual product version.

1.1 Overview

With the development of medical information technology, mobile healthcare services have become increasingly important. The WLAN responsible for supporting the mobile healthcare services has strict requirements on the latency, packet loss, and bandwidth.

Medical staff needs to carry handheld devices frequently and process tasks at any time. During the entire process, quick response is required without client connection latency and data transmission delay. The mobile medical service range must cover all patients, even those in the innermost of wards, with requirements including picture archiving and communication system (PACS) image calling and medical condition update. The handheld clients used for mobile healthcare services generally require high wireless signal quality, where the signal strength in the ward needs to be above –60 dBm. Additionally, they are also highly sensitive to packet loss during roaming, which may cause service interruptions.

Zero roaming is targeted for healthcare scenarios. It can prevent problems caused by roaming and signal overlapping, such as mobile medical service delay, packet loss, and poor performance.

1.2 Applications

Application	Description
Zero Roaming	Applies to the wireless medical scenario.
PoE	Applies to the Internet of Things (IoT) scenario.
Zero Roaming+	Applies to the wireless medical scenario.

1.2.1 Zero Roaming

Scenario

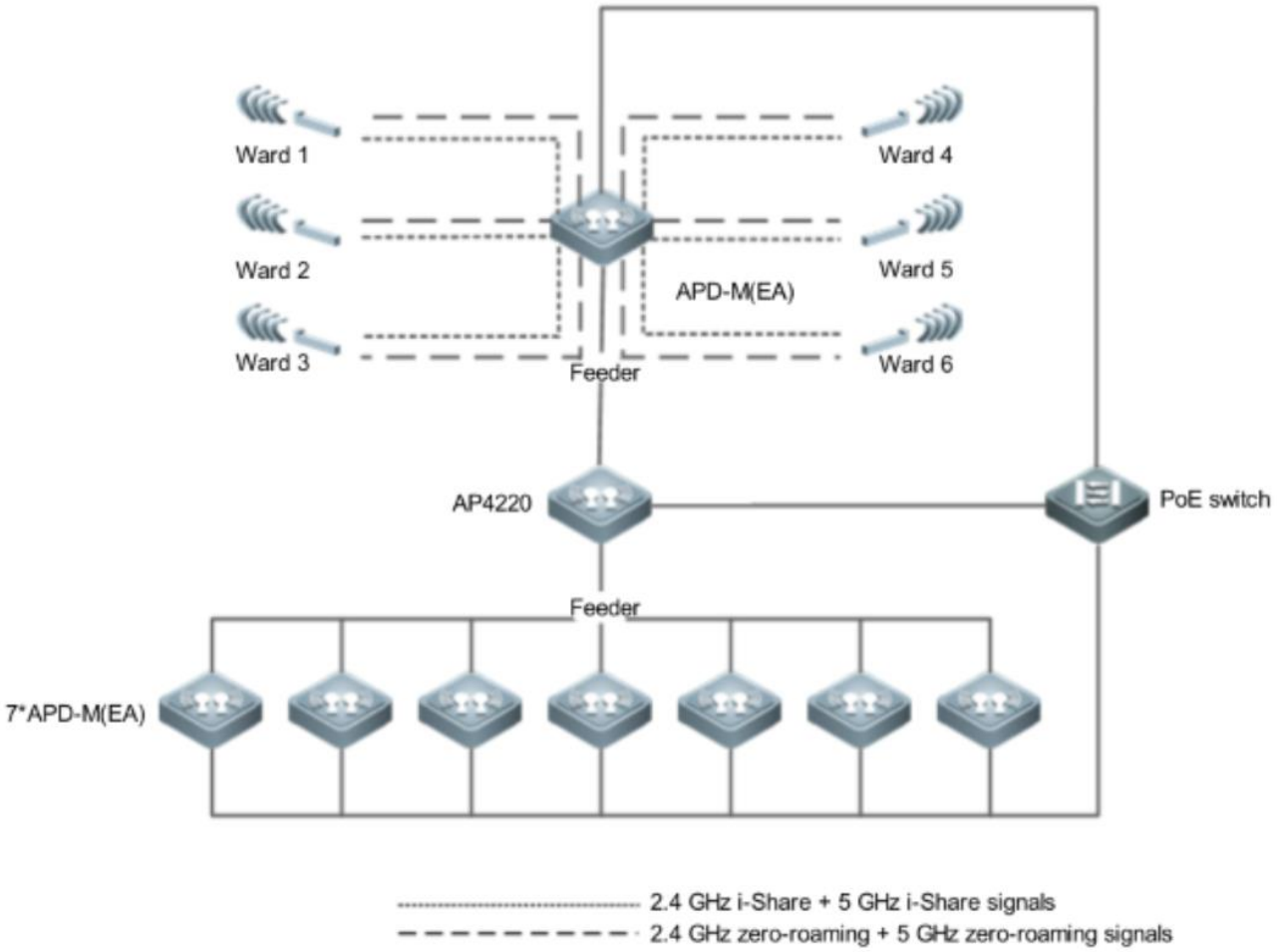
The application scenario of the third-generation zero-roaming medical i-Share solution is as follows:

1. The network is composed of one zero-roaming AP (RG-AP4220) and multiple i-Share units (RG-APD-M(EA)).
2. The zero-roaming AP provides eight channels of signals to an i-Share unit through a feeder.
3. An i-Share unit provides six channels of signals. Therefore, each i-Share cell can cover 6 wards, and all 48 wards are covered in this scenario.
4. The third-generation zero-roaming medical i-Share solution provides the following two operating modes:

- Mode 1: The 5G zero-roaming function is enabled by default. In this case, the zero-roaming AP works in dual-band mode, while the i-Share unit works in single-stream mode on 5G.

- Mode 2: The 5G zero-roaming function is disabled. The zero-roaming AP works in the single 2.4 G band, while the i-Share unit works in the dual-stream 802.11ac mode on 5G.

1.2.1.1.1 Medical Deployment



Deployment

Configure the devices as follows:

1. The 5G zero-roaming function is enabled by default. Both the zero-roaming AP and the i-Share unit work in single-stream mode on 5G, and the 5G signal of the zero-roaming AP serves as the 5G zero-roaming access signal.
2. When the 5G zero-roaming function is disabled, the 5G signal of the zero-roaming AP is disabled in wards covered by the designated i-Share unit, and the 5G signal of the i-Share cell works in dual-stream mode.

1.2.2 PoE on a Wired Port

Scenario

The i-Share unit is connected to the HPoE switch, and the common AP is connected to the second downlink port of the i-Share unit.

1.2.2.1.1 HPoE Scenario



Deployment

The i-Share unit must be connected to an HPoE-powered device. Enable the PoE function on the second downlink port of the i-Share unit, and power on a common AP for startup.

1.2.3 Zero Roaming+

Scenario

The scenario of zero roaming+ is similar to that of the third-generation zero-roaming medical i-Share solution. The zero roaming AP is HAP4720 and the i-Share unit is HAP-APD that does not support access to an extranet.

1. The network is composed of one zero-roaming AP (RG-HAP4720) and multiple i-Share units (RG-HAP-APD).
2. The zero-roaming AP evenly distributes the zero-roaming signals into 8 channels, and connects the i-Share units through feeders.
3. An i-Share unit splits the signals into 6 channels. Each i-Share unit can cover 6 wards, and all together 48 wards can be covered in this scenario.

Deployment

1. If the zero-roaming AP is powered by an HPoE switch, it can work in dual-band (2.4 GHz and 5 GHz) mode.
2. If the zero-roaming AP is powered by a common PoE device or an i-Share+ host, it only supports the single-band mode. By default, the RG-HAP4720 works in 5 GHz band. You can use a command to switch to the 2.4 GHz band.

1.3 Features

Basic Concepts

↘ Zero Roaming

When there are multiple APs on a network and signal coverage ranges among APs overlap, a wireless STA can move within the coverage area of the entire wireless local area network (WLAN). The wireless network interface card (NIC) can automatically discover an AP with the stronger signal around and send and receive data through this AP, ensuring a nonstop network connection. This is called wireless roaming.

A wireless STA is both the decision maker and the initiator of a roaming action, and the roaming decision may vary for different NICs and STAs. In the medical industry, PDAs used by wireless STAs may not support roaming or may have

poor roaming performance, which can affect user experience. The zero-roaming function can effectively solve the roaming issues for PDAs in this scenario.

The zero roaming function ensures that the same wireless SSID signal always exists within the range covered by the zero-roaming AP. Therefore, the wireless client will not encounter packet loss or roaming during moving.

Overview

Feature	Description
Zero Roaming	Enables the 5 GHz zero roaming function.
Wired-Port PoE	Enables the wired-port PoE function.
Zero Roaming+	Bounds the i-Share unit and zero-roaming AP.

1.3.1 Zero Roaming

Working Principle

The zero-roaming AP feeds signals into multiple i-Share units through a feeder, which then control the signals to be fed into multiple coverage areas through the feeder. When wireless STAs move within the signal coverage area of the zero-roaming AP, the signal is provided by the zero-roaming AP. In this case, roaming will not occur.

1.3.2 Wired-Port PoE

Working Principle

Power over Ethernet (PoE) is a technology for supplying direct current (DC) power to IP-based clients (such as the IP phone, WLAN AP, and webcam) while transmitting data signals of these devices without changing the existing Ethernet category 5 cabling infrastructure. PoE is also referred to as Power over LAN (PoL) or Active Ethernet or Ethernet power supply that complies with 802.3af/at/bt standards.

1.3.3 Zero Roaming+

Working Principle

A zero-roaming AP feeds signals into multiple i-Share cells through a feeder, which then control the signals to be fed into multiple coverage areas through the feeder. When wireless STAs move within the signal coverage area of the zero-roaming AP, the signal is provided by the zero-roaming AP. In this case, roaming will not occur.

The zero-roaming AP feeds signals into i-Share units, but the AC cannot detect the relationship between the i-Share units and the zero-roaming AP. To better manage the network, take the following measures:

- Add a binding relationship between the i-Share units and zero-roaming AP.
- Rename the connected i-Share units and bind MAC addresses to them based on the feeder ports R1 to R8 of the zero-roaming AP.
- Rename the connected antennas based on the feeder ports R1 to R6 of i-Share units.

Therefore, the AC can intuitively obtain the number of i-Share units connected to each zero-roaming AP, feeder port information, and antenna port information for each i-Share unit.

1.4 Configuration

Configuration	Description and Command	
Configuring Zero Roaming	(Optional) It is used to configure the zero roaming function.	
	zero-roaming enable	Configures the 5 GHz zero roaming function.
Configuring PoE	(Optional) It is used to configure the PoE function on a wired port.	
	wired-poe enable port *num*	Configures the PoE function on a wired port.
Configuring Zero Roaming+	(Optional) It is used to bind an HAPD to an AP.	
	hapd *num name*	Configures the name of the i-Share unit (HAP-APD).
	hapd mac *H.H.H*	Configures the MAC address of the i-Share unit (HAP-APD).
	hapd *num* **antenna-id** *ant-id ant-name*	Configures the name of the antenna connected to the i-Share unit (HAP-APD).

1.4.1 Configuring Zero Roaming

Note

Whether this function is supported depends on the actual product version.

This function is supported on all wireless ACs and is supported only on APs with the model of RG-APD-M(EA).

Configuration Effect

Enable the 5 GHz zero roaming function.

Notes

If the device does not support the 5 GHz zero roaming function, the configuration does not take effect. Only RG-APD-M(EA) supports the 5 GHz zero roaming function.

Configuration Steps

Enabling Zero Roaming on a Designated AP

- Optional. Run the **zero-roaming** command in AP configuration mode to enable the zero roaming function.
- You can only enable the 5 GHz zero roaming function only on APs that support this function.

Command	**zero-roaming enable**
Parameter Description	**enable**: Enables the zero roaming function.

Defaults	The zero roaming function is enabled by default.
Command Mode	AP configuration mode
Usage Guide	Run this command to enable the 5 GHz zero roaming function on an AP. The configuration does not take effect on devices that do not support zero roaming.

Verification

Run the **show ap-config running** *ap-name* command on the AC to check whether the configuration is successful. Run the **show run** command on the AP to check whether the configuration is successful.

Configuration Example

Enabling Zero Roaming on a Designated AP

Configuration Steps	Enable the 5 GHz zero roaming function on a designated AP.

	`Hostname# configure terminal`
	`Hostname(config)#ap-config apd-ea`
	`Hostname(config-ap)#no zero-roaming enable`
	`Hostname(config-ap)#zero-roaming enable`

Verification	● Run the following commands to check the configuration status of the 5 GHz zero roaming function after it is enabled on the AP. ● Run the **show ap-config running** *ap-name* command on the AC to display the configuration status.

	Configuration on the AC
	`Ruijie(config)#show ap-config running apd-ea`
	`!`
	`ap-config apd-ea`
	`...`
	`no zero-roaming enable`
	`...`
	`...`
	`!`

1.4.2 Configuring PoE on a Wired Port

Configuration Effect

Enable PoE on a wired port.

Notes

- If the device does not support the wired port, the configuration does not take effect. The i-Share unit supports the wired port.
- If Port 1 of the device is not powered through HPoE, the configuration does not take effect.

- i-Share units support PoE only on LAN 2 ports.

Configuration Steps

Enabling Wired-Port PoE on Designated AP

- Optional. Run the following command in AP configuration mode to enable the PoE function on a wired port.
- You can enable this function only on APs that support PoE on a wired port.

Command	**wired-poe enable port** *num*
Parameter Description	*num*: Indicates the number of a wired port.
Defaults	The PoE function on a wired port is disabled by default.
Command Mode	AP configuration mode on the AC
Usage Guide	This command can be used to enable the PoE function on a wired port of an AP. The configuration does not take effect on devices that do not this function.

Verification

Run the **show ap-config running** *ap-name* command on the AC to check whether the configuration is successful.

Configuration Example

Enabling Zero Roaming on a Designated AP

Configuration Steps	Enable the PoE function on a wired port of a designated AP.

	`Ruijie# configure terminal`
	`Ruijie(config)#ap-config apd-ea`
	`Ruijie(config-ap)#wired-poe enable port 2`

Verification	● Run the following commands to check the configuration after it is enabled on the AP. ● Run the **show ap-config running** *ap-name* command on the AC to display the configuration.

	Configuration on the AC
	`Ruijie(config)#show ap-config running apd-ea`
	`!`
	`ap-config apd-ea`
	`...`
	`wired-poe enable port 2`
	`...`
	`...`
	`!`

1.4.3 Configuring Zero Roaming+

Configuration Effect

After i-Share units are bound to a zero-roaming AP, the antenna and feeder information of i-Share units can be uploaded to the AC through the zero-roaming AP. The AC can display the RG-HAP-APD's feeder status and the relationship between antennas, i-Share units, and RG-HAP4720.

Notes

None

Configuration Steps

Configuring the Name of a i-Share Unit

- (Optional) Configure the name of an HAP-APD connected to a feeder port on the HAP4720.

Command	**hapd** *num name*
Parameter Description	*num*: Indicates the number of a feeder port of the zero-roaming AP that is connected to the i-Share unit. The value range is from 1 to 8. *name*: Indicates the new name the i-Share unit.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the MAC Address of the i-Share Unit

- (Optional) Pre-configure the MAC address for the i-Share unit connected to the zero-roaming AP.

Command	**hapd** *num* **mac** *mac-address*
Parameter Description	*num*: Indicates the number of a feeder port of the zero-roaming AP that is connected to the i-Share unit. The value range is from 1 to 8. *mac-address*: Indicates the MAC address of the i-Share unit.
Defaults	
Command Mode	AP configuration mode
Usage Guide	

Configuring the Name of an Antenna of an HAP-APD

- Optional. Name the antenna connected to a feeder port on an HAP-APD.

Command	**hapd** *num antenna-id ant-id ant-name*
Parameter Description	*num*: Indicates the number of a feeder port corresponding to R1 to R8 on the zero-roaming AP (APHAP4720) that is connected to the i-Share unit. The value range is from 1 to 8. *ant-id*: Indicates the number of an antenna (R1 to R6) connected to the i-Share unit (HAP-APD). The value range is from 1 to 6. *ant-name*: Indicates the name of the antenna connected to the i-Share unit.
Defaults	No antenna name is configured by default.
Command Mode	AP configuration mode
Usage Guide	The configuration takes effect only on devices that support HAP-APD binding.

Verification

Run the **show ap-config running** *ap-name* command on the AC to display the configuration.

Configuration Example

Binding a Specified HAP-APD to an AP

Configuration Steps	Bind a specified HAP-APD to an AP.
	Ruijie# configure terminal Ruijie(config)#ap-config HAP4720 Ruijie(config-ap)#hapd 1 Hallway on floor 1 Ruijie(config-ap)#hapd 1 mac 0800.1111.2222 Ruijie(config-ap)#hapd 1 antenna-id 1 Ward 101 Ruijie(config-ap)#hapd 1 antenna-id 2 Ward 102 Ruijie(config-ap)#hapd 1 antenna-id 3 Ward 103 Ruijie(config-ap)#hapd 1 antenna-id 4 Ward 104 Ruijie(config-ap)#hapd 1 antenna-id 5 Ward 105 Ruijie(config-ap)#hapd 1 antenna-id 6 Ward 106
Verification	Run the following commands to display the configuration after the specified HAP-APD is bound to an AP: ● Run the **show ap-config running** *ap-name* command on the AC to display the configuration. ● Run the **show run** command on the AP to display the configuration.
	AC: Ruijie(config)#show ap-config running HAP4720 ! ap-config HAP4720 ... hapd 1 Hallway on floor 1 hapd 1 mac 0800.1111.2222 hapd 1 antenna-id 1 Ward 101 hapd 1 antenna-id 2 Ward 102 hapd 1 antenna-id 3 Ward 103 hapd 1 antenna-id 4 Ward 104 hapd 1 antenna-id 5 Ward 105 hapd 1 antenna-id 6 Ward 106 ... ... !

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show hapd antenna { **all** | **single** *ant-name* }	Displays the antenna and feeder status of the i-Share unit.
show hapd antenna summary	Displays the configuration of the i-Share unit.
show hapd information	Displays the status of the i-Share unit connected to the zero-roaming AP.

Debugging

N/A

1 Configuring SFN

1.1 Overview

Same Frequency Net (SFN) is a wireless solution that virtualizes multiple access points (APs) into a single AP within a wireless local area network (WLAN).

In industries such as healthcare, handheld devices such as personal digital assistants (PDAs) often lack support for roaming or have poor roaming performance, resulting in a suboptimal user experience with APs. SFN technology effectively addresses these roaming issues. SFN operates on a single channel to deploy the network, enabling zero roaming. By deploying multiple layers of independent intra-frequency networks, it supports high-density deployment while simplifying both installation and maintenance. However, one downside of using a single channel for deployment is that, in dense environments, co-frequency interference can become significant, which may negatively impact overall network throughput.

Based on the preceding analysis, you are advised to use SFN in the following scenarios:

- Scenarios where APs are densely deployed, with low wireless throughput requirements but high roaming requirements, such as in healthcare, logistics, and similar industries
- Scenarios with less dense AP deployment but involving high-speed moving wireless terminals

Protocols and Standards

IEEE 802.11

1.2 Applications

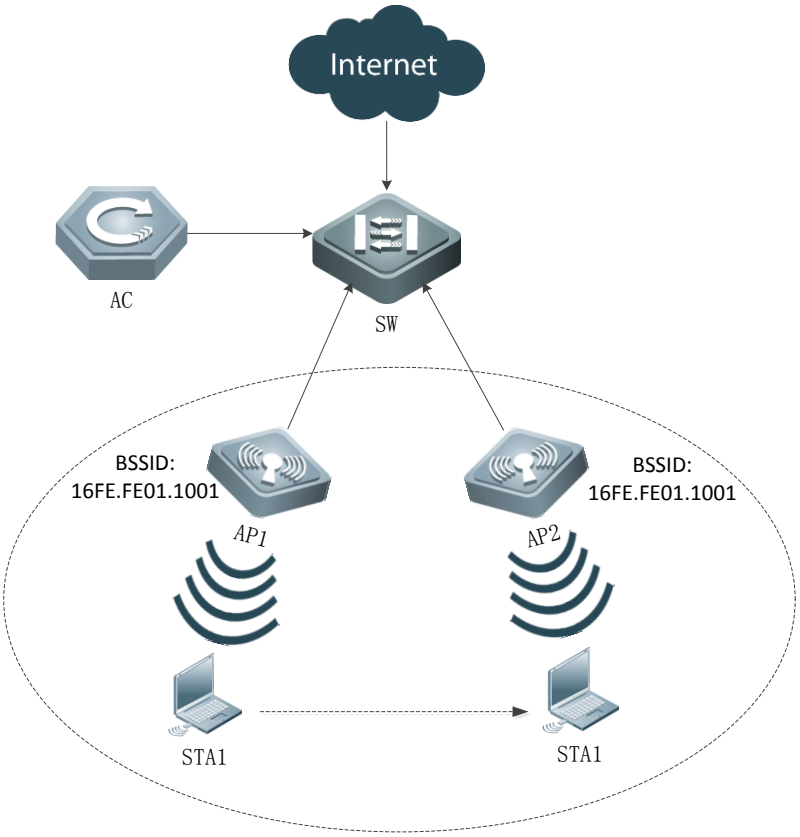
Application	Description
SFN Application	SFN is applicable to thin AP topologies and the following scenarios: ● Scenarios where APs are densely deployed, with low wireless throughput requirements but high roaming requirements, such as in healthcare, logistics, and similar industries ● Scenarios with less dense AP deployment but involving high-speed moving wireless terminals

1.2.1 SFN Application

Scenario

Stations (STAs) are associated with the SFN network. Initially, AP1 provides the strongest signal and the wireless link service. As a STA moves, the signal from AP2 becomes stronger, and SFN technology automatically switches the service to AP2, which then takes over as the wireless link service provider for the STA.

Figure 1-1SFN Application Scenario



Deployment

SFN Network Implementation

1. Deploy the fit AP environment as needed.
2. Create an SFN group and add the specified AP group to the SFN group. Then all APs in the AP group form a large virtual AP to provide services for STAs.
3. Ensure that all physical APs that constitute the virtual AP provide full coverage for STAs' active area to achieve seamless roaming of STAs.
4. Ensure that the physical AP providing the wireless service for STAs will switch accordingly when a STA moves within the coverage area of the virtual AP. No packet loss occurs during handover, resulting in seamless roaming.

Notes

The configuration points on the device are as follows:

1. Create an SFN group.
2. Enable SFN for the specified radio.
3. For the SFN group, configure the channel and RSSI threshold for STA handover.
4. Add the specified AP group to the SFN group.

1.3 Features

Basic Concepts

BSSID

The Base Service Set Identifier (BSSID) is a 48-bit locally managed IEEE MAC address. Each Base Service Set (BSS) is assigned a BSSID to identify itself. In an SFN group, each STA is assigned a unique BSSID, which is automatically generated by the access controller (AC) and assigned to the AP.

SFN Group

An SFN group refers to configuring all APs within a specified AP group to operate on the same frequency, with consistent configuration across all APs in the group.

Overview

Feature	Description
SFN Group	Creates an SFN network and configures network parameters.

1.3.1 SFN Group

Working Principle

AC Control Mode Intra-frequency Handover

The basic principle of SFN is that all specified APs within a network operate on the same channel and broadcast the same SSID. When a STA associates with an AP, a unique BSS is created based on the STA's Association Identifier (AID). The AP providing this BSS is determined by the AC, based on the STA's location. From the STA's perspective, all APs broadcasting the same SSID within the network can be viewed as a single virtual AP. This virtual AP can consist of hundreds or even thousands of physical APs, enabling coverage across areas such as hospital wards or dormitories. As the STA moves within this coverage area, it will appear to stay connected to the same AP, without experiencing roaming. In practice, the STA may be connected to different physical APs. The specific AP that the STA connects to is determined by the AC, which considers factors such as the STA's Received Signal Strength Indicator (RSSI) on the AP and AP's load. The handover between APs is managed by the AC, and the STA is unaware of the transition.

AP Control Mode Intra-frequency Handover

The basic principle is similar to that in "AC Control Mode Intra-frequency Handover." The difference is that the specific AP associated with a STA is determined by the neighboring AP and associated AP when the STA moves within the coverage area of the SFN network. If the neighboring AP has sufficient capacity and the STA's RSSI is stronger than the RSSI threshold of the associated AP by a specific threshold, the STA will request a handover. The associated AP then decides on the optimal AP and migrates the STA to it. The handover between APs is managed by the AC, and the STA is unaware of the transition.

Unique Association Between a STA and a Physical AP

All APs on the SFN network are virtualized as a single AP. For any STA, at any given moment, it is associated with only one physical AP, which provides wireless services for the STA.

STA Handover Between APs

No matter where the STA moves within the coverage area of the SFN network, it will not experience disconnection. However, as the STA's location changes, the physical AP providing wireless services for the STA may change. The condition for this change is that the SFN network system determines that another AP can provide better wireless service for the STA, in which case the physical AP serving the STA will be switched to this new AP.

1.4 Configuration

Configuration	Description and Command	
Creating an SFN Group and Associating the SFN Group with a Specified AP Group	(Mandatory) It is used to create an SFN group and apply it to the specified AP group, and to enable SFN for the specified radio.	
	sfn-group	Creates an SFN group.
	ap-group	Associates the SFN group with an AP group.
	enable-sfn radio	Enables SFN for the specified radio.
Configuring SFN Group Information	(Optional) It is used to enable the specified radio to support 802.11a/802.11g/802.11ac/802.11ax, configure the MCS index of 802.11n/802.11ac for the specified radio, configure the receiving/transmitting antenna type of the specified radio, configure the delivery traffic indication message (DTIM) period for the specified radio, configure a channel/channel width/working frequency band for the specified radio, configure the RSSI threshold for STA handover, configure the OUI field for the BSSID of a virtual port, and enable AP control mode intra-frequency handover.	
	11nasupport enable	Enables the specified radio to support 802.11a.
	11ngsupport enable	Enables the specified radio to support 802.11g.
	11acsupport enable	Enables the specified radio to support 802.11ac.
	11axsupport enable	Enables the specified radio to support 802.11ax.
	802.11n mcs support	Configures the MCS index of 802.11n for the specified radio.
	802.11ac mcs support	Configures the MCS index of 802.11ac for the specified radio.
	antenna	Configures the receiving/transmitting antenna type of the specified radio.
	beacon dtim-period	Configures the DTIM period for the specified radio.
	channel	Configures a channel for the specified radio.
	chan-width	Configures the channel width for the specified radio.
	handoff-rssi-thresh	Configures the RSSI threshold for STA handover.
	radio-type	Configures the working frequency band for the specified radio.
	sfn-vp-oui	Configures the OUI field for the BSSID of a virtual port.
	handoff-ap-mode enable	Enables AP control mode intra-frequency handover.

1.4.1 Creating an SFN Group and Associating the SFN Group with a Specified AP Group

Configuration Effect

- Create an SFN group.
- Apply the SFN group to the specified AP group.
- It takes effect after you enable the SFN function on the specified radio.

Notes

- Ensure that all APs in the same SFN group use the same configuration before joining the group. After APs are added to an SFN group, you are not advised to change configurations of some APs individually. Some common commands similar to those in AP configuration mode are available in SFN group configuration mode, allowing the configuration of radio attributes of the specified frequency band for all APs within the same group. If other AP configurations need to be changed, you are advised to remove APs from the SFN group first.
- Due to differences in wireless capabilities between different models of APs, you are not advised to add them to the same SFN group.
- By default, APs do not join any SFN group, so AP groups do not support the SFN configuration by default.
- When you delete the SFN group, its associated AP group is automatically disassociated, and all APs in the AP group automatically exit the SFN group.
- An AP group can be associated with only one SFN group, and an SFN group can be applied to only one AP group.
- After an SFN group is applied to an AP group, automatic channel and power adjustment of Radio Resource Management (RRM) is invalid for radios of APs in that group.
- Remote Intelligent Perception Technology (RIPT) and SFN cannot be enabled on an AP simultaneously.

Configuration Step

↘ Creating an SFN Group

- Mandatory.
- After an SFN group is successfully created, the system enters the SFN group configuration mode. Then you can continue to configure other information about the SFN group.

Command	**sfn-group** *group-id* **{ AP720-I | AP730-I | AP850-A | APD4930-AX }**
Parameter	*group-id*: Specifies the ID of an SFN group. The value range is from 1 to 64.
Description	**AP720-I** | **AP730-I** | **AP850-A** | **APD4930-AX**: Specifies the model of the AP associated with the SFN group.
Defaults	No SFN group is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Associating the SFN Group with an AP Group

- Mandatory.

Command	**ap-group** *group-name*
Parameter Description	*group-name*: Specifies the name of an AP group to be associated with an SFN group.
Defaults	No AP group is associated with an SFN group by default.
Command Mode	SFN group configuration mode
Usage Guide	• An SFN group can be associated with only one AP group. • After an SFN group is associated with an AP group, all APs in the AP group join the SFN group.

Enabling SFN for the Specified Radio

- Mandatory.
- After creating an SFN group and applying it to the specified AP group, enable SFN for the specified radio and bind the SFN group to the specified WLAN. This SFN group will not take effect until you complete these configurations.

Command	**enable-sfn radio** *radio-id* **ap-wlan-id** *wlan-id*
Parameter Description	*radio-id*: Specifies the radio ID. The value is 1, 2, or 3. *wlan-id*: Specifies the ID of a WLAN. *ap-wlan-id* must be configured in the **interface-mapping** command in AP group configuration mode.
Defaults	SFN is not enabled for any radio by default.
Command Mode	SFN group configuration mode
Usage Guide	N/A

Verification

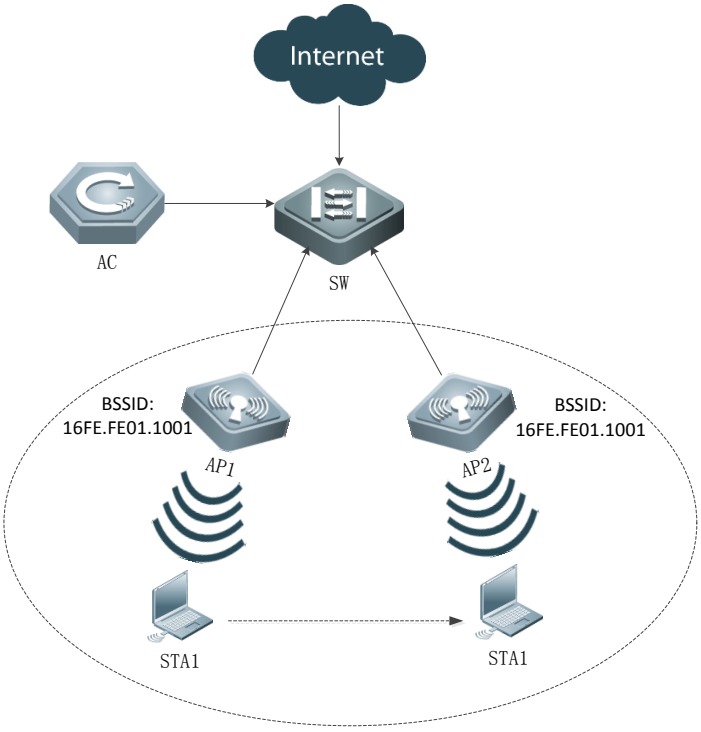
- Run the **show running-config** command to display the configuration.
- Run the **show sfn-group summary** command to display the SFN group list.
- Run the **show sfn-group summary** *group-id* command to display basic information about the SFN group and APs associated with the SFN group.
- Use wireless signal scanning software to scan two or more APs transmitting the same SSID, and check whether their corresponding BSSIDs are similar. For example, if two APs are associated with an SFN group, check whether they broadcast the same SSID with similar BSSIDs (for example, 16:fe:fe:02:10:02 and 16:fe:fe:01:10:01).

Configuration Example

Creating an SFN Group and Associating It with the Specified AP Group

Scenario	Normal fit AP environment

Figure 1-2



Assuming that AP1 and AP2 have joined the AP group **apg-1** in the fit AP environment, there are the following configuration requirements for SFN networking on the AC:

1. Create an SFN group.
2. Enable SFN for the AP group **apg-1**.
3. Enable SFN for radio 2 and bind it to WLAN 1.

-

Configuration Steps Create an SFN group and apply it to the specified AP group. Enable SFN for the specified radio.

AC

1. Create an SFN group.

```
Hostname# configure terminal
Hostname(config)# sfn-group 11 AP720-I
```

2. Apply the SFN group to the specified AP group.

```
Hostname(config)# sfn-group 11 AP720-I
Hostname(config-sfn-group)# ap-group apg-1
```

3. Enable SFN for radio 2.

```
Hostname(config)# sfn-group 11 AP720-I
Hostname(config-sfn-group)# enable-sfn radio 2
```

Verification After the SFN group is associated with the specified AP group, check whether the corresponding BSSIDs are similar when two or more than two APs send out the same SSID.

AC Run the **show sfn-group summary** command to display the SFN group list.

```
Hostname#show sfn-group summary

SFN Group  AP Model   AP Group Name                                    Radio  AP Wlan
Id

---------- ---------- ------------------------------------------------
------ ----------

11         AP720-I    apg-1                                            2      1


Total SFN Group Num: 1
```

1.4.2 Configuring SFN Group Information

Configuration Effect

- Support for multiple standards: Support 802.11a/g/ac/ax, enabling good network compatibility and scalability.
- Adjustable MCS range: Promote higher data transfer speed and lower bit error rate (BER), optimizing network efficiency.
- Receiving or transmitting antenna type optimization and DTIM period adjustment: Enhance signal coverage and device power-saving capabilities.
- Channel and channel width utilization: Optimize network throughput and reduce interference by properly configuring channels and channel width.
- RSSI threshold for STA handover: Adjust the RSSI threshold for STA handover, improving the handover experience when signal strength changes, reducing disconnection and latency.
- Operating frequency band selection: Flexibly select operating frequency bands to enhance network flexibility and adaptability, reducing congestion.
- Optimization of the OUI field for the BSSID of a virtual port: Configuring the OUI field improves virtual port identification and management, making network management more efficient.
- AP control mode intra-frequency handover: Implement AP control mode handover to optimize network resource utilization, reduce interference between APs, and improve overall performance and stability.

Notes

- The RF attribute configuration takes effect for the specified radios of all APs associated with the specified SFN group. You need to evaluate the impact before configuration.
- You do not need to perform optional configurations excluding the channel and channel width.

Configuration Step

Enabling the Specified Radio to Support 802.11a

- Optional.

Command	**11nasupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	802.11a is supported by default.
Command Mode	SFN group configuration mode
Usage Guide	The configuration is valid for the specified radio of an AP in the AP group on 5 GHz.

Enabling the Specified Radio to Support 802.11g

- Optional.

Command	**11ngsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	802.11g is supported by default.
Command Mode	SFN group configuration mode
Usage Guide	The configuration is valid for the specified radio of an AP in the AP group on 2.4 GHz.

Enabling the Specified Radio to Support 802.11ac

- Optional.

Command	**11acsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	802.11ac is supported by default.
Command Mode	SFN group configuration mode
Usage Guide	N/A

Enabling the Specified Radio to Support 802.11ax

- Optional.

Command	**11axsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	802.11ax is supported by devices of Wi-Fi 6 or higher capabilities by default.
Command Mode	SFN group configuration mode
Usage Guide	This command can be only configured on devices of Wi-Fi 6 or above.

Configuring the MCS Index of 802.11n

- Optional.

Command	**802.11n mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: Specifies the MCS index. The value range is from 0 to 15. *radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	The default MCS index of 802.11n is 15.
Command Mode	SFN group configuration mode
Usage Guide	The configuration is valid for the specified radio working in 802.11n mode of an AP in the AP group.

Configuring the MCS Index of 802.11ax

- Optional.

Command	**802.11ac mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: Specifies the MCS index. The value range is from 0 to 39. *radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	The default MCS index of 802.11ac is 19.
Command Mode	SFN group configuration mode
Usage Guide	The configuration is valid for the specified radio working in 802.11ac mode of an AP in the AP group.

Configuring the Receiving/Transmitting Antenna Type of the Specified Radio

- Optional.

Command	**antenna { transmit | receive }** *value* radio *radio-id*
Parameter Description	**transmit**: Configures the transmitting antenna type. **receive**: Configures the receiving antenna type. *value*: Specifies the antenna mask. The value range is from 1 to 7. *radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	The default antenna mask is 3.
Command Mode	SFN group configuration mode
Usage Guide	You must first check whether the APs joining the specified SFN group support the antenna direction to be configured. Otherwise, this command does not take effect.

Configuring the DTIM Period for the Specified Radio

- Optional.

Command	**beacon dtim-period** *period-num* **radio** *radio-id*
Parameter Description	*period-num*: Specifies the DTIM period, indicating the Beacon frame period. The value range is from 1 to 255. *radio-id*: Specifies the radio ID. The value is 1, 2, or 3.

Defaults	The default DTIM period is 1, that is, one Beacon frame period.
Command Mode	SFN group configuration mode
Usage Guide	N/A

Configuring a Channel for the Specified Radio

- Optional.

Command	**channel** *channel-id* **radio** *radio-id*
Parameter Description	*channel-id*: Specifies the ID of a channel. *radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	• RG-AP720-I: • The default channel ID for radio 1 is 1. • The default channel ID for radio 3 is 149. RG-AP730-I: • The default channel ID for radio 1 is 1. • The default channel ID for radio 2 is 36. • The default channel ID for radio 3 is 149. RG-AP850-A: • The default channel ID for radio 3 is 36. RG-APD4930-AX: • The default channel ID for radio 1 is 1. • The default channel ID for radio 2 is 149.
Command Mode	SFN group configuration mode
Usage Guide	• You must first confirm the frequency bands of the specified radios of all APs in the specified SFN group and the corresponding country codes before configuring the corresponding channels. Otherwise, this command does not take effect. • Channel switching will cause all STAs associated with the AP group to be disconnected. Exercise caution when you perform this operation.

Configuring the Channel Width for the Specified Radio

- Optional.

Command	**chan-width { 20 | 40 | 80 } radio** *radio-id*
Parameter Description	**20**: Configures the channel width as 20 MHz. **40**: Configures the channel width as 40 MHz. **80**: Configures the channel width as 80 MHz. *radio-id*: Specifies the radio ID. The value is 1, 2, or 3.
Defaults	The default channel width is 20 MHz on 2.4 GHz frequency band. The default channel width is 40 MHz on 5 GHz frequency band.
Command Mode	SFN group configuration mode

Usage Guide The channel width of 80 MHz is applicable to only radios on 5 GHz frequency band.

Configuring the RSSI Threshold for STA Handover

- Optional.
- The default threshold is 4 dB, meaning that the STA is only allowed to switch to another AP if the signal strength on the other AP is at least 4 dB stronger than the signal strength on the currently associated AP.

Command **handoff-rssi-thresh** *rssi*

Parameter Description *rssi*: Specifies the RSSI threshold for STA handover, in dB. The value range is from 1 to 100.

Defaults The default RSSI threshold is 4 dB.

Command Mode SFN group configuration mode

Usage Guide Configuring a low RSSI threshold for STA handover will cause the STA to switch between APs frequently, while configuring a high RSSI threshold may prevent the STA from switching to a better AP, leading to disconnection. You are advised to use the default value.

Configuring the Working Frequency Band for the Specified Radio

- Optional.

Command **radio-type { 802.11a | 802.11b } radio** *radio-id*

Parameter Description **802.11a**: Indicates the 5 GHz band.
802.11b: Indicates the 2.4 GHz band.
radio-id: Specifies the radio ID. The value is 1, 2, or 3.

Defaults The default value varies with modes of the AP.

Command Mode SFN group configuration mode

Usage Guide When an AP joins an SFN group, the radio type of the radio of the AP will switch to the radio type of the SFN group.
The configuration takes effect for the specified radios of all APs in the group.

Configuring the OUI Field for the BSSID of a Virtual Port

- Optional.

Command **sfn-vp-oui** *oui*

Parameter Description *oui*: Specifies the OUI field for the BSSID of a virtual port. The value is in the format of XX.XX.

Defaults By default, the 5th and 6th bytes of the AC's MAC address is used as the 2nd and 3rd bytes of the BSSID. Run the **show sysmac** command to display the MAC address of the AC.

Command Mode Global configuration mode

Usage Guide N/A

Enabling AP Control Mode Intra-frequency Handover

- Optional.

Command	**handoff-ap-mode enable**
Parameter Description	N/A
Defaults	AC control mode intra-frequency handover (except for the virtual AC) is enabled by default.
Command Mode	SFN group configuration mode
Usage Guide	Except for the virtual AC, the AC control mode is used by default. The virtual AC only supports the AP control mode. In a hierarchical AC environment, if the central AC is a virtual AC, the branch AC must be configured in AP control mode. Conversely, if the branch AC is a virtual AC, the central AC must also be configured in AP control mode.

Verification

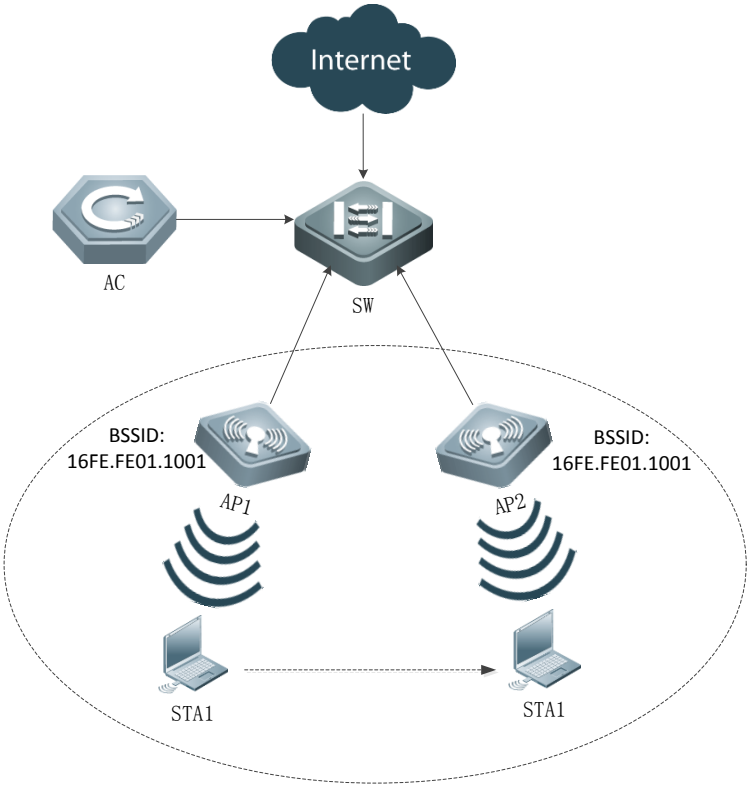
- Run the **show running-config** command to display the configuration.
- Run the **show ap-config running** command to display the AP configuration.
- Run the **show sfn-group summary** *group-id* command to display basic information about the SFN group and APs associated with the SFN group.
- Use packet obtaining on the air interface to display Beacon frame information.

Configuration Example

Creating an SFN Group and Configuring Parameters

Scenario Normal fit AP environment

Figure 1-3



Assume that there are the following parameter configuration requirements for the SFN group on the AC in the fit AP environment:

1. Configure APs in the group to use radio 2 for SFN networking.
2. Configure the RSSI threshold for STA handover as 12 for APs in the group.
3. Configure radio 2 of APs in the group to support 802.11a.
4. Configure radio 2 of APs in the group to support 802.11ac.
5. Configure the MCS index of 802.11n as 13 for radio 2 of APs in the group.
6. Configure the MCS index of 802.11ac as 7 for radio 2 of APs in the group.
7. Configure the receiving/transmitting antenna mask as 1 for radio 2 of APs in the group.
8. Configure the channel ID as 40 for radio 2 of APs in the group.
9. Configure the channel width as 40 MHz for radio 2 of APs in the group.
10. Configure the DTIM period as 2 for radio 2 of APs in the group.
11. Enable AP control mode intra-frequency handover.

Note: For application scenarios where the operating frequency band of radios of APs in an AP group needs to be switched, you can run the **radio-type** command in SFN group configuration mode.

Configuration Steps

- Configure an SFN group.

AC

```
Hostname(config)#sfn-group 1 AP720-I
Hostname(config-sfn-group)#ap-group sfn-xxx
Hostname(config-sfn-group)#enable-sfn-radio 2
```

```
Hostname(config-sfn-group)#handoff-rssi-thresh 12
Hostname(config-sfn-group)#11nasupport enable radio 2
Hostname(config-sfn-group)#11acsupport enable radio 2
Hostname(config-sfn-group)#802.11n mcs support 13 radio 2
Hostname(config-sfn-group)#802.11ac mcs support 7 radio 2
Hostname(config-sfn-group)#antenna transmit 1 radio 2
Hostname(config-sfn-group)#antenna receive 1 radio 2
Hostname(config-sfn-group)#channel 40 radio 2
Hostname(config-sfn-group)#chan-width 40 radio 2
Hostname(config-sfn-group)#beacon dtim-period 2 radio 2
Hostname(config-sfn-group)#handoff-ap-mode enable
```

Verification

AC

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

```
Hostname(config)#show running-config
!
sfn-group 1 AP720-I
 channel 40 radio 2
 802.11n mcs support 13 radio 2
 802.11ac mcs support 7 radio 2
 beacon dtim-period 2 radio 2
 chan-width 40 radio 2
 antenna transmit 1 radio 2
 antenna receive 1 radio 2
 handoff-rssi-thresh 12
 ap-group sfn-xxx
 enable-sfn-radio 2
 handoff-ap-mode enable
!
```

- Run the **show ap-config running** *ap-name* command to check whether the configuration is valid for specified APs in the SFN group.

AC

```
Hostname(config)#show ap-config running AP1
!
```

```
ap-config AP1
 ap-group sfn-xxx
 antenna receive 1 radio 2
 antenna transmit 1 radio 2
 802.11n mcs support 13 radio 2
 802.11ac mcs support 7 radio 2
 beacon dtim-period 2 radio 2
 channel 40 radio 2
 chan-width 40 radio 2
!
```

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show sfn-group summary	Displays the SFN group list.
show sfn-group summary *group-id*	Displays basic information about the SFN group and APs associated with the SFN group.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

N/A

Configuring RF Management

1. Configuring WBS
2. Configuring Band Selection
3. Configuring HE Radio Selection
4. Configuring RF Resource Scheduling
5. Configuring RRM
6. Configuring 802.11kv
7. Configuring CorrectLink
8. Configuring Frequency Spectrum Scanning
9. Configuring Wireless Location
10. Configuring Smart Antenna

1 Configuring WBS

1.1 Overview

The Wireless Basic Service (WBS) is used to configure wireless-specific parameters on access controllers (ACs) when Fit access points (APs) are deployed.

Link integrity detection is a basic service of the WBS. It detects wired uplinks on APs. When a link of an AP is disconnected, access services of the AP are stopped to disconnect the connected stations (STAs). When the link is restored, the AP continues to provide wireless access services. Enabling link integrity detection in a Fit AP architecture with dense AP deployment helps reduce the network disconnection time and improve user experience.

Protocols and Standards

- 802.11n: Enhancements for Higher Throughput
- 802.11ac: Enhancements for Very High Throughput for Operation in Bands below 6 GHz
- 802.11ax: Enhancements for High Efficiency WLAN

1.2 Applications

Application	Description
Configuring Fit APs	Run commands on an AC to configure parameters of Fit APs.
Enabling Link Integrity Detection	Enable link integrity detection in a Fit AP architecture to improve the quality of service (QoS) of wireless access.

1.2.1 Configuring Fit APs

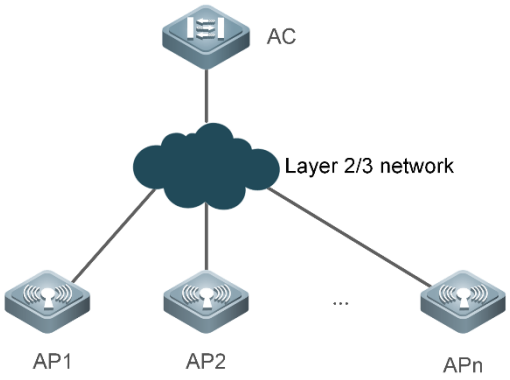
Scenario

Configure Fit APs. A network administrator can manage the configuration of Fit APs on an AC in a centralized manner. Assume that a network has the following deployment requirements:

1. Allow the AC to monitor the status of feeder links on i-Share APs.
2. Prevent STAs with received signal strength indication (RSSI) smaller than 20 dB from accessing the network.
3. Enable short guard interval (GI) in 20 MHz.
4. Prevent the use of low data rates, such as 1 Mbps, 2 Mbps, and 5.5 Mbps.

Figure 1-1 shows the Fit AP networking topology.

Figure 1-1 Fit AP Networking Topology



Deployment

Main configuration points on the AC:

1. Enable i-Share antenna feeder link detection for all the APs and set the detection interval.
2. Run **response-rssi** for radios of all the APs and set the threshold to 20 dB.
3. Run **short-gi enable** for radios of all the APs and set the bandwidth to 20 MHz.
4. Disable the use of 1 Mbps, 2 Mbps, and 5.5 Mbps data rates for 802.11b/g network users.

1.2.2 Enabling Link Integrity Detection

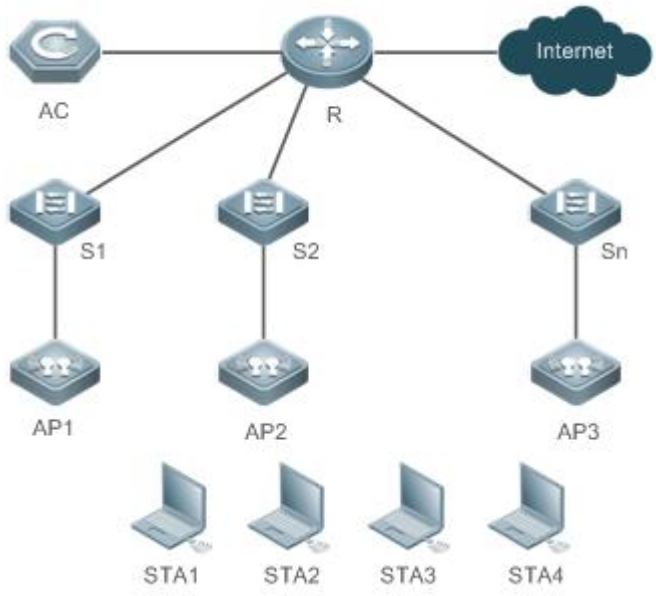
Scenario

Enable link integrity detection on wireless networks with the Fit AP architecture.

See Figure 1-2.

- An AC is connected to the Internet through a router. AP1, AP2, and AP3 are connected to the router through three switches and associated with the AC.
- STA1 is associated with AP1, STA2 and STA3 are associated with AP2, and STA4 is associated with AP3. The STAs access the Internet through the AC.

Figure 1-2



Remarks	The R is an egress router. S1, S2, and S3 are Layer 2 switches and function as access devices for APs. AP1, AP2, and AP3 are directly connected to S1, S2, and S3 respectively.

Deployment

- Layer 2 switches provide the access service for APs.
- The R sets up connections between ACs and APs and between STAs and the Internet.

1.3 Features

Basic Concepts

A-MPDU

The 802.11n standards utilize the aggregate MAC protocol data unit (A-MPDU). Multiple MPDUs are aggregated into an A-MPDU, retaining only one PHY header while removing those of other MPDUs. This approach reduces the additional information carried by the PHY header of each transmitted MPDU, resulting in a decrease in the number of ACK frames. As a result, it alleviates the burden and enhances network throughput.

A-MSDU

The 802.11n protocol introduces a new MAC feature known as the aggregate MAC service data unit (A-MSDU), which aggregates multiple MSDUs into one MSDU for transmission. Similar to A-MPDU, A-MSDU reduces additional information carried by the MAC header of each MSDU to be transmitted, thereby improving the transmission efficiency of the MAC layer.

MCS

The physical layer of 802.11n supports high data transmission rates and is compatible with 802.11a/b/g rates. The supported rates are called modulation and coding scheme (MCS) rates.

Beacon

APs on a wireless local area network (WLAN) periodically send beacon frames externally. The beacon frames contain AP information, and STAs receive beacon frames to discover WLANs.

RSSI

The RSSI indicates the quality of wireless connections.

Country or Region Code

A country or region code identifies a country or region with radio frequency (RF) usage. RFs, channels, and powers vary with country or region codes. Before you configure an AP, determine the country or region code supported by the AP. If the configured country or region code is changed, the RFs, channels, and powers mapped to the country or region code are also changed.

Frequency Band

The 2.4 GHz, 5 GHz, and 6 GHz frequency bands are supported.

Wireless Channel

Wireless channels transmit RF medium between APs and STAs. The use of channels varies with countries or regions and frequency bands.

The 2.4 GHz frequency band can be configured with 13 channels (channel 1 to channel 13). The overlapping channels in the 2.4 GHz frequency band cause interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision.

The 5 GHz frequency band can be configured with 25 channels (channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, and 165).

The 6 GHz frequency band can be configured with 15 channels (channels 5, 21, 25, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213, and 229).

Transmit Power

The transmit power indicates the strength of RF signals transmitted by an AP. It is proportional to the radio signal coverage area of the AP.

Timeslot Type

Channel contention may occur when multiple STAs send data on the same WLAN. To mitigate this issue, STAs are required to first check the idle state of channels before sending data. If a STA detects that a channel is idle, the STA does not send data until the backoff time has elapsed. The backoff time is a random integer, measured in slot times, which serves as a timing mechanism specified in the MAC protocol. After each slot time interval, the value of the backoff time is automatically decremented by 1. Once the backoff time reaches 0, the STA can begin transmitting data. On WLANs, the slot time is categorized into two intervals: 20 μs and 9 μs, with the latter referred to as the "short slot time."

Antenna Transmit or Receive Types

You can configure some antennas on an RF card to transmit signals and the other antennas to receive signals.

Short GI

802.11n adds optional support for a 0.4 μs guard interval, compared to the standard 0.8 μs guard interval.

Fragmentation Threshold

To increase the transmission success rate, the IEEE 802.11 MAC protocol supports fragmentation of packets before transmission. This process entails packet fragmentation based on a threshold, thereby reducing the interference probability and saving bandwidth resources during retransmission.

RTS/CTS

To avoid channel conflicts and resulting data transmission failures, the IEEE 802.11 MAC protocol provides a handshake protocol called Request To Send (RTS) or Clear To Send (CTS). When STA A needs to send data to STA B, it first sends an RTS frame. STA B responds with a CTS frame if it permits STA A to send data. After receiving the CTS frame, STA A starts sending data. In cases where multiple STAs send RTS frames to the same STA, only those that receive CTS frames are permitted to send data. The STAs that do not receive CTS frames can attempt to resend RTS frames after a specific time because a channel conflict is considered to have occurred.

PHY Protection Modes

Frames can be transmitted in Greenfield mode or hybrid mode. The hybrid mode is intended to support compatibility with other physical layers, and the Greenfield mode is used to transmit physical layer headers at high speeds. A device which uses the high-throughput (HT) hybrid mode can transmit frames in 802.11a/b/g and 802.11n modes. Such a device first transmits a conventional format preamble, followed by an HT format preamble. The device must send a conventional CTS-to-Self or RTS/CTS frame before transmitting data. These protection mechanisms enable 802.11a/b/g devices, including those devices not connected to APs in HT hybrid mode to detect the busy state of channels.

Preamble Type

A preamble is a group of bits in a packet header and used to synchronize transmission signals between the transmit end and receive end. You can configure the preamble type (long or short) that an AP supports. The data frames with long preambles take a longer time to be transmitted than the data frames with a short preamble.

U-APSD

802.11e introduces Wi-Fi multimedia power save (WMM-PS) to reduce the delay of services with high real-time performance requirements during power management. WMM-PS adopts the Unscheduled Automatic Power Save Delivery (U-APSD) technology to disable transmission of radio signals during most of the time, which extends the battery life. U-APSD is an enhancement of the 802.11 power saving mechanism.

Transmit Beamforming

Transmit Beamforming (TxBF) can be optionally supported in the 802.11n protocol to improve reliability of packet transmission. The transmitter adjusts the transmission mode of WLAN signals based on the evaluated channel conditions at the receiving antenna, so that the signal is the strongest when it arrives at the receiver, thereby improving the success rate and throughput of the wireless link.

MU-MIMO

802.11ac uses downlink Multi-User Multiple-Input Multiple-Output (MU-MIMO) to enable an AP to send data to multiple STAs through TxBF. 802.11ax uses uplink MU-MIMO to enable multiple STAs to send data to an AP.

OFDMA

Orthogonal Frequency Division Multiple Access (OFDMA) is extended based on OFDM. Multiple access is achieved in OFDMA by assigning subsets of subcarriers to individual users.

DFS

Dynamic Frequency Selection (DFS) allows wireless devices to dynamically switch their channels to prevent interference with key services such as radar systems. When a wireless device detects radar signals on the current channel, DFS triggers an automatic switch to other available channels, reducing or eliminating potential interference and protecting key radar services.

Overview

Feature	Description
Detecting Feeder Link	Checks the status of feeder links on i-Share APs.
In i-Share antenna scenarios, when rooms are limited, some APs do not need to be configured with feeders directed to rooms. However, the system may mistakenly assume that the feeder is not in position and therefore report an exception in the feeder status. To facilitate management, administrators are allowed to configure the feeder status manually. Configuring STA Access Control	Controls access of specified STAs.
Configuring RF Parameters	Configures RF parameters for APs or radios.
Configuring RF Parameters	Configures RF parameters of data rate control.
Configuring Power Saving Parameters	Sets power saving parameters.
Enabling Link Integrity Detection	Detects integrity of links to improve the wireless service quality.
Configuring E-Bag Parameters	Provides a command to quickly configure E-bag network optimization in one-click mode, which improves user experience.
Configuring WLANs in One-Click Mode	Provides the one-click WLAN configuration to achieve fast configuration of unconfigured devices.
Canceling the Power Supply Limit	Cancels the power supply limit.
Managing RF with Insufficient Power Supply	Manages RF based on device capabilities when power supply is insufficient.

Feature	Description
Configuring Forced Power Supply for an AP	Forcibly configures the AP power supply mode as the specified mode.
Configuring the Frequency Band Mode	Configures the frequency band mode of a specified radio on AP.

1.3.1 Detecting Feeder Links of i-Share APs

Working Principle

There may be a large number of i-Share APs on a network, and each AP may have multiple feeders connected to it. To facilitate user management, the device provides feeder link detection, which can automatically detect whether each feeder on each i-Share AP is working properly. In this way, when any feeder on any i-Share AP is not working properly due to poor contact or human damage, the fault can be rapidly detected and eliminated.

In i-Share antenna scenarios, when rooms are limited, some APs do not need to be configured with feeders directed to rooms. However, the system may mistakenly assume that the feeder is not in position and therefore report an exception in the feeder status. To facilitate management, administrators are allowed to configure the feeder status manually.

1.3.2 Configuring STA Access Control

Working Principle

Ruijie Networks provides STA access control.

STAs search for APs through active and passive scan:

- Active scan: A STA sends a Probe Request frame to request access to an AP, which will respond with a Probe Response frame.
- Passive scan: APs broadcast beacon frames periodically. STAs listen to beacon frames and initiate connections to APs.

To control network coverage areas of APs and improve the transmission quality of radio signals, take the following measures to limit the access of STAs:

- Control the range for broadcasting beacon frames on APs to limit the access of long-distance STAs.
- Configure the minimum RSSI applied to STAs during the access process. The STAs which send request frames with RSSI smaller than the minimum value are denied access.
- Configure the minimum RSSI applied to STAs during data transmission. The STAs which send data frames with RSSI smaller than the minimum value are disconnected. Then the STAs can roam to other APs with better radio signals.

1.3.3 Configuring RF Parameters for APs

You can configure RF parameters for APs and radios.

Working Principle

A-MPDU

The 802.11n standards utilize A-MPDU. Multiple MPDUs are aggregated into an A-MPDU, retaining only one PHY header while removing those of other MPDUs. This approach reduces the additional information carried by the PHY header of

each transmitted MPDU, resulting in a decrease in the number of ACK frames. As a result, it alleviates the burden and enhances network throughput.

A-MPDU Aggregation Depth

It refers to the maximum number of MPDUs that can be aggregated in an A-MPDU.

AMSDU

The 802.11n protocol defines a new MAC feature called A-MSDU, which combines multiple MSDUs into one MSDU for transmission. Similar to A-MPDU, A-MSDU reduces the additional information on the MAC header of each MSDU to be transmitted, improving the transmission efficiency of the MAC layer.

A-MSDU Aggregation Depth

It refers to the maximum number of MSDUs that can be aggregated in an A-MSDU.

MCS

In 802.11n, RF rates are configured by using index values of the MCS, which is used to represent the communication rates on WLANs. The MCS is a rate table. The table columns list the factors that affect communication rates, and the table rows show the MCS indexes. Each MCS index maps a physical transmission rate which is determined by a group of parameters. For details of all the MCS rate tables, see the *IEEE P802.11n D2.00*.

Wireless Channel

Wireless channels transmit RF medium between APs and wireless STAs. The use of channels varies with different countries/regions and frequency bands.

The 2.4 GHz radio can be configured with 13 channels (channel 1 to channel 13). The overlapping channels in the 2.4 GHz radio cause interference. It is recommended that these channels be configured as non-overlapping channels (for example, channels 1, 6, and 11) to avoid radio signal collision.

The 5 GHz radio can be configured with 25 channels (channels 36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 149, 153, 157, 161, and 165).

The 6 GHz radio can be configured with 15 channels (channels 5, 21, 25, 37, 53, 69, 85, 101, 117, 133, 149, 165, 181, 197, 213, and 229).

Packet Fragmentation

To increase the transmission success rate, the IEEE 802.11 MAC protocol supports fragmentation of packets before transmission. This process entails packet fragmentation based on a threshold, thereby reducing the interference probability and saves bandwidth resources during retransmission.

RTS/CTS

To avoid channel conflicts and resulting data transmission failures, the IEEE 802.11 MAC protocol provides a handshake protocol called RTS or CTS. When STA A needs to send data to STA B, it first sends an RTS frame. STA B responds with a CTS frame if it permits STA A to send data. After receiving the CTS frame, STA A starts sending data. In cases where STAs send RTS frames to the same STA, only those that receive CTS frames are permitted to send data. The STAs that do not receive CTS frames can attempt to resend RTS frames after a specific time because a channel conflict is considered to have occurred.

If each STA implements RTS/CTS handshake before sending data, many RTS frames will occupy channel bandwidth. To avoid this problem, you can configure an RTS threshold to specify the frame length of transmitted data. If a STA sends data with a frame length smaller than the RTS threshold, the STA will not implement RTS/CTS handshake.

Beacon

APs on a WLAN periodically send beacon frames externally. The beacon frames contain AP information, and STAs receive beacon frames to discover WLANs.

Preamble Type

A preamble is a group of bits in a packet header and used to synchronize transmission signals between the transmit end and receive end. You can configure the preamble type (long or short) that an AP supports. The data frames with long preambles take a longer time to be transmitted than the data frames with a short preamble.

Timeslot Type

Channel contention may occur when multiple STAs send data on the same WLAN. To mitigate this issue, STAs are required to check the idle state of channels before sending data. If a STA detects that a channel is idle, the STA does not send data until the backoff time has elapsed. The backoff time is a random integer, measured in slot times, which serves as a timing mechanism specified in the MAC protocol. Assume that the random integer is 3. After each slot time interval, the value of the backoff time is automatically decremented by 1. Once the backoff time reaches 0, the STA can begin transmitting data. Reducing the slot time can reduce the overall backoff time and increase network throughput.

Channel Bandwidth

In 802.11n and later protocols, channel bonding can be used to expand the communication bandwidth, increase the rate, and improve the throughput of wireless networks. 802.11n supports a maximum bandwidth of 40 MHz, while 802.11ac and 802.11ax support a maximum bandwidth of 160 MHz.

GI

802.11n adds optional support for a 0.4 μs guard interval, compared to the standard 0.8 μs guard interval.

802.11ax supports three types of guard interval: 0.8 μs, 1.6 μs, and 3.2 μs.

Country or Region Code

A country or region code identifies a country or /region with RF usage. RFs, channels, and powers vary with country or region codes. Before you configure an AP, determine the country or region code supported by the AP. If the configured country or region code is changed, the RFs, channels, and powers mapped to the country or region code are also changed.

Antenna Transmit/Receive Types

An AP can use different number of antennas when transmitting and receiving data. This enables the AP to adopt the multi-stream transmission mode to improve data transmission performance. 802.11n supports up to four spatial streams, while 802.11ac and 802.11ax support up to eight spatial streams.

Internal and External Antennas

Internal antennas are integrated inside the enclosures of APs, and external antennas are connected to reserved hardware interfaces of APs. External antennas achieve longer transmission distances than internal antennas with the same transmission power.

Omnidirectional and Directional Antennas

An omnidirectional antenna radiates signals equally in all directions, while a directional antenna radiates signals in a specific direction with a cone-shaped radiation range.

Maximum Distance of Radio Transmission Between AP Radios and the Peer End

Radio signals travel through space at the speed of light. As the distance of radio transmission between AP radios and the peer end increases, the duration for transmitting radio packets in space also increases, subsequently extending the timeout interval for APs to await ACK and CTS frames. It is crucial to adjust the timeout interval according to the distance of radio transmission between AP radios and the peer end; otherwise, radio data may fail to be transmitted. A long timeout interval leads to a wastage of resources on the air interface as APs continue to wait for ACK and CTS frames.

One-Click Configuration of AP's RF Parameters Including the Power, Channel, and Antenna Transmit/Receive Type

The power, channel, and antenna transmit/receive type vary with AP models. One-click configuration of AP's RF parameters can be used to automatically adjust the parameters based on radio types, achieving optimal network performance.

Exchanging Channels

In high-density scenarios, enabling the third radio is enabled for user access results in varying degrees of channel limitation across each RF interface. Directly changing the channel for an RF interface is not allowed, but it is possible to change working channels between two RF interfaces of the same type.

MCell

The MCell function effectively reduces receiving sensitivity and enhances air interface concurrency in high-density scenarios by disabling Low Noise Amplifier (LNA).

Transmit Beamforming

Transmit Beamforming (TxBF) is a technology supported as an option in the 802.11n protocol to improve the reliability of packet transmission. The transmitter adjusts the transmission mode of WLAN signals based on an assessment of the channel conditions between the transmitter and the receiver to target the receiving antenna. This ensures that the signals arrive at their strongest at the receiver, thereby increasing the success rate of wireless link transmissions and improving overall throughput.

Multi-BSSID

Mutli-BSSID (MBSSID) is an optional feature defined in the 802.11v protocol. It allows multiple virtual access points (VAPs) operating on the same radio to share one beacon, reducing the number of beacons and improving the data utilization of air interfaces, thereby improving the performance and throughput of wireless links.

RNR

Reduce Neighbor Report (RNR) enables STAs to learn about the available 6 GHz radio from the RNR information in beacon frames sent by the AP's 2.4 GHz and 5 GHz radios.

FILS

FILS Announcement is an improved passive scanning mechanism added to the 6 GHz radio. FILS Announcement packets are sent at an interval of 20 ms, reducing the waiting time of passive scanning.

UPRS

Unsolicited Probe Response (UPR) is a new passive scanning improvement mechanism in the 6 GHz radio. If UPR is implemented, the 6 GHz AP sends UPR frames at an interval of 20 ms to reduce the waiting time for passive scanning.

BSS Color

BSS Color is used to address the issue of Overlapping Basic Service Set (OBSS) in order to improve spatial reuse and reduce MAC layer competition caused by OBSS. 802.11ax-compliant devices distinguish BSSs by adding a BSS Color field to the physical header. If the BSS Color field in the physical header of different packets is the same, it indicates that the packets are within the same BSS (intra-BSS); otherwise, they are in different BSSs (inter-BSS). By increasing the signal detection threshold between BSSs (inter-BSS) while maintaining a low signal detection threshold within the same BSS (intra-BSS), and adjusting transmit power, the overall throughput and spatial reuse of the current channel can be improved.

TWT

Target Wakeup Time (TWT) is an 802.11ax scheduling algorithm. TWT requesters and TWT responders agree upon a time window called the Service Period (SP) through negotiation, during which the TWT requesters wake up for packet transmission while remaining in sleep mode outside the SP. This aims to achieve power savings for the STA and minimize the BSS activity management at the AP, reducing STA competition.

QBSS Load

The QoS Basic Set Service (QBSS) load enables an AP to inform STAs about the AP's load. When this function is enabled, beacon or probe response packets sent by the device contain the BSS load Information Element (IE) field. The BSS load IE contains information on the STA count, channel utilization, and other information in the BSS at a specific radio. STAs automatically select the optimal network for login according to the information.

BAR Retransmission Count

Block ACK Request (BAR) aggregates multiple acknowledgment frames into a single acknowledgment frame, thus improving channel transmission efficiency. Configuring the BAR retransmission count prevents BAR frame loss. A larger retransmission count indicates a lower probability of losing BAR frames. However, excessive retransmission may increase the load of an air interface.

1.3.4 Configuring RF Parameters for Rate Control

Set RF parameters for rate control.

Working Principle

802.11 is an industrial standard defined by IEEE for WLAN communication, and has been continuously supplemented and improved to form the 802.11x standard series. The main transmission standards are 802.11b/a/g/n/ac/ax/be, which are described as follows:

1. 802.11b

It operates in the 2.4 GHz frequency band, with a maximum data transmission rate of up to 11 Mbps, which can be lowered to 5.5 Mbps, 2 Mbps, or 1 Mbps as needed.

2. 802.11a

It operates in the 5 GHz frequency band, with a maximum data transmission rate of up to 54 Mbps, which can be lowered to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, or 6 Mbps according to actual needs.

3. 802.11g

It operates in the 2.4 GHz frequency band, with a maximum data transmission rate of up to 54 Mbps, which can be lowered to 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, or 6 Mbps as needed. Devices that support 802.11g are backward compatible with 802.11b.

4. 802.11n

It operates in the 2.4 GHz and 5 GHz operating bands, with a maximum data transmission rate of 600 Mbps. 802.11n-compliant device are backward compatible with 802.11a/b/g.

5. 802.11ac

It operates in the 5 GHz frequency band, with a maximum data rate of 6.9 Gbps. 802.11ac-compliant devices are backward compatible with 802.11a/b/g/n.

6. 802.11ax

It operates in the 2.4 GHz, 5 GHz, and 6 GHz frequency bands, with a maximum data transmission rate of 9.6 Gbps. 802.11ax-compliant devices are backward compatible with 802.11a/b/g/n/ac in the 2.4 GHz and 5 GHz frequency bands, but not in the 6 GHz frequency band.

7. 802.11be

It operates in the 2.4 GHz, 5 GHz, and 6 GHz frequency bands, with a maximum data transmission rate of 46 Gbps. 802.11be-compliant devices are backward compatible with 802.11a/b/g/n/ac/ax in the 2.4 GHz and 5 GHz frequency bands, but not in the 6 GHz frequency band.

1.3.5 Configuring Power Saving Parameters

Working Principle

↘ DTIM Period

A delivery traffic indication map (DTIM) is a flag bit in a beacon frame, and is used to determine the interval at which an AP sends broadcast or multicast frames. APs buffer the data that STAs in sleeping state need to receive according to the DTIM period. After the DTIM period has elapsed, APs send the buffered data to STAs.

The DTIM period is expressed based on the number of sent beacon frames. Assume that the DTIM period is set to 3. APs send broadcast or multicast frames each time after three beacon frames are sent.

↘ U-APSD Power Saving

U-APSD is enhanced based on the power saving mode. When clients are associated with ACs, some ACs can be configured with the trigger attribute, some ACs can be configured with the delivery attribute, and the maximum number of packets to be sent after trigger can be set. The trigger and delivery attributes can be changed when flows are created through connection access control (CAC). When a client sleeps, data packets from the AC with the delivery attribute destined for the client are buffered. To retrieve the buffered packets, the client needs to send data packets from the AC

with the trigger attribute. After receiving such packets, the AP sends the buffered packets according to the number of packets to be sent during the access process. Other data packets from the AC without the delivery attribute are stored and transmitted in accordance with 802.11 standards.

1.3.6 Enabling Link Integrity Detection

APs implement functions of the physical layer and MAC layer, and typically do not provide switching functions. A Fat or Fit AP has only one wired uplink, which is the data channel allowing STAs to access the AP. When the wired uplink is disconnected because of a fault, all the STAs connected to the AP cannot access the Internet.

STAs cannot detect link disconnections immediately or take measures. As a result, the network connection cannot be restored for a long time.

Link integrity detection is introduced to solve this problem.

Working Principle

The link integrity detection function continuously detects the status of wired uplinks on APs. When a wired uplink is disconnected, the RF interface of the AP is disabled to stop the access service. STAs associated with the AP are disconnected and have to reconnect to other normal APs.

When the wired uplink is recovered, the link integrity detection function enables the RF interface of the AP to restore the wireless access service again.

When the wired uplink of an AP is disconnected, link integrity detection enables STAs that are associated with the AP to reconnect to other normal APs.

1.3.7 Configuring E-Bag Parameters

You can configure E-bag parameters for APs and radios.

Working Principle

You can run a command to quickly configure E-bag network optimization in one-click mode, which improves user experience.

↘ A-MPDU

A-MPDU is short for aggregate MAC protocol data unit.

↘ LDPC

A low-density parity-check (LDPC) code is a type of linear error correcting code. Known for its ease of use and low complexity, this coding method utilizes forward error correction (FEC) technology to enhance coding reliability and performance. LDPC was developed in the early 1960s and is designed to support information transmission in noisy frequency environments with significant background or content damage. Moreover, LDPC significantly reduces the probability of information loss during transmission in frequencies plagued by severe noise interference. However, note that a small number of STAs may be incompatible with LDPC, and enabling LDPC can lead to packet loss.

↘ STBC

Space time block coding (STBC) is a wireless communication technique that transmits multiple copies of a data stream over several antennas at different time points. This approach improves reliability of data transmission through a

combination of time and space diversity. The key benefit of STBC lies in its capability to leverage maximum likelihood decoding to achieve full antenna gains. Nonetheless, it is important to note that some STAs may be incompatible with STBC.

A-MPDU Software Retransmission Count

The A-MPDU software retransmission mechanism is specifically designed to prevent the loss of sub-frames in wireless communications. The probability of sub-frame loss decreases as the retransmission count increases. However, frequent packet retransmission can impose a higher burden on the air interface, thereby affecting real-time transmission of packets. If there is a high probability of sub-frame loss, increasing the retransmission count can be considered to mitigate packet loss.

A-MPDU-RTS

The RTS protection feature of A-MPDU is designed to prevent resource waste on the air interface caused by packet collision due to hidden nodes. Because RTS interaction consumes air interface resources and can have an adverse impact on several application scenarios, this feature is disabled by default. You are advised ot enable RTS protection only when the resource waste on the air interface caused by hidden nodes outweighs the resource consumption of RTS interaction on the air interface.

One-Time Received Ethernet Packet Quantity

A command is provided to adjust the number of Ethernet packets received at a time. Increasing the number of Ethernet packet received can improve network performance, but it may reduce APs' capability to handle key packets in real time. If high performance is not required but there is a need for real-time packet handling and user concurrency, it may be necessary to reduce the number of Ethernet packet received. In this case, it is recommended that the value be set to 25.

1.3.8 Configuring WLANs in One-Click Mode

The one-click WLAN configuration feature allows you to perform fast configuration on unconfigured devices.

Working Principle

One-Click Configuration

Perform the following configuration on an AC:

1. Assignment of virtual local area networks (VLANs): On the AC, configure VLAN 1 for APs and VLAN 2 for STAs.
2. Address pool: On the AC, configure the network segment 192.168.1.0 for APs and configure the network segment 192.168.2.0 for STAs. The default IP addresses of VLAN 1 and VLAN 2 are 192.168.1.1 and 192.168.2.1 respectively. The default management IP address is 88.88.88.88.
3. WLAN configuration: Name the WLAN **autowifi**_*XXXX*, where *XXXX* is the last four digits of the MAC address of the AC. You can use **wlan-id 1**.
4. Security: By default, WPA2 encryption is used. The password is **autowifi**.
5. WLAN-VLAN mapping: On the AC, configure the mapping between wlan-id 1 and VLAN 2 in the group named **ap-group default**.
6. Service: Enable the Dynamic Host Configuration Protocol (DHCP) service.

1.3.9 Canceling the Power Supply Limit

In situations where some APs with PoE+ power cannot negotiate PoE+ with certain special power supply devices, cancel the power supply limit to ensure that the APs can work at their full capacity.

Working Principle

When the negotiated power supply limit is 15.4 W, configure a command to cancel the power supply limit.

When using the command, ensure that the power supply device meets the maximum power consumption requirement of the corresponding AP. Otherwise, the AP may restart. Exercise caution when configuring this command.

1.3.10 Managing RF with Insufficient Power Supply

In situations where special power supply devices cannot negotiate PoE+ with some APs that have PoE+ power, the negotiated power supply limit may reduce to 15.4 W. This can result in insufficient power supply when all RFs are providing services. Therefore, depending on external power supply conditions, APs will disable certain types of RFs (2.4 GHz, 5 GHz, or 6 GHz) based on their device capability, to ensure sufficient power supply for the remaining RFs to function correctly. However, when the power supply is negotiated as PoE+, all RFs are enabled and can operate properly.

Working Principle

For some APs that are powered by PoE+ and have a negotiated power supply limit of 15.4 W during startup, the APs will disable specific RFs (2.4 GHz or 5 GHz) depending on their device capability. However, the AC can configure the AP to switch between RFs, namely, 2.4 GHz and 5 GHz.

1.3.11 Configuring Forced Power Supply for an AP

Forcibly configure the AP power supply mode as the specified mode.

Working Principle

Forcibly configure the power supply mode of an AP to af/at25w/36w/bt and save the configuration.

NOTE:

The **save** parameter can be specified in the command to indicate whether the forced power supply mode needs to be saved to the environment variables to avoid loss after restart.

1.3.12 Configuring the Frequency Band Mode

Some APs can switch the operating band of the radio by setting the frequency band mode.

Working Principle

Some APs allow the operating band of the radio (2.4 GHz, 5 GHz, or 6 GHz) to be set during startup, but not dynamically switched during operation.

↘ Freqnecy Band Mode

Configure the frequency band mode of a specified radio on an AP.

1.4 Configuration

Configuration	Description and Command	
Configuring Feeder Link Detection	(Optional) It is used to enable the feeder link status detection function on an AP.	
	antdetect enable	Enables the feeder link status detection function.
	antdetect interval	Configures the feeder status detection interval, in minutes.
	antdetect cfg *port_id state*	Configures of the feeder status.
Configuring STA Access Control	(Optional) It is used to configure STA access control.	
	{ **802.11a** | **802.11b** | **6GHz** } **network** { **enable** | **disable** }	Enables or disables the 2.4 GHz, 5 GHz, or 6 GHz network.
	11asupport enable	Enables 802.11a support for specified AP radios in 5 GHz.
	11bsupport enable	Enables 802.11b support for specified AP radios in 2.4 GHz.
	11gsupport enable	Enables 802.11g support for specified AP radios on the 2.4 GHz network.
	11nasupport enable	Enables 802.11n support for specified AP radios in 5 GHz.
	11ngsupport enable	Enables 802.11n support for specified AP radios in 2.4 GHz.
	11acsupport enable	Enables 802.11ac support for specified AP radios.
	11axsupport enable	Enables 802.11ax support for specified AP radios.
	11besupport enable	Enables 802.11be support for specified AP radios.
	802.11 mode max	Configures the highest access mode supported by a specified WLAN.
	coverage-area-control	Configures the management frame power for APs.
	extra-coverage	Configures the third radio for user access.
	response-rssi	Configures the minimum RSSI for wireless STAs to connect to specified AP radios.
	assoc-rssi	Configures the minimum RSSI for wireless STAs to maintain connections with specified AP radios.
Configuring AP's RF Parameters	(Optional) It is used to configure RF parameters for APs.	
	802.11n a-mpdu enable	Enables A-MPDU for specified AP radios.

Configuration	Description and Command	
	ampdu-depth	Configures the aggregation depth for specified AP radios.
	amsdu-depth	Configures the A-MSDU aggregation depth for specified AP radios.
	802.11n a-msdu enable	Configures A-MSDU support for specified AP radios.
	802.11n mcs support	Configures the maximum 802.11n MCS index value for specified AP radios.
	802.11ac mcs support	Configures the maximum 802.11ac MCS index value for specified AP radios.
	802.11ax mcs support	Configures the maximum 802.11ax MCS index value for specified AP radios.
	802.11be mcs support	Configures the maximum 802.11be MCS index value for specified AP radios.
	11ax-gi	Configures the guard interval for specified AP radios.
	antenna	Configures the antenna transmit/receive type for specified AP radios.
	antenna type	Configures an omnidirectional antenna or a directional antenna.
	antenna internal-direction enhance	Configures built-in directional antennas to work in enhanced mode.
	beacon period	Configures the interval for transmitting beacon frames for specified AP radios.
	chan-with	Configures bandwidth for specified AP radios.
	channel	Configures channels for specified AP radios.
	country	Configures the country or region code set supported by an AC or the country or region code used by AP radios.
	country-code	Configures the global country code supported by an AC.
	enable-radio	Enables specified or all AP radios.
	external-antenna enable	Enables usage of external antennas for specified AP radios, and disables usage of internal antennas.
	fragment-threshold	Configures the fragmentation threshold for specified AP radios.
	fragment-burst	Configures the fragment burst mechanism for specified AP radios.
	green-field enable	Enables the protection mode for specified AP radios.

Configuration	Description and Command	
	mcell	Configures the MCell function.
	cell-range-reduction	Reduces the receive sensitivity of a radio.
	anti-interference-level	Configures the anti-interference level of a radio.
	mu-mimo enablelong-gi	Configures MU-MIMO of a radio.
	ofdma	Enables OFDMA for the specified radio.
	peer-distance	Configures the maximum distance allowed between an AP and the peer end.
	power local	Configures the transmit power for specified AP radios (percentage).
	power local-dbm	Configures the transmit power for specified AP radios (dbm).
	preamble radio	Configures the operating preamble type for specified AP radios.
	radio-optimize	Configures radio parameters, including the power, channel, and antenna type.
	radio-type	Specifies the operating band for specified AP radios.
	rts-threshold	Configures the RTS threshold for specified AP radios.
	short-gi	Enables short GI for specified AP radios.
	short-slot-time	Configures the Short Slot Time (SST) function for specified AP radios.
	txbf enable	Configures the TxBF function of a radio.
	update-key-tsc enable	Enables TKIP Sequence Counter (TSC) update for APs during 802.11x re-authentication.
	multi-bssid enable	Sends the BSSID of the specified radio over one beacon.
	rnr enable	Configures the specified radio to probe 6 GHz radio signal through the 2.4 GHz or 5 GHz radio.
	ap-announcement-mode	Configures the announcement function for the specified AP radio to send Frequency Information Location Service (FILS) or Unsolicited Probe Response (UPRS) frames at an interval of 20 ms to reduce the waiting time of passive scanning.
	bss-color enable	Configures BSS color for the specified radio.
	twt enable	Configures TWT for the specified radio.
	qbss-load enable	Configures QBSS load for the specified AP radio.

Configuration	Description and Command	
	bar-retries	Configures the BAR retransmission count for the specified AP radio.
Configuring Data Rate Control Parameters	(Optional) It is used to configure parameters of data rate control.	
	{ **802.11a** | **6GHz** } **network rate**	Configures the data rate set supported by 802.11a (5 GHz) STAs or 6 GHz STAs.
	802.11b network rate	Configures the data rate set supported by 802.11b STAs.
	802.11g network rate	Configures the data rate set supported by 802.11g STAs.
	mcast-rate	Configures the WLAN multicast rate.
	beacon rate	Configures the beacon frame transmission rate.
Configuring Power Saving Parameters	(Optional) It is used to configure power saving parameters.	
	apsd	Enables or disables U-APSD power saving.
	beacon dtim-period	Configures the DTIM period.
Enabling Link Integrity Detection	(Mandatory) It is used to enable link integrity detection.	
	link-check enable	Enables link integrity detection.
Configuring E-Bag Parameters	(Optional) It is used to configure the parameters of E-bag.	
	ampdu-retries	Configures the A-MPDU retransmission count.
	ampdu-rts	Enables or disables RTS protection for A-MPDU packets.
	eth-schd	Configures the one-time received Ethernet packet quantity for APs.
	ldpc	Enables or disables LDPC.
	stbc	Enables or disables transmit or receive STBC.
	ebag	Configures E-bag network optimization in one-click mode.
Configuring WLANs in One-Click Mode	(Optional) It is used to configure WLANs in one-click mode.	
	autowifi	Configures WLANs in one-click mode.
Cancelling the Power Supply Limit	**poe-unlimit**	Cancels the power supply limit for specified AP radios.
Managing the Operating Frequency Band When Power Supply Is Insufficient	**hap-poe enable radio** { **802.11a** | **802.11b** }	Switches to 2.4 GHz or 5 GHz

Configuration	Description and Command	
Enabling or Disabling the PoE Power Supply by an AP to External Devices	**poeout**	Enables or disables the PoE function on an AP.
Configuring or Canceling Forced Power Supply Mode for an AP	**pdpoe-force** { **af** | **at25w** | **at36w** | **bt** } [**save**]	Forcibly configures the AP power supply mode.
Configuring a Frequency Band Mode	⚠ Optional.	
	ap-band-mode	Configures the frequency band mode.

1.4.1 Configuring Feeder Link Detection for i-Share APs

Configuration Effect

- Feeder link detection enables an i-Share AP to periodically detect the feeder link status. When the feeder link is abnormal, the i-Share AP can upload abnormal antenna information to the AC, so that network administrators can detect and troubleshoot the feeder link problem in a timely manner.

Notes

- This function is supported only on AP220-E(M) v3.0 and RG-APD4930.

Configuration Steps

↘ Enabling Feeder Link Detection

- Optional.
- On the AC, configure the AP that needs to be enabled with feeder link detection.
- After enabling this function, the AC will deliver this configuration to the corresponding AP, instructing the AP to enable the feeder link detection function. When the AP detects that the feeder link is abnormal, the AP uploads the link abnormal status to the AC, so that the network administrator can query the AP feeder link status.

Command	**antdetect enable**
Parameter Description	N/A
Defaults	The feeder link detection function is enabled by default.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The feeder link detection function is enabled by default.

↘ Configuring the Feeder Link Detection Interval

- Optional.
- On the AC, configure the AP that needs to be enabled with feeder link detection. The feeder link detection interval can be configured only when feeder link detection is enabled.

- The AC will deliver the parameter configuration to the corresponding AP, informing the AP of the feeder link detection interval, so that it can detect the feeder link status at the specified interval.

Command	**antdetect interval** *interval*
Parameter Description	*interval*: Indicates the detection interval, in minutes. The value range is from 1 to 10,000.
Defaults	The default value is 1 minute, indicating that the AP detects the link status every 1 minute.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The feeder link detection interval is set to 1 minute by default.

Configuring the Feeder Status

- Optional.
- On an AC, configure an AP enabled with the feeder link detection function. If the feeder link detection function is disabled, the configuration does not take effect.
- After configuration, the AC will record the status of the specified antenna of the AP as configured.

Command	**antdetect cfg** *port_id state*
Parameter Description	*port_id*: Indicates the AP port number, that is, antenna number. The value range is from 1 to 8. *state*: Indicates the antenna status. The value can be 1, 2, or 3. The value 1 indicates Y, that is, the feeder is in position. The value 2 indicates N, that is, the feeder is not in position. The value 3 indicates Idle, that is, the feeder is not connected. After configuration, you can view the antenna status on the web interface of the AC.
Defaults	If the feeder link detection function is enabled, the status of the feeder is automatically detected by default.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	1. The feeder link detection function must be enabled before you configure the feeder status. 2. This function is supported only on the RG-APD4930. Whether this command is supported varies depending on the product.

Verification

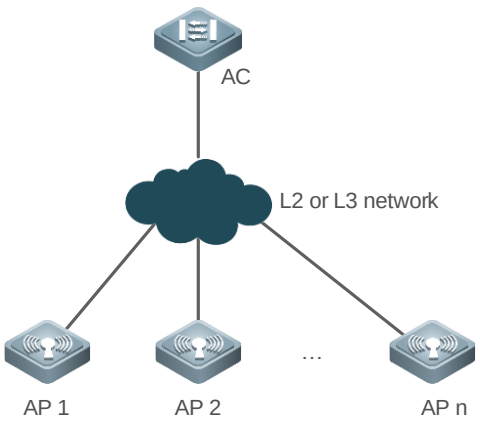
Run the **show antenna all** command to display the feeder link status of all APs.

Configuration Example

Configuring the Feeder Link Detection Function

Scenario

Figure 1-1



Assume that in a Fit AP environment. The following configurations are performed on the AC:

1. Enable feeder link detection of all APs.
2. Set the feeder link detection interval to 30 minutes.

Configuration Steps

Configure i-Share feeder link detection on the AC.

```
Hostname# configure terminal
Hostname(config)# ap-config all
Hostname(config-ap)# antdetect enable
Hostname(config-ap)# antdetect interval 30
```

Verification

Run the **show antenna all** command to display the feeder link status of all APs.

```
Hostname# show antenna all
ap's antenna state                                          R1       R2
R3       R4       R5       R6

                        ap                                0 1 2 3   0 1 2 3
0 1 2 3   0 1 2 3   0 1 2 3   0 1 2 3
-------------------------------------------------------------------   -------
-------   -------   -------   -------   -------

APD-M4                                                  - N N -   - N Y -
- N N -   - N N -   - - - -   - - - -
```

Common Errors

N/A

1.4.2 Configuring STA Access Control

Configuration Effect

- Control the access of a specified type of STAs so that a network administrator can easily manage the STAs.

Configuration Steps

Enabling or Disabling the 2.4 GHz, 5 GHz, or 6 GHz Network

- Optional.
- Enable or disable the 2.4 GHz, 5 GHz, or 6 GHz network on an AC.
- The AC delivers the configuration to all the APs to instruct the APs to enable or disable the 2.4 GHz, 5 GHz, or 6 GHz network.

Command	{ **802.11a** | **802.11b** | **6GHz** } **network** { **enable** | **disable** }
Parameter Description	N/A
Defaults	By default, the 2.4 GHz, 5 GHz, and 6 GHz networks are enabled.
Command Mode	AC configuration mode
Usage Guide	N/A

Enabling 802.11a Support

- Optional.
- The configuration takes effect only when the AP radios operate in 5 GHz.
- On the AC, enable 802.11a support for specified APs.
- The AC delivers the configuration to APs to instruct the APs to support the access of 802.11a STAs in 5 GHz.

Command	**11asupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with 802.11a support. The value range is from 1 to 96.
Defaults	By default, the access of 802.11a STAs is supported in 5 GHz.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 5 GHz. The configuration is supported only by specified APs.

Enabling 802.11b Support

- Optional.
- The configuration takes effect only when AP radios operate in 2.4 GHz.
- On the AC, enable 802.11b support for specified APs.
- The AC delivers the configuration to APs to instruct the APs to support the access of 802.11b STAs in 2.4 GHz.

Command	**11bsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with 802.11b support. The value range is from 1 to 96.
Defaults	By default, the access of 802.11b STAs is supported in 2.4 GHz.
Command Mode	AP configuration mode or all-AP configuration mode

Usage Guide	The configuration takes effect only when AP radios operate in 2.4 GHz. The configuration is supported only by specified APs.

Enabling 802.11g Support

- Optional.
- The configuration takes effect only when AP radios operate in 2.4 GHz.
- On the AC, enable 802.11g support for specified APs.
- The AC delivers the configuration to APs to instruct the APs to support the access of 802.11g STAs in 2.4 GHz.

Command	**11gsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with 802.11g support. The value range is from 1 to 96.
Defaults	By default, the access of 802.11g STAs is supported in 2.4 GHz.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 2.4 GHz. The configuration is supported only by specified APs.

Enabling 802.11na Support

- Optional.
- The configuration takes effect only when AP radios operate in 5 GHz.
- On the AC, enable 802.11na support for specified APs.
- The AC delivers the configuration to APs to instruct the APs to support the access of 802.11n STAs in 5 GHz.

Command	**11nasupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with 802.11na support. The value range is from 1 to 96.
Defaults	By default, the access of 802.11n STAs is supported in 5 GHz.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 5 GHz. The configuration is supported only by specified APs.

Enabling 802.11ng Support

- Optional.
- The configuration takes effect only when AP radios operate in 2.4 GHz.
- On the AC, enable 802.11ng support for specified APs.
- The AC delivers the configuration to APs to instruct the APs to support the access of 802.11n STAs in 2.4 GHz.

Command	**11ngsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with 802.11ng support. The value range is from 1 to 96.
Defaults	By default, the access of 802.11n STAs is supported in 2.4 GHz.

Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 2.4 GHz. The configuration is supported only by specified APs.

Enabling 802.11ac

- Optional.
- On the AC, enable 802.11ac support for specified APs.
- The AC delivers configuration to APs to instruct the APs to support the access of 802.11ac STAs.

Command	**11acsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with 802.11ac support. The value range is from 1 to 96.
Defaults	Only the radios with even IDs support the access of 802.11ac STAs.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Enabling 802.11ax

- Optional.
- On the AC, enable 802.11ax support for specified APs.
- The AC delivers configuration to APs to instruct the APs to support the access of 802.11ax STAs.

Command	**11axsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with 802.11ax support. The value range is from 1 to 96.
Defaults	802.11ax support l is disabled by default for radios that support 802.11ax.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Enabling 802.11be

- Optional.
- On the AC, enable 802.11be support for specified APs.
- The AC delivers configuration to APs to instruct the APs to support the access of 802.11be STAs.

Command	**11besupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with 802.11be support. The value range is from 1 to 96.
Defaults	802.11be is enabled for 802.11be-compliant radios.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Configuring the Highest Access Mode for a WLAN

- Optional.
- Configure the highest access mode supported by a WLAN.
- After this function is configured, the AC delivers the configuration to APs on the WLAN.

Command	**802.11 mode max** { **11ac** | **11ax** | **11be** }
Parameter Description	**11ac**: Sets the highest access mode to 802.11ac. **11ax**: Sets the highest access mode to 802.11ax. **11be**: Sets the highest access mode to 802.11be.
Defaults	The access mode configured for a radio is used.
Command Mode	WLAN configuration mode
Usage Guide	Use this command to configure the highest access mode. When the highest access mode is configured for a WLAN and a radio simultaneously, the lower one takes effect.

Configuring the Management Frame Power for APs

- Optional.
- Perform the configuration only on the required device unless otherwise specified.
- On the AC, configure the management frame power for specified APs.
- The AC delivers the configuration to APs to instruct the APs to use the configured management frame transmit power. In this way, signal coverage areas of the APs are controlled to limit the access of STAs.

Command	**coverage-area-control** *power* **radio** *radio-id*
Parameter Description	*power*: Specifies the management frame power. The value range is from 0 to 32, in the unit of dBm. *radio-id*: Specifies the ID of a radio assigned with channels. The value range is from 1 to 96.
Defaults	By default, the management frame power for APs is 0 dBm.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	N/A

Configuring the Minimum RSSI for STAs to Access APs

- Optional.
- On the AC, configure the minimum RSSI for STAs to access specified AP.
- The AC delivers the configuration to the APs to instruct the APs to use the configured minimum RSSI for allowing the access of STAs.

Command	**response-rssi** *rssi* **radio** *radio-id*
Parameter Description	*rssi: Specifies* the minimum RSSI for STAs to access APs. The value range is from 0 to 100, in the unit of dB. *radio-id*: Specifies the ID of a radio assigned with the minimum RSSI. The value range is from 1 to 96.
Defaults	By default, the RSSI is set to 0, indicating that there is no RSSI limit on the access of STAs.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Configuring the Minimum RSSI for STAs to Maintain Connections with APs

- Optional.
- On the AC, configure the minimum RSSI for wireless STAs to maintain connections to specified AP.
- The AC delivers the configuration to the APs to instruct the APs to use the configured minimum RSSI as the threshold for maintaining the connections of wireless STAs.

Command	**assoc-rssi** *rssi* **radio** *radio-id*
Parameter Description	*rssi: Specifies* the minimum RSSI for wireless STAs to maintain connections. The value ranges from 0 to 100, in the unit of dB. *radio-id*: Specifies the ID of a radio assigned with the minimum RSSI. The value ranges from 1 to 96.
Defaults	By default, the RSSI is set to 0, indicating that there is no RSSI limit on the access of wireless STAs.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Configuring the Third Radio for User Access

- Optional.
- On the AC, configure an AP in a high-density scenario.
- The channel, antenna, power, bandwidth will be adjusted for better access experience.

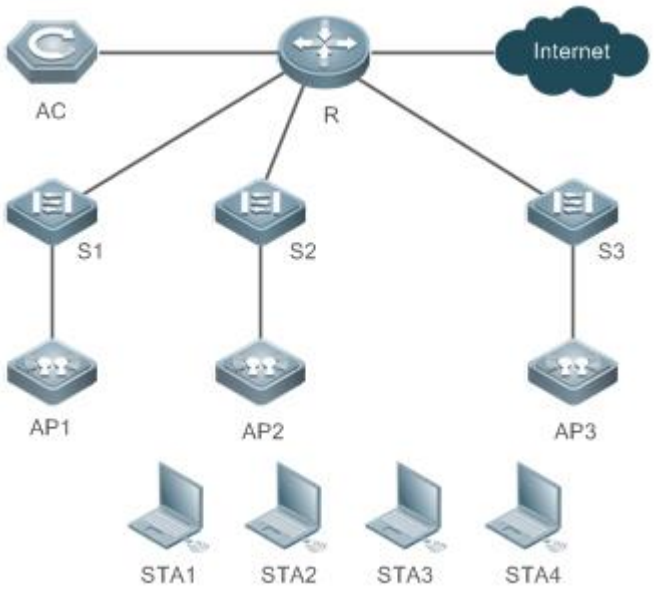
Command	**extra-coverage enable**
Parameter Description	N/A
Defaults	The third radio is disabled by default.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	Use the **no** form of this command to disable the function. Use the **default** form of this command to restore the default setting,

Verification

- Run **show ap-config running** *ap-name* to display parameter settings of STA access control.

Configuration Example

Configuring Parameters of STA Access Control

Scenario **Figure 1-4**	 In Figure 1-, an AC is connected to Fit APs. On the AC, configure STA access control for all the APs according to the following step: 1. Disable the 2.4 GHz network.
	On the AC, configure STA access control for AP1 according to the following steps: 1. Enable access of 802.11a and 802.11na STAs in 5 GHz 2. Enable access of 802.11g and 802.11ng STAs in 2.4 GHz. 3. Enable access of 802.11ac STAs. 4. Set the management frame power to 20 dBm. 5. Set the minimum RSSI for STAs to access APs to 20 dB. 6. Set the minimum RSSI for STAs to maintain connections to 15 dB. 7. Enable the third radio for user access.
Configuration Steps	● Disable the 2.4 GHz network on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ac-controller`
	`Hostname(config-ac)# 802.11b network disable`

	● Set STA access control parameters for AP1 on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# 11asupport enable radio 2`
	`Hostname(config-ap)# 11nasupport enable radio 2`
	`Hostname(config-ap)# 11gsupport enable radio 1`

	Hostname(config-ap)# 11ngsupport enable radio 1 Hostname(config-ap)# 11acsupport enable radio 1 Hostname(config-ap)# no 11bsupport enable radio 1 Hostname(config-ap)# coverage-area-control 20 Hostname(config-ap)# response-rssi 20 radio 1 Hostname(config-ap)# response-rssi 20 radio 2 Hostname(config-ap)# assoc-rssi 15 radio 1 Hostname(config-ap)# assoc-rssi 15 radio 2
Verification	● Run **show running-config** to check whether the 2.4 GHz or 5 GHz network is enabled or disabled.
AC	Hostname(config)# show running-config ! ac-controller sta-limit 1024 no capwap dtls enable 802.11b network disable country CN country US !
	● Run **show ap-config running** *ap-name* to display STA access control parameters for AP1.
AC	Hostname(config)# show ap-config running AP1 ! ap-config 220em no 11bsupport enable radio 1 coverage-area-control 20 response-rssi 20 radio 1 response-rssi 20 radio 2 assoc-rssi 15 radio 1 assoc-rssi 15 radio 2 radio-type 1 802.11b radio-type 2 802.11a !

1.4.3 Configuring AP's RF Parameters

Configuration Effect

- Configure RF parameters for APs and radios so that a network administrator can easily configure and manage APs.

Configuration Steps

Enabling A-MPDU

- Optional.
- On an AC, enable A-MPDU for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to enable A-MPDU.

Command	**802.11n a-mpdu enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the Is of a radio enabled with A-MPDU. The value range is from 1 to 96.
Defaults	By default, A-MPDU is enabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 802.11n, 802.11ac, or 802.11.ax mode. The configuration is supported only by specified APs.

Configuring the A-MPDU Aggregation Depth

- Optional.
- The AC will deliver the configuration to the corresponding AP, informing the AP of the supported aggregation depth.

Command	**ampdu-depth** *depth* **radio** *radio-id*
Parameter Description	*depth*: Indicates the aggregation depth to be configured. The value range is from 1 to 64. *radio-id*: Indicates the ID of a radio to be configured. The value range is from 1 to 96.
Defaults	By default, the A-MPDU aggregation depth is not configured, and the default aggregation depth of the device is used.
Command Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	The configuration only takes effect when the AP radio is operating in 802.11n, 802.11ac, or 802.11ax mode.

Enabling A-MSDU

- Optional.
- After enabling this function, the AC will deliver the configuration to the corresponding AP, instructing the AP to enable the A-MSDU function.

Command	**802.11n a-msdu enable** *radio radio-id*
Parameter Description	*radio-id:* Indicates the ID of a radio to be configured. The value range is from 1 to 96.
Defaults	The A-MSDU function is supported by default.

Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration only takes effect when the AP radio is operating in 802.11n, 802.11ac, or 802.11ax mode. This command cannot be configured for all APs simultaneously.

Configuring the A-MSDU Aggregation Depth

- Optional.
- The AC will deliver this configuration to the corresponding AP, informing the AP of the supported aggregation depth.

Command	**amsdu-depth** *depth* **radio** *radio-id*
Parameter Description	*Depth*: Indicates the aggregation depth. The value range is from 0 to 3. ● 0: Indicates that the maximum number of aggregated MSDU frames is not limited. ● 1: Indicates that the maximum number of aggregated MSDU frames is 32. ● 2: Indicates that the maximum number of aggregated MSDU frames is 16. ● 3: Indicates that the maximum number of aggregated MSDU frames is 8. *radio-id*: Indicates the ID of a radio. The value range is from 1 to 96.
Defaults	The A-MSDU aggregation depth is configured based on the AP capability by default.
Command Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	This configuration takes effect only when AP radios operate in 802.11n, 802.11ac, or 802.11ax mode.

Configuring the Maximum 802.11n MCS Index Value

- Optional.
- On an AC, configure the maximum 802.11n MCS index value for specified APs. Then the AC delivers the configuration to the APs to inform the APs of the maximum 802.11n MCS index value.

Command	**802.11n mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: Specifies the MCS index value, which ranges from 0 to 23. *radio-id*: Specifies the IDs of the radios assigned with the maximum 802.11n MCS index value. The value range is from 1 to 96.
Defaults	By default, the maximum 802.11n MCS index value is 23.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 802.11n or 802.11ac mode.

Configuring the Maximum 802.11ac MCS Index Value

- Optional.
- On an AC, configure the maximum 802.11ac MCS index value for specified AP. Then the AC delivers the configuration to the APs to inform the APs of the maximum 802.11ac MCS index value.

Command	**802.11ac mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: Specifies the MCS index value, which ranges from 0 to 79.

	radio-id: Specifies the IDs of the radios assigned with the maximum 802.11ac MCS index value. The value range is from 1 to 96.
Defaults	By default, the maximum 802.11n MCS index value is 79.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 802.11ac mode.

Configuring the Maximum 802.11ax MCS Index Value

- Optional.
- On an AC, configure the maximum 802.11ax MCS index value for specified APs. Then the AC delivers the configuration to the APs to inform the APs of the maximum 802.11ax MCS index value.

Command	**802.11ax mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: Specifies the MCS index value, which ranges from 0 to 95. *radio-id*: Specifies the IDs of the radios assigned with the maximum 802.11ac MCS index value. The value ranges from 1 to 96.
Defaults	By default, the maximum 802.11n MCS index value is 95.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	1. The configuration takes effect only when AP radios operate in 802.11ax mode. 2. Number of spatial streams = Maximum MCS index value/12 + 1 For example, if the maximum MCS index value is 31, the maximum number of spatial streams is 3.

Configuring the Maximum 802.11be MCS Index Value

- Optional.
- Configure the maximum 802.11be MCS index value for specified APs. After configuration, the MCS index value used by 802.11be does not exceed the configured value.

Command	**802.11be mcs support** *num* **radio** *radio-id*
Parameter Description	*num*: Specifies the MCS index value. The value range is from 0 to 223. *radio-id*: Indicates the ID of the radio to be configured. The value range is from 1 to 96.
Defaults	The maximum 802.11n MCS index value is 223.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	1. The configuration takes effect only when AP radios operate in 802.11be mode. 2. Number of spatial streams = Maximum MCS index value/14 + 1 For example, if the maximum MCS index value is 50, the maximum number of spatial streams is 4 and the maximum MCS index value of each spatial stream is 8 (that is, the remainder).

Configuring the Guard Interval

- Optional.

- The AC will deliver the configuration to the corresponding AP, instructing the AP radio to use the specified guard interval.

Command	**11ax-gi** { **0.8** | **1.6** | **3.2** | **auto** } **radio** *radio-id*
Parameter Description	*radio-id*: Indicates the ID of a radio to be configured. The value range is from 1 to 96. **0.8**: Configures it as 0.8 μs. **1.6**: Configures it as 1.6 μs. **3.2**: Configures it as 3.2 μs. **auto**: Configures the auto mode where parameters are adapted automatically.
Defaults	Auto mode
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Configuring the Antenna Transmit/Receive Type

- Optional.
- On an AC, configure the antenna transmit/receive type for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to use the specified antenna selection masks to send and receive packets.

Command	**antenna** { **transmit** | **receive** } *value* **radio** *radio-id*
Parameter Description	**transmit**: Indicates the antenna transmit parameter. **receive**: Indicates the antenna receive parameter. *value*: Specifies the antenna selection mask. The value range is from 1 to 255. *radio-id*: Specifies the ID of a radio assigned with the antenna transmit/receive type. The value range is from 1 to 96.
Defaults	In AP configuration mode, the default antenna selection mask varies with different device models and antenna quantities, and is determined based on the device model. By default, no antenna transmit/receive type is configured in AP group configuration mode.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 802.11n or 802.11ac mode.

Enabling External Antennas for APs

- Optional.
- On an AC, enable external antennas for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to enable external antennas and disable internal antennas.

Command	**external-antenna enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with the external antenna. The value range is from 1 to 96.
Defaults	By default, internal antennas are enabled and external antennas are disabled.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring Omnidirectional or Directional Antennas

- Optional.
- The AC delivers the configuration to an AP to notify the AP of the antenna to be used.

Command	**antenna type** { **omnidirection** | **direction** } **radio** *radio-id*
Parameter Description	**omnidirection**: Specifies an omnidirectional antenna. **direction**: Specifies a directional antenna. *radio-id*: Specifies the ID of a radio. The value range is from 1 to 96.
Defaults	An omnidirectional antenna is used by default.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	1. This configuration is valid only for radios supporting both omnidirectional and directional antennas. 2. If internal and external antennas can be switched, the configuration of internal and external antennas takes precedence over that of omnidirectional and directional antennas. 3. When no radio is specified, the configuration takes effect for all radios of an AP. 4. The **antenna type omnidirection** and **antenna type direction radio** *radio-id* commands cannot be simultaneously configured for a specific AP, AP group, or all APs; otherwise, the latest configuration overrides the previous configuration.

Configuring Built-in Directional Antennas to Work in Enhanced Mode

- Optional.
- After this function is configured, the AC delivers this configuration to the corresponding AP, enabling the built-in directional antennas of the AP to work in enhanced mode, This will decrease the coverage angle of the built-in directional antenna and enhance the transmit power in a specific direction.

Command	**antenna internal-direction enhance radio** *radio-id*
Parameter Description	*radio-id*: Indicates the ID of the radio to be configured. The value range is from 1 to 96.
Defaults	The enhanced mode of directional antennas does not take effect.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	1. The configuration takes effect only on radios where directional antennas are used and external antennas are disabled. 2. The configuration takes effect only for radios supporting enhanced mode of built-in directional antennas. 3. If built-in antennas are switched to external antennas, the configuration becomes invalid. 4. If the built-in antenna mode is switched to omnidirectional antenna mode, the configuration becomes invalid. 5. If no radio is specified, the configuration takes effect on all radios of the AP.

Configuring the Interval for Transmitting Beacon Frames

- Optional.
- On an AC, configure the interval for transmitting beacon frames for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to transmit beacon frames at intervals.

Command	**beacon period** *milliseconds* **radio** *radio-id*
Parameter Description	*milliseconds*: Specifies the interval for transmitting beacon frames. The value range is from 20 to 1000, in milliseconds. *radio-id*: Specifies the IDs of the radios assigned with the beacon frame transmission period. The value range iss from 1 to 96.
Defaults	By default, the interval for transmitting beacon frames is 100 ms.
Command Mode	AP configuration mode
Usage Guide	The configuration is supported only by specified APs.

Configuring Bandwidth Assignments

- Optional.
- On an AC, configure bandwidth assignments for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to switch the channel bandwidth to the specified bandwidth.

Command	**chan-width** { **20** | **40 | 80** | **160** } **radio** *radio-id*
Parameter Description	**20**: Specifies the 20 MHz bandwidth. **40**: Specifies the 40 MHz bandwidth. **80**: Specifies the 80 MHz bandwidth. **160**: Specifies the **160** MHz bandwidth. *radio-id*: Specifies the IDs of the radios assigned with bandwidth. The value ranges from 1 to 96.
Defaults	The default channel bandwidth of 5G radio on new 802.11ax devices is 40 Mbps. The default channel bandwidth of the other radio is 20 Mbps.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The bandwidth configuration takes effect only when the AP operates in 802.11n or higher mode.

Configuring Channel Assignments

- Optional.
- On an AC, configure channel assignments for specified APs. Then the AC delivers the configuration to the APs to instruct the AP radios to operate in specified channels.

Command	**channel** { **global** | *channel-id* } **radio** *radio-id*
Parameter Description	*channel-id*: Specifies the operating channel for an AP radio. *radio-id*: Specifies the ID of a radio assigned with a channel. The value range is from 1 to 96.
Defaults	The radio resource management (RRM) system automatically adjusts channels. By default, no channel assignments are configured.
Command Mode	AP configuration mode
Usage Guide	The configuration is supported only by specified APs.

Configuring the Country or Region Code Set Supported by an AC

- Optional.

- Add a country or region code to the country or region code set supported by an AC before you configure AP radios to use the country or region code.

Command	**country** *country-code*
Parameter Description	*country-code*: Specifies the country/region code to be added.
Defaults	The country or region code set supported by the AC is {"CN"}.
Command Mode	AC configuration mode
Usage Guide	The country or region code "CN" supported by the AC cannot be deleted.

Configuring a Country Code

- Optional.
- Ensure that the configured country or region code is in the country or region code set supported by an AC. The AC will assign the settings to the APs to instruct the APs to use the configured country or region code.

Command	**country** *country-code* **radio** *radio-id*
Parameter Description	*country-code*: Specifies the country/region code to be added. *radio-id*: Specifies the IDs of the radios assigned with the country/region code. The value ranges from 1 to 48.
Defaults	The country or region code used by APs is "CN".
Command Mode	AP configuration mode
Usage Guide	1. The country or region code "CN" supported by the AC cannot be deleted. 2. The configuration is supported only by specified APs. 3. Before you configure APs, determine the country or region code set supported by the AC. If the country or region code used by an AP is changed, the RF band, channel, and power for the AP are also changed. 4. 2.4 GHz radios do not support channel 14.

Configuring the Country or Region Code Set Supported by an AC

- Optional.
- Add a country or region code to the country or region code set supported by an AC before you configure AP radios to use the country or region code.

Command	**country-code** *country-code*
Parameter Description	*country-code*: Specifies the country or region code to be added.
Defaults	The country or region code set supported by the AC is CN.
Command Mode	AP configuration mode
Usage Guide	The country or region code "CN" supported by the AC cannot be deleted. For details about country codes, see WLAN Country or Region Codes and Channel Compliance. The supported countries are subject to the country codes that can be configured in the version.

Enabling Radios

- Optional.
- Enable radios on an AC. Then the AC delivers the configuration to the APs to instruct the APs to enable the corresponding radios.

Command	**enable-radio** { *radio-id* | **all** }
Parameter Description	*radio-id*: Specifies the IDs of the radios to be enabled. The value range is from 1 to 96. **all**: Indicates that all radios are enabled.
Defaults	By default, radios are enabled.
Command Mode	AP configuration mode
Usage Guide	When radios are enabled or disabled, STAs connected to the radios will go offline. The configuration is supported only by specified APs.

Configuring the Fragmentation Threshold

- Optional.
- On an AC, configure the fragmentation threshold for specified APs. Then the AC delivers the configuration to the APs to instruct the AP radios to perform fragmentation according to the configured threshold.

Command	**fragment-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: Specifies the fragmentation threshold, which must be an even number ranging from 256 to 2346. *radio-id*: Specifies the ID of a radio assigned with the fragmentation threshold. The value range is from 1 to 96.
Defaults	The default fragmentation threshold is 2346 bytes.
Command Mode	AP configuration mode
Usage Guide	The configuration is supported only by specified APs.

Configuring the Fragment Burst Mechanism

- Optional.
- The AC will deliver the configuration to the corresponding AP, instructing it to enable, disable, or dynamically adapt to the fragment burst mechanism of a radio.

Command	**fragment-burst** { **enable** | **disable** | **dynamic** } **radio** *radio-id*
Parameter Description	**enable**: Enables the fragment burst mechanism. **disable**: Disables the fragment burst mechanism. **dynamic**: Dynamically adapts to the fragment burst mechanism. *radio-id*: Indicates the ID of a radio to be configured. The value range is from 1 to 96.
Defaults	By default, the device dynamically adapts to the fragment burst mechanism.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Enabling the Protection Mode

- Optional.
- On an AC, enable the protection mode for specified APs. Then the AC delivers the configuration to the APs to instruct the AP radios to enable the protection mode.

Command	**green-field enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with the protection mode. The value range is from 1 to 96.
Defaults	By default, the protection mode is disabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 2.4 GHz.

Enabling the Mcell Function

- Optional.
- After this command is configured, the AP's receiving sensitivity will be reduced.

Command	**mcell enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio. The value range is from 1 to 96.
Defaults	By default, the Mcell function is disabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Reducing the Receive Sensitivity of a Radio

- Optional.
- After this command is configured, the receive sensitivity of a radio is reduced.

Command	**cell-range-reduction** *dbm* **radio** *radio-id*
Parameter Description	*dbm*: Specifies the receive sensitivity value to be decreased, in dBm. The value range is from 0 to 50. *radio-id*: Indicates the ID of the radio to be configured. The value range is from 1 to 96.
Defaults	The configuration is subject to the AP capability.
Command Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	N/A

Configuring the Anti-interference Level of a Radio

- Optional.
- After this command is configured, the anti-interference level of a radio can be adjusted.

Command	**anti-interference-level** *value* **radio** *radio-id*
Parameter Description	*value*: Configures the anti-interference level. The value range is from 0 to 15. *radio-id*: Indicates the ID of the radio to be configured. The value range is from 1 to 96.
Defaults	The anti-interference level of a radio is 0.

<table>
<tr><td>Command Mode</td><td>AP configuration mode, AP group configuration mode, or all-AP configuration mode</td></tr>
<tr><td>Usage Guide</td><td>When the co-channel interference in the environment is strong, a higher anti-interference level needs to be configured. The recommended configuration is as follows:
Distance between two APs: 8–15 m
<table>
<tr><th>Interference Strength</th><th>Anti-interference Level</th></tr>
<tr><td>Weak co-channel interference (< –95 dBm)</td><td>0</td></tr>
<tr><td>Weak co-channel interference (–95 dBm to –90 dBm)</td><td>2</td></tr>
<tr><td>Weak co-channel interference (–90 dBm)</td><td>3</td></tr>
<tr><td>Weak co-channel interference (–85 dBm)</td><td>4</td></tr>
<tr><td>Strong co-channel interference (–80 dBm)</td><td>5</td></tr>
</table>
Distance between two APs: 6–8 m
<table>
<tr><th>Interference Strength</th><th>Anti-interference Level</th></tr>
<tr><td>Weak co-channel interference (–90 dBm)</td><td>8</td></tr>
<tr><td>Weak co-channel interference (–85 dBm)</td><td>9</td></tr>
<tr><td>Strong co-channel interference (–80 dBm)</td><td>10</td></tr>
</table>
Distance between two APs:< 6 m
<table>
<tr><th>Interference Strength</th><th>Anti-interference Level</th></tr>
<tr><td>Weak co-channel interference (–85 dBm)</td><td>14</td></tr>
<tr><td>Strong co-channel interference (–80 dBm)</td><td>15</td></tr>
</table>
This command can be configured only on the RG-AP9751-R and RG-AP9520-RDX.</td></tr>
</table>

Configure MIMO

- Optional.
- After this command is configured, the AC will deliver the configuration to the AP to enable the MU-MIMO function on the AP.

Command	**mu-mimo enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio. The value range is from 1 to 96.
Defaults	If the radio does not support the MU-MIMO function, the AC does not support it by default. If the radio supports the MU-MIMO function and MU-MIMO is enabled on the AP by default, it is enabled on the AC by default. If the radio supports the MU-MIMO function and MU-MIMO is disabled on the AP by default, it is disabled on the AC by default.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	N/A

Enabling OFDMA for a Radio

- Optional.
- After this command is configured, 802.11ax STAs can transmit data by using OFDMA.

Command	**ofdma enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio. The value range is from 1 to 96.
Defaults	By default, OFDMA is enabled.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	N/A

Configuring the Maximum Distance of Wireless Transmission Between an AP and the Peer End

- Optional.
- On an AC, configure the maximum distance of wireless transmission between an AP and the peer end. Then the AC delivers the configuration to the AP to instruct the AP radios to send and receive packets based on the maximum distance.

Command	**peer-distance** *val* **radio** *radio-id*
Parameter Description	*val*: Specifies the maximum wireless transmission distance allowed by APs. The value ranges from 1000 to 25000, in the unit of m. *radio-id*: Specifies the ID of a radio assigned with the maximum wireless transmission distance. The value range is from 1 to 96.
Defaults	By default, the maximum wireless transmission distance is 1000 m.
Command Mode	AP configuration mode
Usage Guide	The configuration is supported only by specified APs. The configuration is mandatory only when the actual maximum distance of wireless transmission between an AP and the peer end is greater than 1000 m. You can set the distance to a large value but do not set it to a value smaller than the actual distance.

Configuring the Transmit Power

- Optional.
- On an AC, configure the transmit power for specified APs. Then the AC delivers the configuration to the APs to instruct the AP radios to use the transmit power.

Command	**power local** *power* **radio** *radio-id* **power local-dbm** *dbm-value* **radio** *radio-id*
Parameter Description	*power*: Specifies the percent of transmit power for APs. The value range is from 1 to 100. *radio-id*: Specifies the ID of a radio assigned with the transmit power. The value range is from 1 to 96. *dbm-value*: Specifies the transmit power of an AP in dBm. The value range is from 1 to 36.
Defaults	By default, the percentage of the transmit power is set to 100%.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	• The configuration is supported only by specified APs.

	● When both **local** and **local-dbm** are configured, the configuration of **local-dbm** takes effect.

Configuring the Preamble Type

- Optional.
- The AC will deliver the configuration to the corresponding AP to instruct it to work with the specified preamble code type.

Command	**preamable** { **long** | **short** } **radio** *radio-id*
Parameter Description	**long**: Specifies the AP to transmit frames with the long preamble code only. **short**: Specifies the AP to transmit frames with the short or long preamble code. *radio-id*: Indicates the ID of a radio to be configured. The value range is from 1 to 96.
Defaults	By default, the short preamble code is supported.
Command Mode	AP configuration mode
Usage Guide	The configuration is supported only by specified APs.

Configuring Radio Parameters (Power, Channel, and Antenna Receive/Transmit Type)

- Optional.
- After this command is configured, the AC will change the radio type or optimize the power, channel, antenna configuration and deliver the configuration to the AP.

Command	**radio-optimize**
Parameter Description	N/A
Defaults	By default, this function is disabled.
Command Mode	AP configuration mode
Usage Guide	This command cannot be configured in all-AP configuration mode. If the target AP is offline, you can optimize the radio configuration but cannot change the radio type. To change the radio type, run the radio-type command. The optimized configuration will be saved and take effect next time when the AP goes online. If the target AP is online, you can optimize the radio configuration and change the radio type. You can also optimize the current radio configuration without changing the radio type. If the AP does not support this function, the radio configuration will not be changed. If the AP supports this function, the radio configuration will be optimized immediately and this command will be saved.

Configuring a Frequency Band

- Optional.
- After a frequency band is assigned to AP radios, the RRM module analyzes the operating channel of the AP radios in global mode, adjusts the channel, and assigns the optimal channel to the AP. The AP radios are instructed to operate in the specified channel.

Command	**radio-type** *radio-id* { **802.11a** | **802.11b** | **6GHz** }
Parameter Description	*radio-id*: Specifies the IDs of the radios assigned with the frequency band. The value ranges from 1 to 96.

	802.11a: Specifies the 5 GHz operating band. **802.11b**: Specifies the 2.4 GHz operating band. **6GHz**: Specifies the 6 GHz operating band.
Defaults	A single-band AP (radio 1) supports the 2.4 GHz frequency band. For a dual-band AP, radio 1 supports the 2.4 GHz frequency band, and radio 2 supports the 5 GHz frequency band.
Command Mode	AP configuration mode
Usage Guide	The configuration is supported only by certain APs.

Configuring the RTS Threshold

- Optional.
- On an AC, configure the RTS threshold for specified APs. Then the AC delivers the configuration to the APs to instruct the AP radios to use the configured threshold.

Command	**rts-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: Specifies the value of the RTS threshold. The value range is from 257 to 2347, in the unit of bytes. *radio-id*: Specifies the ID of a radio assigned with the RTS threshold. The value range is from 1 to 96.
Defaults	The default RTS threshold is 2347.
Command Mode	AP configuration mode
Usage Guide	N/A

Enabling Short GI

- Optional.
- On an AC, enable short GI for specified APs. Then the AC delivers the configuration to the APs to instruct the AP radios to use short GI.

Command	**short-gi enable radio** *radio-id* **chan-width** { **20** | **40** | **80** | **160** }
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with short GI. The value range is from 1 to 96. **20**: Specifies the 20 MHz bandwidth. **40**: Specifies the 40 MHz bandwidth. **80**: Specifies the 80 MHz bandwidth. **160**: Specifies the 160 MHz bandwidth.
Defaults	For 2.4G radio, enable 20 MHz and 40 MHz bandwidths and disable 80 MHz and 160 MHz bandwidths; for 5G radio, enable all bandwidths. The 6 GHz radio does not support this function.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Configuring the Short Slot Time

- Optional.
- On an AC, configure the short slot time for specified APs. Then the AC delivers the configuration to the APs to instruct the AP radios to enable the short slot time feature.

Command	**short-slot-time radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio assigned with the short slot time. The value range is from 1 to 96.
Defaults	By default, the short slot time function is enabled
Command Mode	AP configuration mode
Usage Guide	N/A

Enabling Transmit Beamforming

- Optional.
- After this function is enabled, the AC will deliver the configuration to the corresponding AP, instructing it to enable or disable transmit beamforming.

Command	**txbf enable radio** *radio-id*
Parameter Description	*radio-id*: Indicates the ID of a radio to be configured. The value range is from 1 to 96.
Defaults	By default, the transmit beamforming function is supported.
Command Mode	AP configuration mode, all-AP configuration mode, or AP group configuration mode
Usage Guide	The configuration takes effect only when the AP radio operates in 802.11ac or 802.11ax mode.

Enabling TSC Update

- Optional.
- On an AC, enable TSC update for specified APs. Then the AC delivers the configuration to the APs to instruct the AP to enable TSC update.

Command	**update-key-tsc enable**
Parameter Description	N/A
Defaults	By default, TSC update is disabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Configuring Multi-BSSID

- Optional.
- After this command is configured, the BSSID of the specified radio is sent over one beacon.

Command	**multi-bssid enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID, in the range from 1 to 96.
Defaults	This function is enabled on the 2.4 GHz and 5 GHz radios and disabled on the 6 GHz radio by default.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	The Multi-BSSID function cannot be disabled on the 6 GHz frequency band.

> ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Configuring RNR

- Optional.
- After this command is configured, the device advertises 6G radio information through beacon and probe response frames of 2.4 GHz and 5 GHz radios or advertises other channel information through Preferred Scanning Channel (PSC) of the 6 GHz radio.

Command	**rnr enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID, in the range from 1 to 96.
Defaults	This function is disabled on the 2.4 GHz, 5 GHz, and 6 GHz radios by default.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Configuring Announcement on a Radio

- Optional.
- When FILS announcement is configured, FILS frames are sent at an interval of 20 ms.
- When UPRS announcement is configured, UPRS packets are sent at an interval of 20 ms.

Command	**ap-announcement-mode** { **fils** | **uprs** } **radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID. The value range is from 1 to 96. **fils**: Enables FILS announcement and disables UPRS announcement. **uprs**: Enables UPRS announcement and disables FILS announcement.
Defaults	FILS and UPRS announcement are not applicable to 2.4 GHz and 5 GHz frequency bands, and they are disabled on the 6 GHz frequency band.
Command Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Configuring BSS Color

- Optional.
- After this command is configured, the BSS Color field is added to the packet header to distinguish BSS.

Command	**bss-color enable radio** *radio-id*

Parameter Description	*radio-id*: Specifies the radio ID, in the range from 1 to 96.
Defaults	BSS Color is disabled by default.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	N/A

Configuring TWT

- Optional.
- After this command is configured, the TWT field is added to the beacon packet.

Command	**twt enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the radio ID, in the range from 1 to 96.
Defaults	TWT is enabled by default.
Command Mode	AP configuration mode, AP group configuration mode, and all-AP configuration mode
Usage Guide	N/A

Configuring QBSS Load

- Optional.
- After this function is configured, the AC will deliver the configuration to the corresponding AP.

Command	**qbss-load enable radio** *radio-id*
Parameter Description	*radio-id*: Indicates the ID of a radio. The value range is from 1 to 96.
Defaults	By default, QBSS load is configured based on the AP capability value.
Command Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	N/A

Configuring the BAR Retransmission Count

- Optional.
- After the BAR retransmission count is configured, the AC will deliver the configuration to the corresponding AP.

Command	**bar-retries** *times* **radio** *radio-id*
Parameter Description	*times*: Indicates the BAR retransmission count. The value range is from 1 to 50. *radio-id*: Indicates the ID of a radio. The value range is from 1 to 96.
Defaults	By default, the BAR retransmission count is configured based on the AP capability value.
Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	N/A

Verification

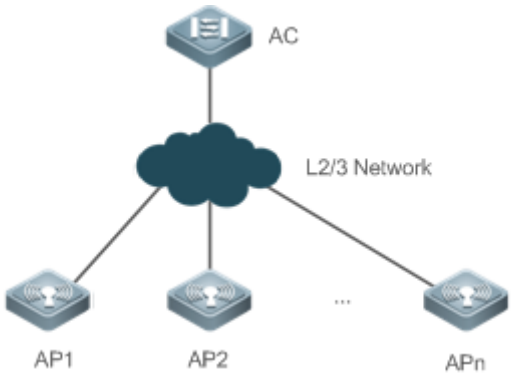
- Run **show ap-config running** *ap-name* to display parameter settings of STA access control.

Configuration Example

Configuring AP RF Parameters

Scenario

Figure 1-5



In Figure 1-5, an AC is connected to Fit APs. On the AC, configure RF parameters for AP1 by performing the following steps:

1. Set the global country or region code to CN.
2. Configure CN support on the AC.
3. Enable A-MPDU for radio 1 of AP1.
4. Set the aggregation depth to 12 for radio 1 of AP 1.
5. Enable A-MSDU for radio 1 of AP 1.
6. Set the maximum 802.11n MCS index value to 15 for radio 1 of AP1.
7. Set the maximum 802.11ac MCS index value to 19 for radio 1 of AP1.
8. Set the maximum 802.11ax MCS index value to 21 for radio 2 of AP1.
9. Set the antenna selection masks of the transmit type and receive type to 7 and 5 respectively for radio 1 of AP1.
10. Enable external antennas and disable usage of internal antennas for radio 1 of AP1.
11. Enable the directional antenna on AP1.
12. Set the interval for transmitting beacon frames to 200 ms for radio 1 of AP1.
13. Configure the country code CN for radio 1 of AP1.
14. Assign channel 11 to radio 1 of AP1.
15. Assign 20 MHz bandwidth to radio 1 of AP1.
16. Enable short GI for radio 1 of AP1 in 20 MHz.
17. Enable the protection mode for radio 1 of AP1.
18. Configure 3.2 μs guard interval for 802.11ax packets on radio 2 of AP1.
19. Configure the short preamble type for radio 1 of AP1.
20. Configure the short slot time for radio 1 of AP1.
21. Assign channel 149 to radio 2 of AP1.
22. Assign 40 MHz bandwidth to radio 2 of AP1.
23. Enable radio 2 of AP1.
24. Set the fragmentation threshold to 2346 bytes for radio 2 of AP1.
25. Set the percent of the transmit power to 100% for radio 2 of AP1.
26. Set the RTS threshold to 2347 bytes for radio 2 of AP1.

	27. Enables TSC update for AP1. 28. Set the maximum distance of wireless transmission between an AP and the peer end to 3000 m for radio 1 of AP1. 29. Enable transmit beamforming for radio 2 of AP 1.
	30. Enable MU-MIMO for radio 2 of AP1. 31. Enable MCell for radio 1 of AP 1. 32. Enable OFDMA for radio 2 of AP1.
Configuration Steps	● On the AC, configure RF parameters for AP1.
	Hostname# configure terminal Hostname(config)# country-code CN Hostname(config)# ac-controller Hostname(config-ac)# country CN Hostname(config-ac)# exit Hostname(config)# ap-config AP1 Hostname(config-ap)# 802.11n a-mpdu enable radio 1 Hostname(config-ap)# ampdu-depth 12 radio 1 Hostname(config-ap)# 802.11n a-msdu enable radio 1 Hostname(config-ap)# 802.11n mcs support 15 radio 1 Hostname(config-ap)# 802.11ac mcs support 19 radio 1 Hostname(config-ap)# 802.11ac mcs support 21 radio 2 Hostname(config-ap)# antenna transmit 7 radio 1 Hostname(config-ap)# antenna receive 5 radio 1 Hostname(config-ap)# external-antenna enable radio 1 Hostname(config-ap)# country CN radio 1 Hostname(config-ap)# antenna type direction Hostname(config-ap)# beacon period 200 radio 1 Hostname(config-ap)# country CN radio 1 Hostname(config-ap)# channel 11 radio 1 Hostname(config-ap)# chan-width 20 radio 1 Hostname(config-ap)# short-gi enable radio 1 chan-width 20 Hostname(config-ap)# green-field enable radio 1 Hostname(config-ap)# preamble short radio 1 Hostname(config-ap)# short-slot-time radio 1 Hostname(config-ap)# channel 149 radio 2

```
Hostname(config-ap)# chan-width 40 radio 2
Hostname(config-ap)# enable-radio 2
Hostname(config-ap)# fragment-threshold 2346 radio 2
Hostname(config-ap)# power local 100 radio 2
Hostname(config-ap)# rts-threshold 2347 radio 2
Hostname(config-ap)# update-key-tsc enable
Hostname(config-ap)# peer-distance 3000 radio 1
Hostname(config-ap)# txbf enable radio 2
Hostname(config-ap)# mu-mimo enable radio 2
Hostname(config-ap)# mcell enable radio 1
Hostname(config-ap)# ofdma enable radio 2
```

Verification Run **show ap-config running** *ap-name* to display RF parameter settings of AP1.

```
Hostname(config)# show ap-config running AP1
!
ap-config AP1
802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
802.11ac mcs support 19 radio 1
 update-key-tsc enable
 short-gi enable radio 1 chan-width 20
 green-field enable radio 1
 station-role root-ap radio 1
 station-role root-ap radio 2
 chan-width 40 radio 2
 antenna receive 5 radio 1
external-antenna enable radio 1
 channel 11 radio 1
 channel 149 radio 2
 beacon period 200 radio 1
 power local 100 radio 2
peer-distance 3000 radio 1
mu-mimo enable radio 2
mcell enable radio 1
!
```

1.4.4 Configuring Data Rate Control Parameters

Configuration Effect

- Configure data rate control parameters for Fit APs so that a network administrator can easily configure and manage them.

Configuration Steps

Configuring the Data Rate Set Supported by 802.11a (5 GHz) STAs or 6 GHz STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11a STAs. Then the AC delivers the configuration to all the APs to instruct the APs to apply the configured data rate set to 802.11a (5 GHz) STAs or 6 GHz STAs.

Command	{ **802.11a** | **6GHz** } **network rate** { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }
Parameter Description	**6**: Specifies the 6 Mbps data rate. **9**: Specifies the 9 Mbps data rate. **12**: Specifies the 12 Mbps data rate. **18**: Specifies the 18 Mbps data rate. **24**: Specifies the 24 Mbps data rate. **36**: Specifies the 36 Mbps data rate. **48**: Specifies the 48 Mbps data rate. **54**: Specifies the 54 Mbps data rate. **disabled**: Indicates that the data rate set is not supported. **mandatory**: Indicates that support for the data rate set is mandatory. **supported**: Indicates that support for the data rate set is optional.
Defaults	Support for the 6 Mbps, 12 Mbps, and 24 Mbps data rates is mandatory, whereas support for the 9 Mbps, 18 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps data rates is optional.
Command Mode	AC configuration mode, AP configuration mode, or AP group configuration mode
Usage Guide	N/A

Configuring the Data Rate Set Supported by 802.11b STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11b STAs. Then the AC delivers the configuration to all the APs to instruct the APs to apply the configured data rate set to 802.11b STAs.

Command	**802.11b network rate** { **1** | **2** | **5** | **11** } { **disabled** | **mandatory** | **supported** }
Parameter Description	**1**: Specifies the 1 Mbps data rate. **2**: Specifies the 2 Mbps data rate. **5**: Specifies the 5.5 Mbps data rate. **11**: Specifies the 11 Mbps data rate. **disabled**: Indicates that the data rate set is not supported. **mandatory**: Indicates that support for the data rate set is mandatory. **supported**: Indicates that support for the data rate set is optional.

Defaults	Support for the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps data rates is mandatory.
Command Mode	AC configuration mode, AP configuration mode, or AP group configuration mode
Usage Guide	The **disabled** configuration takes effect only when radio frequency is set to 802.11b mode. In addition, if low-speed rates that overlap with those of 802.11b are disabled in 802.11g mode, the corresponding rates in 802.11b will also be disabled.

Configuring the Data Rate Set Supported by 802.11g STAs

- Optional.
- On an AC, configure the data rate set supported by 802.11g STAs. Then the AC delivers the configuration to all the APs to instruct the APs to apply the configured data rate set to 802.11g STAs.

Command	**802.11g network rate** { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disabled** | **mandatory** | **supported** }
Parameter Description	**1**: Specifies the 1 Mbps data rate. **2**: Specifies the 2 Mbps data rate. **5**: Specifies the 5.5 Mbps data rate. **6**: Specifies the 6 Mbps data rate. **9**: Specifies the 9 Mbps data rate. **11**: Specifies the 11 Mbps data rate. **12**: Specifies the 12 Mbps data rate. **18**: Specifies the 18 Mbps data rate. **24**: Specifies the 24 Mbps data rate. **36**: Specifies the 36 Mbps data rate. **48**: Specifies the 48 Mbps data rate. **54**: Specifies the 54 Mbps data rate. **disabled**: Indicates that the data rate set is not supported. **mandatory**: Indicates that support for the data rate set is mandatory. **supported**: Indicates that support for the data rate set is optional.
Defaults	Support for the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps data rates is mandatory, whereas support for the 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps data rates is optional.
Command Mode	AC configuration mode, AP configuration mode, or AP group configuration mode
Usage Guide	When the low-speed rates of 1 Mbps, 2 Mbps, and 5.5 Mbps, which overlap with the 802.11b data rate set, are disabled in 802.11g mode, the corresponding rates in 802.11b will also be disabled.

Configuring the Rate at Which Beacon Frames Are Transmitted

- Optional.
- On an AC, configure the rate at which beacon frames are transmitted for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to transmit beacon frames at the configured rate.

Command	**beacon rate** *rate-Mbps* **radio** *radio-id*
Parameter Description	*rate_Mbps*: Specifies the rate at which beacon frames are transmitted.

	radio-id: Specifies the ID of a radio assigned with the rate at which beacon frames are transmitted. The value range is from 1 to 96.
Defaults	By default, no rate at which beacon frames are transmitted is configured.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The rate that is disabled in the data rate set settings cannot be configured. Because the 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps rates are not supported in 5 GHz, do not set the rate to any of the preceding values for radios in 5 GHz.

Configuring the Multicast Rate

- Optional.
- On an AC, configure the multicast rate for a WLAN. Then the AC delivers the configuration to all the APs on the WLAN to instruct the APs to apply the configured multicast rate within the range of the WLAN.

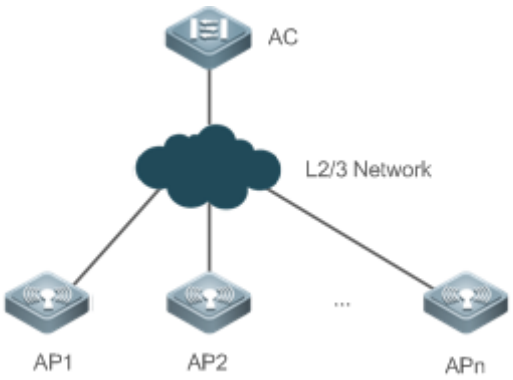
Command	**mcast-rate** *mcas-num*
Parameter Description	*mcast-num*: Specifies the WLAN multicast rate. The 1 Mbps, 6 Mbps, 11 Mbps, 24 Mbps, and 54 Mbps options are available.
Defaults	The default multicast rate is 24 Mbps.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run **show running-config** to display parameter settings of data rate control.

Configuration Example

Configuring Data Rate Control Parameters

Scenario **Figure 1-6**	 In Figure 1-6, an AC is connected to Fit APs. On the AC, configure data rate control parameters by performing the following steps: 1. Disable the 6 Mbps rate for 802.11a STAs. 2. Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11b STAs. 3. Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11g STAs. 4. Set the multicast rate for WLAN1 to 54 Mbps.

	On the AC,configure the rate at which beacon frames are transmitted for radio 1 of AP1.
Configuration Steps	● On the AC, configure data rate control parameters.
	Hostname# configure terminal Hostname(config)# ac-controller Hostname(config-ac)# 802.11a network rate 6 disabled Hostname(config-ac)# 802.11b network rate 1 disabled Hostname(config-ac)# 802.11b network rate 2 disabled Hostname(config-ac)# 802.11b network rate 5 disabled Hostname(config-ac)# 802.11g network rate 1 disabled Hostname(config-ac)# 802.11g network rate 2 disabled Hostname(config-ac)# 802.11g network rate 5 disabled Hostname(config-ac)# exit Hostname(config)# wlan-config 1 Hostname(config-wlan)# mcast-rate 54
	● On the AC, configure the rate at which beacon frames are transmitted for AP1.
	Hostname# configure terminal Hostname(config)# ap-config AP1 Hostname(config-ap)# beacon rate 12.0 radio 1
Verification	● Run **show running-config** to display parameter settings of data rate control.
	Hostname# show running-config ... ! wlan-config 1 ss enable-broad-ssid mcast-rate 54 ! ... ! ac-controller

```
country CN
802.11g network rate 1 disabled
802.11g network rate 2 disabled
802.11g network rate 5 disabled
802.11g network rate 11 mandatory
802.11g network rate 6 supported
802.11g network rate 9 supported
802.11g network rate 12 supported
802.11g network rate 18 supported
802.11g network rate 24 supported
802.11g network rate 36 supported
802.11g network rate 48 supported
802.11g network rate 54 supported
802.11b network rate 1 disabled
802.11b network rate 2 disabled
802.11b network rate 5 disabled
802.11b network rate 11 mandatory
802.11a network rate 6 disabled
802.11a network rate 9 supported
802.11a network rate 12 mandatory
802.11a network rate 18 supported
802.11a network rate 24 mandatory
802.11a network rate 36 supported
802.11a network rate 48 supported
802.11a network rate 54 supported
!
...
```

- Run **show ap-config running** *ap-name* to display the rate at which beacon frames are transmitted of AP1.

```
Hostname(config)# show ap-config running AP1
!
ap-config AP1
channel 11 radio 1
 channel 149 radio 2
```

	beacon period 200 radio 1 beacon rate 12.0 radio 1 power local 100 radio 2 !

1.4.5 Configuring Power Saving Parameters

Configuration Effect

- Configure power saving parameters for Fit APs so that a network administrator can easily configure and manage them.

Configuration Steps

Enabling or Disabling U-APSD Power Saving

- Optional.
- Enable U-APSD power saving to reduce the delay of services with high real-time performance requirements during power management. The transmission of radio signals can be disabled during most of the time to extends the battery life.

Command	**apsd** { **enable** | **disable** } **radio** *radio-id*
Parameter Description	**enable**: Enables U-APSD power saving. **disable**: Disables U-APSD power saving. *radio-id*: Specifies the IDs of the radios enabled with U-APSD power saving. The value ranges from 1 to 96.
Defaults	By default, U-APSD power saving is enabled.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the DTIM Period

- Optional.
- The power saving effect is improved if the DTIM period is set to a large value, but the delay for downstream multicast packets is increased.

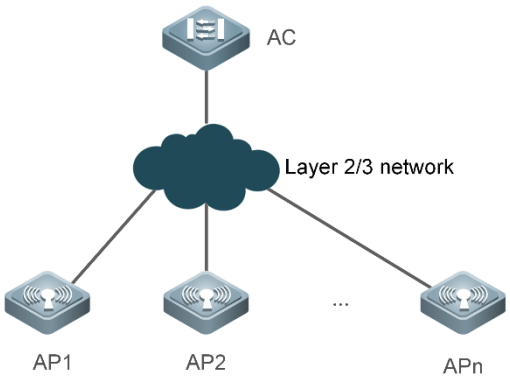
Command	**beacon dtim-period** *period-num* **radio** *radio-id*
Parameter Description	*period-num*: Specifies the DTIM period. The value range is from 1 to 255. The unit is expressed as the period of one beacon frame. *radio-id*: Specifies the ID of a radio assigned with the DTIM period. The value range is from 1 to 96.
Defaults	By default, the DTIM period is expressed as the period of one beacon frame.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run **show ap-config running** *ap-name* to display power saving parameter settings.

Configuration Example

Configuring Power Saving Parameters

Scenario **Figure 1-7**	
Configuration Steps	• On the AC, set the DTIM period to 3 for radio 1 of AP1. • On the AC, enable U-APSD power saving for radio 1 of AP1.

	`Hostname#configure terminal`
	`Hostname(config)#ap-config AP0001`
	`Hostname(config-ap)#beacon dtim-period 3 radio 1`
	`Hostname(config-ap)#apsd enable radio 1`

Verification	• Run **show ap-config running** *ap-name* to display power saving parameter settings of AP1.

	`Hostname(config)# show ap-config running AP1`
	`!`
	`ap-config AP1`
	`802.11n mcs support 15 radio 1`
	`802.11n mcs support 15 radio 2`
	`update-key-tsc enable`
	`short-gi enable radio 1 chan-width 20`
	`green-field enable radio 1`
	`station-role root-ap radio 1`
	`station-role root-ap radio 2`
	`chan-width 40 radio 2`
	`antenna receive 5 radio 1`
	`channel 11 radio 1`
	`channel 149 radio 2`

	beacon period 200 radio 1 beacon dtim-period 3 radio 1 power local 100 radio 2 !

1.4.6 Enabling Link Integrity Detection

Configuration Effect

- Enable link integrity detection.

Configuration Steps

Enabling Link Integrity Detection

- Mandatory. Run **link-check enable** to enable link integrity detection.

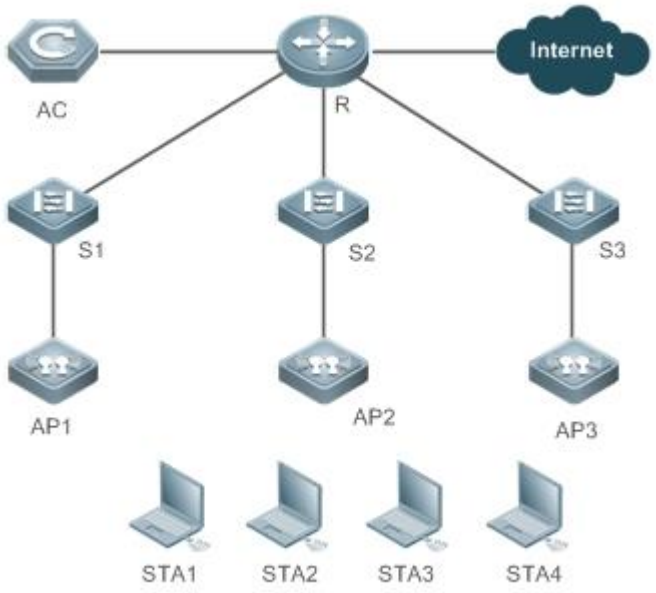
Command	**link-check enable**
Parameter Description	N/A
Defaults	By default, link integrity detection is disabled.
Command Mode	Global configuration mode
Usage Guide	By default, link integrity detection is disabled.

Verification

Run **show running-config** to display the status of link integrity detection.

Configuration Example

Enabling Link Integrity Detection

Scenario **Figure 4-3**	 In Figure 4-3, an AC is connected to Fit APs. Enable link integrity detection.
Configuration Steps	Enable link integrity detection on the AC.
	`Hostname# configure terminal` `Hostname(config)# link-check enable`
Verification	Run **show running-config** to display the status of link integrity detection.

	`Hostname(config)# show running-config`
	`……`
	`link-check enable`
	`……`

1.4.7 Configuring E-Bag Parameters

Configuration Effect

Configure E-bag parameters for APs and radios so that a network administrator can easily configure and manage them.

Configuration Steps

Configuring the A-MPDU Software Retransmission Count

- Optional.
- On an AC, configure the A-MPDU software retransmission count for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to transmit A-MPDU packets based on the retransmission count.
- A larger retransmission count indicates a lower probability of sub-frame loss. If packets are retransmitted frequently, the burden on the air interface is increased, which affects the real-time transmission of packets on the air interface.

You can increase the retransmission times if you need to avoid packet loss when there is a high probability of sub-frame loss.

Command	**ampdu-retries** *times* **radio** *radio-id*
Parameter Description	*times*: Specifies the A-MPDU software retransmission count. The value range is from 1 to 10. *radio-id*: Specifies the ID of a radio assigned with the A-MPDU software retransmission count. The value range is from 1 to 96.
Defaults	By default, the A-MPDU software retransmission count is 10.
Command Mode	AP configuration mode
Usage Guide	The configuration takes effect only when AP radios operate in 802.11n or 802.11ac mode. The configuration is supported only by specified APs.

Enabling or Disabling RTS Protection for A-MPDU Packets

- Optional.
- On an AC, enable RTS protection for A-MPDU packets for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to transmit A-MPDU packets using RTS protection.
- Enable RTS protection only when the resource waste on the air interface caused by hidden nodes is greater than the resource consumption of RTS interaction on the air interface.

Command	**ampdu-rts radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with RTS protection. The value range is from 1 to 96.
Defaults	By default, RTS protection for A-PMDU packets is disabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Configuring E-bag Network Optimization in One-Click Mode

- Optional.
- In AP configuration mode, run the **ebag** command to quickly configure e-bag network optimization.
- Optimization items for the AP530 are as follows:

  (1) Use default STA idle time of 1800 for radio 1 and 2

  (2) Optimization for radio 1: Disable the mandatory rate of 125 Mbps for 802.11b/802.11g STAs, disable the mandatory rate of 1124 Mbps for 802.11g STAs, and enable A-MPDU RTS.
- The AC will deliver the configuration to the corresponding AP, instructing it to use the specified parameters for packet transmission and receiving.

Command	**ebag**
Parameter Description	N/A
Defaults	By default configuration, e-bag network optimization is not configured.
Command Mode	AP configuration mode

Usage Guide It is typically used for e-bag scenarios. Use it with caution in other scenarios.

Configuring the Single-Time Received Ethernet Packet Quantity for APs

- Optional.
- By default, the single-time received Ethernet packet quantity varies with APs.
- On an AC, configure the single-time received Ethernet packet quantity for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to limit the number of Ethernet packets received at a single time according to the settings. Increasing Ethernet packet receiving can improve network performance but may reduce APs' capability to handle key packets in real time. You can reduce Ethernet packet receiving when the requirements for performance are not high but user concurrency and real-time packet handling are required. In this case, it is recommended that the single-time received Ethernet packet quantity be set to 25.

Command	**eth-schd** *limit*
Parameter Description	*limit*: Specifies the number of Ethernet packets received at a single time. The value rang is from 1 to 256.
Defaults	By default, the single-time received Ethernet packet quantity varies with APs.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Enabling or Disabling LDPC

- Optional.
- On an AC, enable LDPC for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to send and receive packets using LDPC.
- LDPC improves the coding reliability and gains. It also greatly reduces the probability of information loss during transmission in frequencies with serious noise interference. However, a small number of STAs are incompatible with LDPC, and enabling LDPC will result in packet loss.

Command	**ldpc radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with LDPC. The value range is from 1 to 96.
Defaults	By default, LDPC is enabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Enabling or Disabling Transmit/Receive STBC

- Optional.
- On an AC, enable transmit/receive STBC for specified APs. Then the AC delivers the configuration to the APs to instruct the APs to send and receive packets using STBC.
- STBC improves the reliability of data transmission. Some STAs may be incompatible with STBC.

Command	**stbc radio** *radio-id*

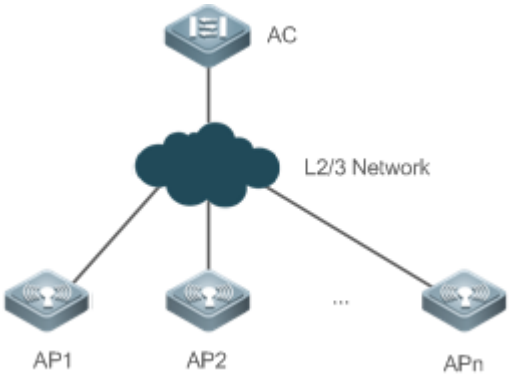
Parameter Description	*radio-id*: Specifies the ID of a radio enabled with STBC. The value range is from 1 to 96.
Defaults	By default, STBC is enabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Verification

- Run **show ap-config running** *ap-name* to display E-bag parameter settings.

Configuration Example

Configuring E-Bag Parameters

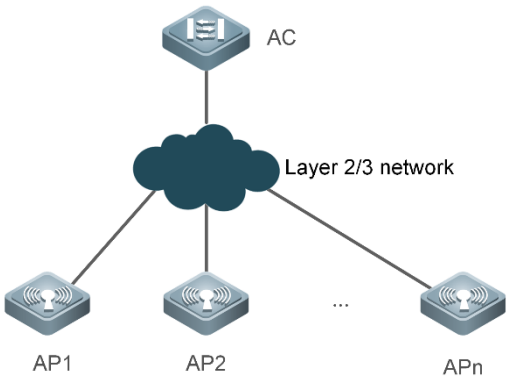
Scenario Figure 1-9	 In Figure 1-9, an AC is connected to APs. On the AC, configure the E-bag parameters for AP1 according to the following steps: 1. Set the A-MPDU software retransmission count to 3 for radio 1 of AP1. 2. Enable RTS protection for A-MPDU packets for radio 1 of AP1. 3. Set the single-time received Ethernet packet quantity to 100 for AP1. 4. Disable LDPC for radio 1 of AP1. 5. Disable transmit/receive STBC for radio 1 of AP1.
Configuration Steps	● On the AC, configure RF parameters for AP1.

	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# ampdu-retries 3 radio 1`
	`Hostname(config-ap)# ampdu-rts radio 1`
	`Hostname(config-ap)# eth-schd 100`
	`Hostname(config-ap)# no ldpc radio 1`
	`Hostname(config-ap)# no stbc radio 1`

Verification	● Run **show ap-config running** *ap-name* to display E-bag parameter settings of AP1.

	`Hostname(config)# show ap-config running AP1`
	`!`
	`ap-config AP1`
	` ap-mac 00d0.f801.0528`
	`channel 11 radio 1`
	` no 11acsupport enable radio 2`
	` ampdu-retries 3 radio 1`
	` ampdu-rts radio 1`
	` no stbc radio 1`
	` no ldpc radio 1`
	` eth-schd 100`
	` wmm edca-radio video aifsn 1 cwmin 3 cwmax 4 txop 90 radio 1`
	` wmm edca-radio back-ground aifsn 7 cwmin 4 cwmax 10 txop 5 radio 2`
	`!`

Configuring E-bag Network Optimization in One-Click Mode

Scenario **Figure 1-10**	 In Figure 1-10, an AC is connected to Fit APs. On the AC, configure E-bag network optimization for AP1 in one-click mode.
Configuration Steps	● On the AC, configure E-bag network optimization for AP1 in one-click mode.

	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# ebag`

Verification	● Run **show ap-config running** *ap-name* to display E-bag parameter settings of AP1.

```
Hostname(config)# show ap-config running AP1
!
ap-config AP1
 ap-mac 00d0.f801.0528


 channel 11 radio 1
 no 11acsupport enable radio 2
 ampdu-retries 2 radio 1
 ampdu-retries 2 radio 2
 eth-schd 25
 ebag
 wmm edca-radio video aifsn 1 cwmin 3 cwmax 4 txop 90 radio 1
 wmm edca-radio back-ground aifsn 7 cwmin 4 cwmax 10 txop 5 radio 2
!
```

1.4.8 Configuring WLANs in One-Click Mode

Configuration Effect

- Configure WLANs quickly on unconfigured devices in one-click mode. The one-click WLAN configuration feature helps the site survey personnel improve operation efficiency and the channel personnel execute performance tests conveniently.

Configuration Steps

↘ Configuring WLANs in One-Click Mode

- Optional.
- Run **autowifi** in configuration mode to configure WLANs in one-click mode, realizing fast configuration of wireless networks. The one-click WLAN configuration feature helps the site survey personnel improve operation efficiency and the channel personnel execute performance tests conveniently.

Command	**autowifi**
Parameter Description	N/A
Defaults	By default, the one-click WLAN configuration feature is not configured.
Command Mode	AC global configuration mode
Usage Guide	The one-click WLAN configuration feature allows you to perform fast configuration on unconfigured devices.

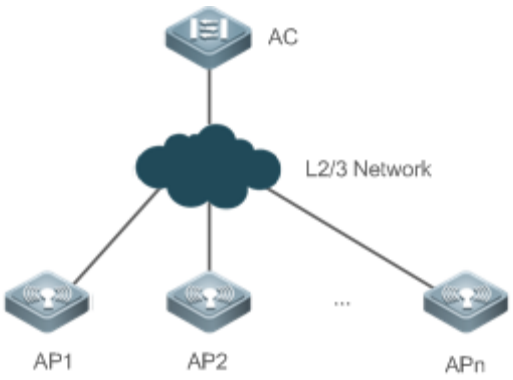
	The one-click WLAN configuration feature helps the site survey personnel improve the operation efficiency and the channel personnel execute performance tests conveniently.

Verification

- Run **show running-config** to display the one-click WLAN configuration.

Configuration Example

Configuring WLANs in One-Click Mode

Scenario **Figure 1-11**	 In Figure 1-11, an AC is connected to Fit APs. Configure WLANs in one-click mode on the AC.
Configuration Steps	● Configure WLANs in one-click mode on the AC.
	`Hostname# configure terminal` `Hostname(config)# autowifi`
Verification	● Run **show running-config** to display the one-click WLAN configuration.

	`Hostname(config)# show running-config`
	`!`
	`wlan-config 1 autowifi_1234`
	`!`
	`ap-group default`
	` interface-mapping 1 2 ap-wlan-id 1`
	`!`
	`ap-config all`
	` fair-schedule`
	`!`
	`ac-controller`

```
 802.11g network rate 1 mandatory
 802.11g network rate 2 mandatory
 802.11g network rate 5 mandatory
 802.11g network rate 6 supported
 802.11g network rate 9 supported
 802.11g network rate 11 mandatory
 802.11g network rate 12 supported
 802.11g network rate 18 supported
 802.11g network rate 24 supported
 802.11g network rate 36 supported
 802.11g network rate 48 supported
 802.11g network rate 54 supported
 802.11b network rate 1 mandatory
 802.11b network rate 2 mandatory
 802.11b network rate 5 mandatory
 802.11b network rate 11 mandatory
 802.11a network rate 6 mandatory
 802.11a network rate 9 supported
 802.11a network rate 12 mandatory
 802.11a network rate 18 supported
 802.11a network rate 24 mandatory
 802.11a network rate 36 supported
 802.11a network rate 48 supported
 802.11a network rate 54 supported
!
ip dhcp pool web_ap_pool_1
 option 138 ip 88.88.88.88
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool web_sta_pool_1
 network 192.168.2.0 255.255.255.0
 dns-server 8.8.8.8
 default-router 192.168.2.1
```

```
!
link-check disable
!
vlan 1
!
vlan 2
!
interface Loopback 0
 ip address 88.88.88.88 255.255.255.255
!
interface VLAN 1
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 2
 ip address 192.168.2.1 255.255.255.0
!
wlansec 1
 security rsn enable
 security rsn ciphers aes enable
 security rsn akm psk enable
 security rsn akm psk set-key ascii autowifi
!
```

1.4.9 Cancelling the Power Supply Limit

Configuration Effect

When the negotiated power supply limit is 15.4 W, configure this command to cancel the power supply limit.

Notes

- N/A

Configuration Steps

↘ Configuring poe-unlimit

- Optional.
- The AC delivers the configuration to the corresponding AP, instructing it to cancel the power supply limit.
- For APs powered through PoE+, if the PoE+ mode cannot be negotiated because some special power supply devices fail to work properly, the power supply limit can be canceled to ensure that the APs can work at the maximum capacity.

Command	**poe-unlimit radio** { *radio-id* | **802.11a** | **802.11b** | **6GHz** } **poe-unlimit radio-type** { **802.11a** | **802.11b** | **6GHz** }
Parameter Description	*radio-id*: Indicates the ID of a radio to be configured. The value range is from 1 to 96. **802.11a**: Indicates the 5 GHz operating band. **802.11b**: Indicates the 2.4 GHz operating band. **6GHz**: Indicates the 6 GHz operating band.
Defaults	By default, PoE is disabled and limited based on the PoE negotiation result.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

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

NOTE:

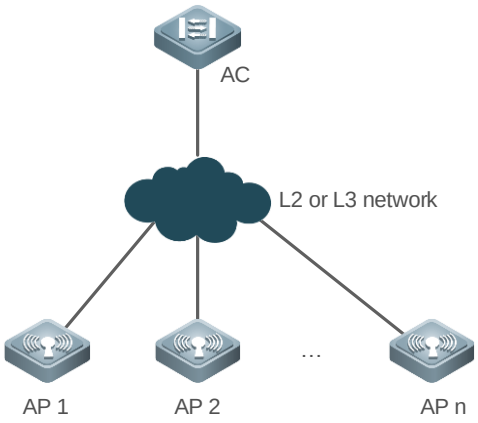
Ensure that the power supply device meets the maximum power consumption requirement of a corresponding AP. Otherwise, the AP may restart. Exercise caution when configuring this command.

Configuration Example

Configuring Power Supply Limit Cancelation

Scenario

Figure 1-2



Assume that in a Fit AP high-density environment, radio 1 of AP 1 on the AC must cancel the power supply limit.

Configuration Steps

On the AC, cancel the power supply limit on AP 1.

```
Hostname# configure terminal
Hostname(config)# ap-config AP1
Hostname(config-ap)# poe-unlimit radio 1
```

Verification

Run the **show ap-config running** *ap-name* command to display the power supply limit of a specified AP.

```
Hostname(config)# show ap-config running AP1
!
ap-config AP1
 ap-mac 00d0.f801.0528
 poe-unlimit radio 1
!
```

1.4.10 Managing the Operating Frequency Band When Power Supply Is Insufficient

Configuration Effect

When the AP power supply mode is negotiated to 15.4 W, the AP can work only in 2.4 GHz or 5 GHz. This configuration enables the AP to switch the operating frequency band to 2.4 GHz or 5 GHz.

Notes

- None

Configuration Steps

- Optional
- After this command is configured, the AC delivers the configuration to an AP to notify the AP of the operating frequency band in the case of insufficient power supply.

Command	**hap-poe enable radio** { **802.11a** | **802.11b** }
Parameter Description	**802.11a**: Indicates the 5 GHz band. **802.11b**: Indicates the 2.4 GHz band.
Defaults	By default, the operating frequency band is selected based on the AP capability value.
Command Mode	AP configuration mode, AP group configuration mode, or all-AP configuration mode
Usage Guide	N/A

Verification

Run the **show ap-config running** *ap-name* command to display configurations in AP configuration mode and run the **show running-config** command to display configurations in AP group configuration mode and all-AP configuration mode.

Configuration Example

Switching to 5 GHz When AP Power Supply Is Insufficient

Configuration Steps The following example switches the operating frequency band to 5 GHz on the AC when power supply to AP1 is insufficient.

```
Hostname# configure terminal
Hostname(config)# ap-config AP1
Hostname(config-ap)# hap-poe enable radio 802.11a
```

Verification Run the **show ap-config running** *ap-name* command to display the configuration of a specific AP.

```
Hostname(config)# show ap-config running AP1
!
ap-config AP1
 ap-mac 00d0.f801.0528
 hap-poe enable radio 802.11a
!
```

1.4.11 Enabling or Disabling the PoE Power Supply by an AP to External Devices

Configuration Effect

- Enable or disable the PoE power supply by an AP to external devices.

Notes

- N/A

Configuration Steps

Configuring poeout

- Optional.
- The AC can enable or disable the PoE power supply by the Fit AP to external devices by running the **exec-cmd** command.

Command	**poeout** { **enable** | **disable** | **default** }
Parameter Description	**enable**: Enables PoE power supply by an AP to external devices. **disable**: Disables PoE power supply by an AP to external devices. **default**: Uses the default settings for PoE power supply by an AP to external devices.
Defaults	By default, the default PoE power supply settings of the device are used.
Command Mode	AP configuration mode
Usage Guide	After the command is configured, the configuration is saved automatically, without using the write command. This command does not support the no and default forms. After poeout default is configured, the default PoE power supply configuration of the device is adopted. In Fit AP mode, the AC can enable or disable PoE power supply by an AP to external devices by running the exec-cmd command. The default PoE power supply status may vary depending on the AP model. Run the poeout default command to make APs of different models in the same group stay in their respective default PoE power supply status.

Verification

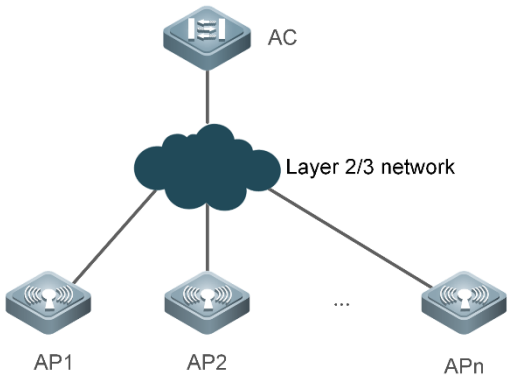
Run the **show ap–config running** command to display the configuration. insufficient

Configuration Example

Configuring PoEoutpot.

Scenario

Figure 1-3



Configuration Steps

Enable PoE power supply by an AP to external devices.

```
Hostname#configure
Hostname(config)# ap-config ap1
Hostname(config-ap)# exec-cmd mode config cmd "poeout enable"
```

Verification

Run the **show ap–config running** command to display the configuration.

```
Hostname#show ap-config running
!
ap-config ap1
 exec-cmd mode config cmd " poeout enable"
!
```

1.4.12 Configuring or Canceling Forced Power Supply Mode for an AP

Configuration Effect

- This command is used to configure or cancel the forced power supply mode (including four power supply levels: AF, AT25W, AT36W, and BT) of an AP and confirm whether to save the configuration to the environment variables.

Notes

- N/A

Configuration Steps

Configuring the Forced Power Supply Mode

- Optional.
- The AC can configure the forced power supply mode or cancel the configuration for a Fit AP on the AC by running the **exec-cmd** command.

- For APs powered via PoE+, if the PoE+ mode cannot be negotiated because some special power supply devices fail to work properly, the power supply limit can be canceled to ensure that the APs can work at the maximum capacity.

Command	**pdpoe-force** { **af** | **at25w** | **at36w** | **bt** } [**save**]
Parameter Description	**af**: Indicates that the power supply mode is forcibly configured as AF, with the level-1 power consumption of 13.0 W. **at25w**: Indicates that the power supply mode is forcibly configured as AT, with the level-2 power consumption of 25.5 W. **at36w**: Indicates that the power supply mode is forcibly configured as AT36, with the level-3 power consumption of 36.0 W. **bt**: Indicates that the power supply mode is forcibly configured as BT, with the level-4 power consumption of 62.0 W. **save**: Indicates that the configured forced power supply mode will be saved to the environment variables and will not be lost after a restart.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	The configuration of the command is saved only when save is specified in the command. The no form of this command can be used to cancel the configuration. You can run the no pdpoe-force command to cancel the forced power supply mode. You can run the no pdpoe-force save command to cancel the forced power supply mode and remove the environment variables. In Fit AP mode, the AC can be configured to cancel the forced power supply mode or cancel the configuration for an AP on the AC by running the exec-cmd command. The default forced power supply mode is not supported.

Verification

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

NOTE:

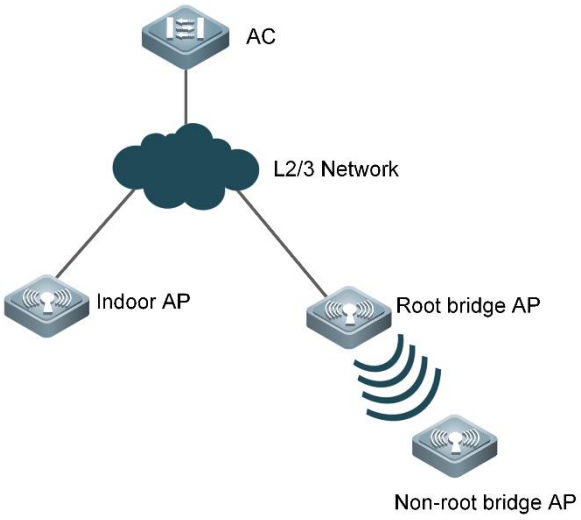
Ensure that the power supply device meets the maximum power consumption requirement of a corresponding AP. Otherwise, the AP may restart. Exercise caution when configuring this command.

Configuration Example

Configuring the Forced Power Supply Mode

Scenario

Figure 1-4



Configuration Steps

Assume that the AP680 is configured as a non-root bridge and powered by a non-standard BT adapter. If the third frequency of BT cannot be identified, a bridge fails to be established. That is, the AP cannot be connected to the AC. In this case, the AP needs to be pre-configured.

On the AC, forcibly configure the AP to the BT power supply mode.

Run the **exec-cmd** command to configure the AP.

```
Hostname(config)# ap-config ap1
Hostname(config-ap)#exec-cmd mode config cmd "pdpoe-force bt save"
```

Verification

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

```
Hostname#show ap-config running
!
ap-config ap1
 exec-cmd mode config cmd "pdpoe-force bt save"
!
```

1.4.13 Configuring a Frequency Band Mode

Configuration Effect

- Configure a frequency band mode of an AP, and specify the operating frequency (802.11a or 802.11b) of the radio during startup.

Notes

- This configuration is supported only by some APs (including the AP680).

Configuration Steps

Configuring a Frequency Band Mode

- Optional.
- The AC will deliver the configuration to the corresponding AP, instructing it to switch to the specified operating band and restart.

Command	**ap-band-mode** { **802.11a** | **802.11b** | **6GHz** } **radio** [*radio-id*]
Parameter Description	**802.11a**: Indicates the 5 GHz operating band. **802.11b**: Indicates the 2 GHz operating band. **6GHz**: Indicates the 6 GHz operating band. *radio-id*: Indicates the ID of a radio to be configured. The value range is from 1 to 96.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	1. This configuration is used to set the initial mode and cannot be saved. 2. This configuration will automatically restart the AP.

Verification

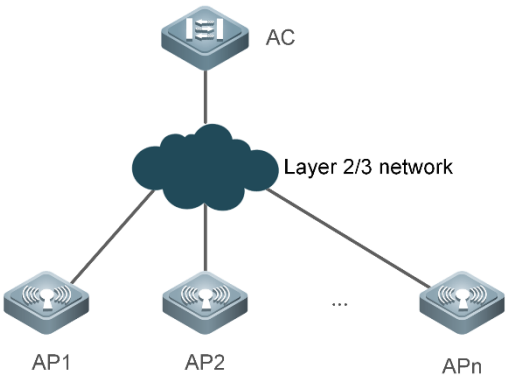
- The AP will automatically restart after this command is configured. Then run the **show ap-config summary** command to confirm the operating band of the corresponding radio.

Configuration Example

Configuring the Operating Frequency Band

Scenario

Figure 1-10



Configuration Steps

On the AC, configure the operating band for radio 3 of AP680 as 802.11a.

```
Hostname# configure terminal
Hostname(config)# ap-config ap680
Hostname(config-ap)# ap-band-mode 802.11a radio 3
Switch the band model will auto reload system, continue?(Y/N)  Y
```

Verification

After AP restart, run the **show ap-config summary** command to display the operating band of the corresponding radio.

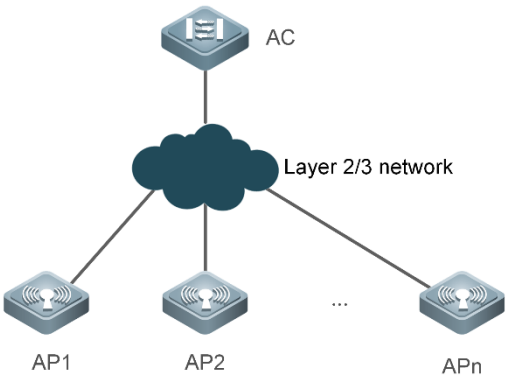
```
Hostname#show ap-config summary
========= show ap status =========
Radio: Radio ID or Band: 2.4G = 1#, 5G = 2#
      E = enabled, D = disabled, N = Not exist, V = Virtual AP
      Current Sta number
      Channel: * = Global
      Power Level = Percent

Online AP number: 2
Offline AP number: 29

AP Name                              IP Address     Mac Address    Radio
Radio            Up/Off time   State
---------------------------------------- --------------- -------------- --
----------------- ------------------- ------------- -----
```

Scenario

Figure 1-10



Configuration Steps

On the AC, configure the operating band for radio 3 of AP680 as 802.11a.

```
Hostname# configure terminal
Hostname(config)# ap-config ap680
Hostname(config-ap)# ap-band-mode 802.11a radio 3
Switch the band model will auto reload system, continue?(Y/N)  Y
```

Verification

After AP restart, run the **show ap-config summary** command to display the operating band of the corresponding radio.

```
ap680                                172.30.103.216  f822.5896.5858 1  E   0
6   100 2  E   0  153   100    0:00:00:32 Run
                                                                    3  E   0   40
100 4  N   -    -     -
```

1.5 Monitoring

Displaying

Command	Description
linktest	Displays link information about STAs.
show ac-config { **802.11a** | **802.11b** | **6GHz** } **summary**	Displays the AP list that maps the 802.11a, 802.11b, or 6 GHz network on an AC.
show antenna all	Displays the antenna feeder status of all APs.
show antenna single *ap-name*	Displays the antenna feeder status of an AP.
show ap-config radio	Displays radio information about all APs.
show ap-config radio ap-name *ap-name*	Displays radio information about an AP.
show ap-config radio *radio-id* **config** *ap-name*	Displays the configuration of an AP radio.
show ap-config radio *radio-id* **status** *ap-name*	Displays status information about an AP radio.
show ap-config radio status *ap-name*	Displays the radio list of an AP.

Command	Description
show ap-config summary radio	Displays radio information about all APs.
show client details *sta-mac*	Displays STA information mapped to a MAC address.
show dfs adjustment-channels [**ap-name**]	Displays the frequency-hopping channel and bandwidth of the specified AP or all APs.
show dfs non-occupancy-channels [**ap-name**]	Displays the list of non-occupancy radar channels of the specified AP or all APs.
show dfs historical-radar-channels [**ap-name**]	Displays historical information about radar channels of the specified AP or all APs.
show wopt dcca	Displays the DCCA configuration.
show wopt dtpc	Displays the DTPC configuration.

1 Configuring Band Select

1.1 Overview

Band Select optimizes access band distribution for stations (STAs) on a WLAN.

Band steering technology steers STAs to connect to higher-capacity frequency bands, enhancing user experience.

The Band Select function is suitable for the following scenario: multi-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
Band Select for a WLAN with a Fit AP Architecture	In a Fit AP architecture, a WLAN composed of multiple multi-band APs is enabled with the Band Select function.

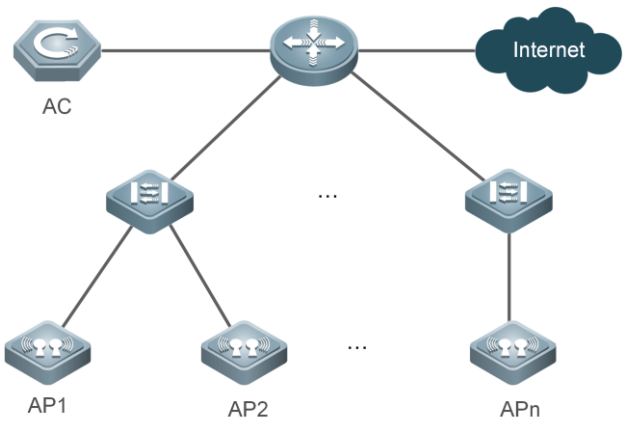
1.2.1 Band Select for a WLAN with a Fit AP Architecture

Scenario

In a Fit AP architecture, a WLAN composed of multiple multi-band APs is enabled with the Band Select function, as shown in Figure 4-1:

- One AC is associated with multiple multi-band APs. The AC and APs are connected through Layer 2 switches and Layer 3 routers.
- The WLAN is mapped to the multiple RF interfaces of all APs.

Figure 1-1



Remarks	The AC is a wireless access controller. AP1, AP2 … AP*n* are multi-band APs.

Deployment

- Manage parameters of the Band Select function on the AC.
- Apply the Band Select function, identify STA types, and steer STA access on the AC.

1.3 Features

Basic Concepts

Frequency Bands Used by IEEE802.11 for Communication

IEEE802.11 uses three frequency bands:

- 2.4 GHz (2412 MHz to 2472 MHz) (IEEE 802.11b/g/n/ax operates in this frequency band)
- 5 GHz (5180 MHz to 5320 MHz, 5500MHz to 5700MH, and 5445MHz~5825MHz) (IEEE 802.11a/n/ac/ax 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

STAs discover a WLAN through passive or proactive scanning:

- Passive scanning: A STA monitors beacon frames sent by neighboring APs on all channels of all supported bands. The beacon frames contain WLAN and auxiliary information. The STA parses the information to learn about the WLANs that are available nearby.
- Proactive 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 send a Probe Response frame containing WLAN information to the STA.

Typically, a STA summarizes the SSIDs of all discovered WLANs and generates a list of accessible WLANs 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 GHz.

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 a STA is a multi-band STA.
Controlling the Proactive Scanning Process	The Band Select function controls proactive scanning of a multi-band STA to prevent the STA from discovering WLANs of the 2.4 GHz band.
Preventing a Multi-band STA from Accessing the 2.4 GHz Band	The Band Select function rejects a multi-band STA from accessing the 2.4 GHz band and improves the chance of accessing the 5 GHz band.

1.3.1 Identifying STA Types

To steer a multi-band STA to access the 5 GHz or 6GHz band, it is necessary to first identify whether the STA is a multi-band STA; that is, identify the bands supported by the STA.

Working Principle

Proactive scanning is an approach for a STA to discover WLANs. A STA sends a Probe Request frame on each supported channel. If 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.

Because a single-band AP can receive the Probe Request frame only on one band, only a multi-band AP can correctly identify the STA type. This is why the multi-band AP is required for the Band Select function.

STA Classification Criteria

A multi-band AP classifies STAs based on the following criteria:

- 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 a STA only on the 6 GHz band, the AP learns that the STA is a 6 GHz STA.
- If the AP can receive the Probe Request frame from a STA only on the 5 GHz band, the AP learns that the STA is a 5 GHz STA.
- If the AP can receive the Probe Request frame from a STA only on the 2.4 GHz band, the AP learns that the AP is a 2.4 GHz STA.

Because an AP must wait for a period of time to verify that no Probe Request frame is received on a band, identifying a single-band STA is time-consuming. Among the five types of STAs, the first two types are called multi-band STAs in the Band Select function and the last three types are called the inhibition 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

STA information identified by a multi-band AP must be saved for enforcing subsequent responding policies.

Because Probe Request frames sent by STAs are broadcast, an AP may receive many Probe Request frames. It is unnecessary to save all the frames because some distant STAs may not access the AP. The Band Select function saves only the information of neighboring STAs based on the Received Signal Strength Indication (RSSI) of STAs. Only STAs with the RSSI exceeding a threshold can access the AP, and their information needs to be saved.

STA Information Aging

Frequency bands supported by some STAs are configurable. When a STA accesses the network, the frequency bands supported by the STA may change.

An 802.11a/g/n-compliant WNIC is used as an example. The WNIC works as a multi-band STA initially. However, the 802.11a mode or the support for the 5 GHz channels is disabled manually. In this case, the WNIC changes to a single-band 2.4 GHz STA.

An aging mechanism is introduced for the identified STA. After a period of time, the previously identified STA information is discarded.

1.3.2 Controlling the Proactive Scanning Process

After identifying the bands supported by a STA, a multi-band AP can control the proactive scanning process of the STA based on the STA information. The prevents a multi-band STA from discovering 2.4 GHz WLANs and steers the multi-band STA to access the optimal band.

Working Principle

During proactive 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 proactive 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 proactive scanning and adopts different response approaches as needed.

Proactive Scanning Before the Band Select Function Identifies STA Types

If the Band Select function is enabled for a WLAN, the WLAN may have a change for the response to proactive scanning of a STA. Before STA types are identified, the following situations occur:

- 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 on 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, the STA supports the 5 GHz and 6 GHz band. In this case, the AP sends a Probe Response frame immediately to notify the STA that the WLAN provides access service on the 5 GHz and 6 GHz band.

Proactive 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 has a passive response.
- The AP responds to a 5 GHz and 6 GHz Probe Request.

Disabling the response 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 on the 2.4 GHz band. In this way, the multi-band STA only discovers that the WLAN provides access service on the 5 GHz and 6 GHz band. The multi-band STA needs to connect to the 5 GHz and 6 GHz band for access.

The AP must respond to the 2.4 GHz Probe Request from an inhibition STA. Because 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 passive.

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 instruct the WLAN to provide access service on the 5 GHz and 6 GHz band.

Passive Response to an Inhibition STA

The Band Select function always proactively 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 passively. For example, when receiving multiple Probe Requests consecutively, the AP sends only one Probe Response.

The passive response depends on two parameters: STA scanning cycle threshold and probe count of the inhibition STA.

- STA scanning cycle threshold

The STA scanning cycle refers to the time for scanning all supported channels during proactive scanning of a STA. The time depends on characteristics of STAs. The STA scanning cycle can be configured and is the minimum value for limiting STA scanning. If the scanning cycle of a STA is smaller than this value, two consecutive scanning cycles may be considered to be one by an AP. This parameter is valid when some STAs send multiple Probe Requests within one scanning cycle.

Assume that a 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. Because 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.

- Probe count of an inhibition STA

The probe count of an inhibition STA reflects the passive response degree of an RF interface to the STA. This parameter indicates the number of the cycles for which an inhibition STA performs proactive 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 Preventing a Multi-band STA from Accessing the 2.4 GHz Band

The Band Select function controls only the proactive scanning process of a 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 take ineffective.

The Band Select function can reject 2.4 GHz access requests from multi-band STAs to improve the probability of multi-band STAs accessing the 5 GHz and 6 GHz band.

Rejecting a multi-band STA's 2.4 GHz access request helps improve the chance of successfully applying the Band Select function. However, the Band Select function may be unavailable.

Working Principle

After a STA discovers a WLAN, the STA sends an Authentication Request to the AP. 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 from the 2.4 GHz band, the Authentication Request will be rejected until the multi-band STA sends an Authentication Request from the 5 GHz or 6 GHz band. In this case, the STA is steered to access the 5 GHz or 6 GHz band.

When a multi-band STA searches for WLANs, the STA sends one or more Authentication Requests from one band and waits for responses. If the STA does not receive responses, the STA sends Authentication Requests from the other band and waits for responses. However, some multi-band STAs send Authentication Requests only from the 2.4 GHz. To achieve high availability, you can use the Band Select function to set the count for rejecting a multi-band STA.

Assuming that a multi-band STA sends Authentication Requests for *M* times before band change, and the count for rejecting a multi-band STA 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. Regardless of the band a multi-band STA accesses, if the multi-band STA attempts to access the 2.4 GHz band at first, *M* or *N* (whichever is smaller) Authentication Requests are rejected or ignored. As a result, the STA's access is delayed. The delay depends on characteristics 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 function such as load balancing accepts the access request, the STA will still gain access. This is because the Band Select function is only used to steer STA access and has a lower priority. When the Band Select function conflicts with other functions, the other function takes effect.

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 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 count for rejecting 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 a STA.

1.4.1 Configuring Band Select

Configuration Effect

- Enable the Band Select function for a WLAN to steer 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.
- Unless otherwise specified, enable this function on an AC.

Command	**band-select enable**
Parameter Description	N/A
Defaults	By default, the Band Select function is disabled.
Command Mode	WLAN configuration 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.
- Unless otherwise specified, enable this function on an AC.
- A higher value indicates a smaller coverage of the Band Select function. However, if the value exceeds a threshold, the STA that gains access may have weak signals, causing the entire network to slow down.

Command	**band-select acceptable-rssi** *value*
Parameter Description	*value*: Specifies the minimum SSID for the Band Select function. The value range is from -100 to -50 dBm.
Defaults	The default value is -80 dBm
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Count for Rejecting 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 from multi-band STAs. If many STAs fail to access a band or it takes a long time to access the band, set a smaller value or use the value of 0.
- Unless otherwise specified, enable this function on an AC.
- A larger value indicates more difficult for the multi-band STA to access the 2.4 GHz band or longer time taken for the STA to access the 2.4 GHz band.

Command	**band-select access-denial** *value*
Parameter Description	*value*: Specifies the count for rejecting a multi-band STA's 2.4 GHz access requests. The value range is 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 the situation is uncertain, use the default value.
- Unless otherwise specified, enable this function on an AC.
- A longer aging time indicates a longer lifecycle of STA information, and the less sensitivity 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. The value range is from 20 to 120 seconds. **suppression** *value*: Specifies the aging time of inhibition STA information. The value range is from 10 to 60 seconds.
Defaults	By default, 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 thrice 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, use a smaller value.
- Unless otherwise specified, enable this function on an AC.
- The greater the probe count of a STA, the stronger inhibition the Band Select function performs on an inhibition STA, and the more difficult the inhibition STA discovers a WLAN.

Command	**band-select probe-count** *value*
Parameter Description	*value*: Specifies the probe count of an inhibition STA. The value range is 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 a STA

- Optional.
- If a single-band 2.4 GHz STA cannot discover a WLAN for a long time, use a smaller value. If the situation is uncertain, use the default value.
- Unless otherwise specified, enable this function on an AC or a fat AP.
- The greater the scanning cycle threshold of a STA, the more slowly the probe count of the STA increases, and the more difficult the STA discovers a WLAN

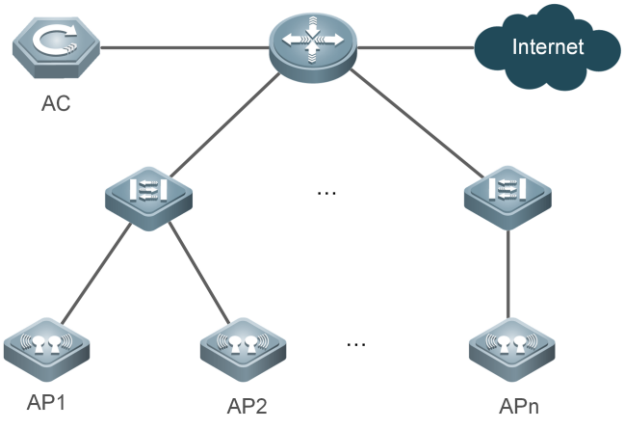
Command	**band-select scan-cycle** *value*
Parameter Description	*value*: Specifies the scanning cycle threshold of a STA. The value range is from 1 to 1000 milliseconds.
Defaults	The default value is 200 milliseconds.
Command Mode	Global configuration mode
Usage Guide	N/A

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 time, run the **show band-select statistics** command to check the statistics on the AC.
- Check whether the Band Select function controls the proactive scanning process by obtaining packets.

Configuration Example

Configuring Band Select for a WLAN with a Fit AP Architecture

Scenario **Figure 1-2**	 Figure 1-2 shows a typical WLAN with a Fit AP architecture. ● The AC is a wireless access controller. ● AP_1, AP_2 … AP_n are multi-band APs. ● The AC and APs are connected through Layer 2 switches and Layer 3 routers. ● The Band Select function is enabled on WLAN 99, whose SSID is **wlan-band select**. This WLAN is mapped to the two RF interfaces of all multi-band APs.
Configuration Steps	● (Optional) Configure parameters of the Band Select function on the AC. ● Enable the Band Select Function for WLAN 99 on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# wlan-config 99`
	`Hostname(config-wlan)# band-select enable`

Verification	Connect a multi-band STA to the WLAN with the SSID **wlan-band select**. ● The STA accesses the 5 GHz band. (The STA may also access the 2.4 GHz band upon band selection failure.) ● Check statistics of the Band Select function on the AC. The count should increase.

AC	`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

- Parameters of the Band Select function are improper.
- The Band Select function is not enabled.

- One of the multiple RF interfaces of a multi-band AP is disabled.

1.5 Monitoring

Displaying

Command	Description
show band-select configuration	Displays the configuration of the Band Select function.
show band-select statistics	Displays statistics of the Band Select function.

1 Configuring HE Radio Selection

1.1 Overview

The high-efficiency (HE) radio selection technology selects an HE radio frequency (RF) interface on an access point (AP) based on the channel load and other conditions when multiple types of stations (STAs) coexist. This enables high-performance STAs (HIGH STAs) to preferentially access the HE RF interface 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 Fit AP Architecture	In the Fit AP architecture with densely deployed tri-radio APs, Wi-Fi 4, Wi-Fi 5, and Wi-Fi 6 STAs are randomly distributed across radios. Low-speed STAs affect the user experience of Wi-Fi 6. The HE radio selection function steers HIGH STAs to HE radios.

1.2.1 Configuring HE Radio Selection in the Fit AP Architecture

Scenario

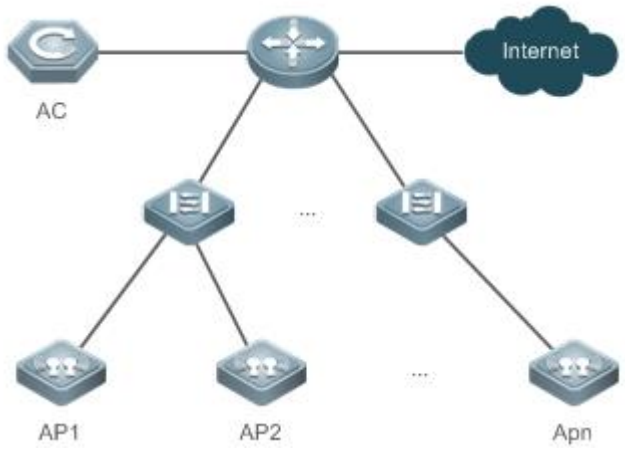
On a wireless local area network (WLAN) formed by multiple tri-radio APs in the Fit AP architecture, a large number of Wi-Fi 4, Wi-Fi 5, and Wi-Fi 6 STAs exist and these STAs may connect to APs randomly. When low-speed STAs are used with Wi-Fi 6 STAs, Wi-Fi 6 STAs cannot unleash high throughput. With the HE radio selection function enabled, HE STAs can be steered to HE radios.

The HE radio selection technology dynamically assigns HIGH STAs to the most suitable RF when both high-speed and low-speed STAs exist. If there are only low-speed or high-speed STAs, you are not advised to enable this function.

In Figure 1-1:

- One access controller (AC) is associated with multiple tri-radio APs, and the AC connects to APs using Layer 2 switches and Layer 3 routers.
- WLAN signals are mapped to the three RF interfaces of all tri-radio APs.

Figure 1-1



Note	The AC is the wireless network controller. AP1, AP2, …AP*n* are tri-radio APs.

Deployment

- Manage and configure working parameters of the HE radio selection function on the AC.
- Run the HE radio selection function on APs. Based on the RF environment of an AP, the HE radio selection function automatically selects an HE radio, identifies HIGH STAs, and steers the HIGH STAs to the HE radio.

1.3 Features

Basic Concepts

Frequency Bands Used by IEEE802.11 for Communication

IEEE802.11 uses two frequency bands:

- 2.4 GHz (2.4 GHz to 2.4835 GHz), where 802.11b/g/n operates
- 5 GHz (5.15 GHz to 5.35 GHz and 5.725 GHz to 5.825 GHz), where 802.11a/n operates

As WLANs become popular, more and more wireless users increase on WLANs. Many users use dual-band wireless clients (STAs) supporting both 2.4 GHz and 5 GHz. However, 802.11b or 802.11g is more widely applied than 802.11a. Many dual-band STAs use 2.4 GHz, causing congestion on the 2.4 GHz band and underutilization of the 5 GHz band. However, the 5 GHz band has a higher access capacity. The 2.4 GHz band has up to three non-overlapping channels, whereas the 5 GHz band provides more non-overlapping channels.

STA Scanning

STAs discover a WLAN through passive or proactive scanning:

- Passive scanning: A STA monitors beacon frames sent by neighboring APs on all channels of all supported bands. The beacon frames contain WLAN and auxiliary information. The STA parses the information to learn about the WLANs that are available nearby.

- Proactive 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 send a Probe Response frame containing WLAN information to the STA.

Typically, a STA summarizes the SSIDs of all discovered WLANs and generates a list of accessible WLANs for users.

HIGH STA

As Wi-Fi 6 is introduced and tri-radio APs become popular, if wireless STAs are randomly associated with an AP's radio, the user experience of HIGH STAs that support 802.11ac/802.11ax is easily affected when they access 2.4 GHz radio, or when 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 steer these STAs to HE RF interfaces.

Dual-5G AP

Dual-5G APs can access two 5 GHz frequency bands simultaneously and tri-radio APs need to support dual-5G coverage. Signals of a WLAN enabled with HE radio selection must be mapped to the three RF interfaces of all tri-radio APs, and all the three RF interfaces provide access service to STAs.

Overview

Feature	Description
Identifying the STA Type	Identifies whether a STA is a HIGH STA. (STAs that support 802.11ax are identified as HIGH STAs by default, which is configurable.)
Automatically Selecting an HE Radio	Automatically selects an HE radio based on the RF load and interference of an AP.
Controlling the Proactive Scanning Process	Controls proactive 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 access non-HE radios. Identifies the type of STAs and rejects non-HIGH STAs to access 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 a STA is a HIGH STA, that is, check whether a STA supports HT_CAP.

Working Principle

Proactive scanning is a method for a STA to discover a WLAN. When a STA uses proactive scanning, it sends a probe request frame to each supported channel. If HT/VHT/HE information can be identified based on the 802.11 field carried in the probe request frame sent by the STA, protocols supported by the STA can be identified.

STA Classification Criteria

An AP classifies STAs based on the following criteria:

- 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 a STA accesses an AP, the AP parses the Probe Request and Assoc Request packets to confirm 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 probe request and assoc request packets. However, in the authentication phase, the packets cannot be parsed.

STA Information Saving

STA information identified by a dual-band AP must be saved for enforcing subsequent responding policies.

Because Probe Request frames sent by STAs are broadcast, an AP may receive many Probe Request frames. It is unnecessary to save all the frames because some distant STAs may not access the AP. The Band Select function saves only the information of neighboring STAs based on the Received Signal Strength Indication (RSSI) of STAs. Only STAs with the RSSI exceeding a threshold can access the AP, and their information needs to be saved.

STA Information Aging

Frequency bands supported by some STAs are configurable. When a STA accesses the network, the frequency bands supported by the STA may change. 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 802.11ac/ax mode is disabled manually, the NIC is changed to a non-HIGH-STA that supports 802.11n.

In this case, 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 an HE Radio

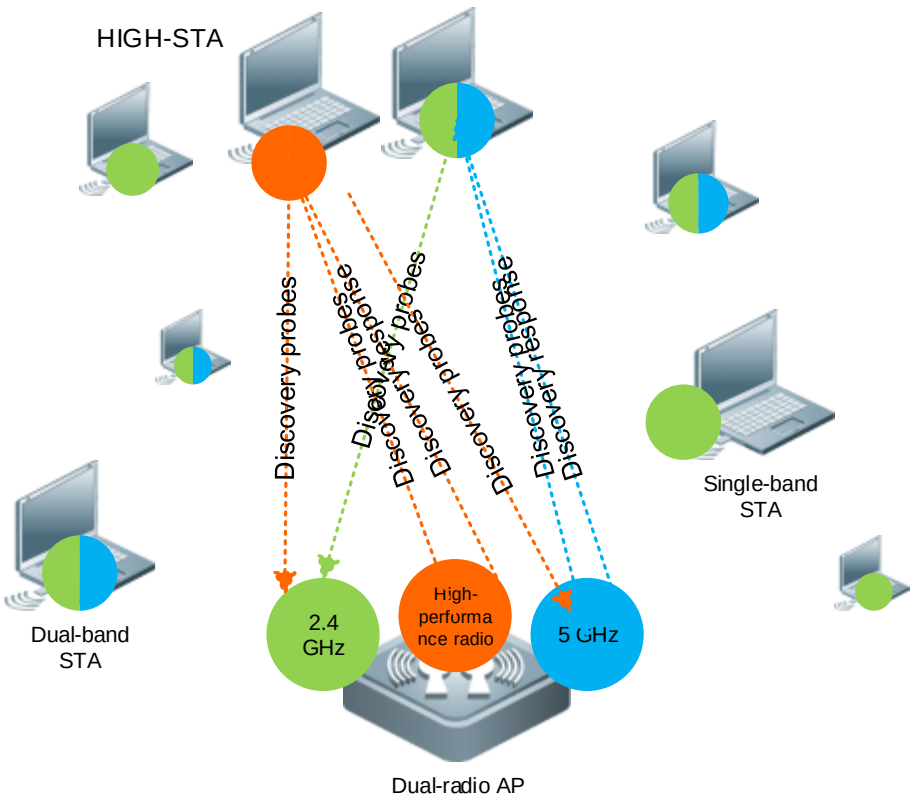
The HE radio selection function requires an AP to support dual-band 5G and use an HE radio with small interference. After the HE radio selection function is enabled, the AP can automatically select a radio with a light load and low interference based on the channel environment to ensure user experience of HIGH STAs.

1.3.3 Controlling the Proactive Scanning Process

After identifying capabilities supported by a STA, a tri-radio AP can control proactive scanning of the STA. This prevents HIGH STAs from discovering signals of non-HE radios and steers 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 proactive scanning, a STA broadcasts a probe request frame. After an AP receives the frame, it responds with a probe response frame and notifies the STA of signals on the AP that can provide the access service. During proactive scanning, a 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 proactive scanning and adopts different response methods in different scenarios.



Response of HE Radio Selection to Proactive Scanning of STAs

If HE radio selection is enabled on an AP, response to proactive scanning of a STA will be changed. After identifying STA capability information:

✓ HE radios

- The AP does not respond to probe requests from non-HIGH-STAs but responds 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.

Passive Response of HE Radio Selection to Non-HIGH-STAs

HE RF interfaces proactively respond to probe requests from HIGH-STAs and do not respond to probe requests from non-HIGH-STAs. Non-HE RF interfaces passively respond to probe requests from HIGH STAs. That is, non-HE RF interfaces only respond with one probe response after receiving multiple consecutive probe requests.

The passive response degree of HE radio selection to probe requests from STAs depends on two parameters: STA scan cycle threshold and STA probe scan cycle count.

- STA scan cycle threshold
- The STA scan cycle indicates the time for scanning all supported channels during STA proactive scanning, and the time varies with the STA. The STA scan cycle threshold is a configurable value and indicates the minimum value for the STA scan cycle. If the STA scan cycle is less than the value, the AP regards two consecutive scan cycles as one . A STA may send multiple probe request frames in one scan cycle.

For example, a STA scans all channels every 150 ms and sends two consecutive probe request frames on each channel. If the minimum value of the STA scan cycle is not specified on the AP, the AP cannot determine whether a STA sends two probe request frames in one scan cycle or one probe request frame in two consecutive scan cycles. If the minimum value of the STA scan cycle 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 scan cycle and the scan cycle count of the STA on the AP is 1. Because the minimum value of the STA scan cycle specified on the AP is 200 ms, which is different from the actual scan cycle of 150 ms, inconsistent counts may exist. When a STA has three scan cycles, only two cycles are counted on the AP because the AP regards the previous two cycles as one.

- STA scan cycle count

  The STA scan cycle count reflects the passive response degree of an HE RF interface to a STA. The count indicates the number of STA proactive scan cycles that an AP sends a response. For example, the default count is 2. That is, the AP sends a probe response frame after two consecutive scan cycles of a STA.

1.3.4 Rejecting STAs

⚠ The HE radio selection function only controls the proactive scanning process of a 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.

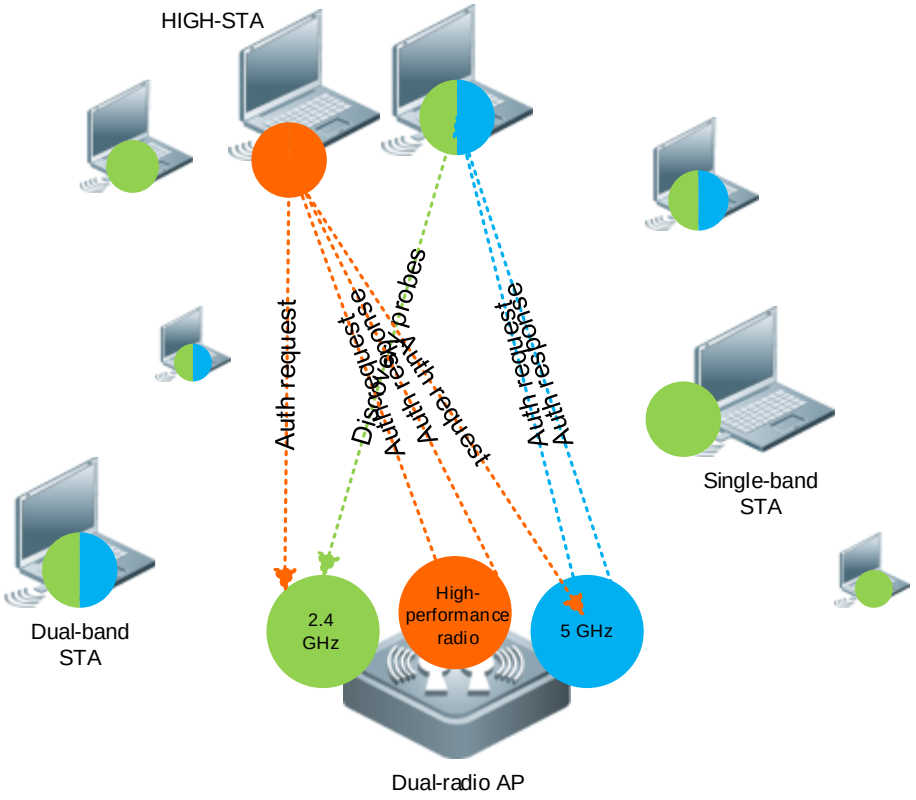
⚠ Rejecting access requests from HIGH STAs in non-HE radios can improve the success rate of HE radio selection, but there is a possibility that HE radio selection becomes unavailable.

Working Principle

After a 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 an HE radio, the HE radio can reject its authentication request until it receives an authentication request from a HIGH STA. This steers tri-radio STAs to access HE radios.

When a HIGH STA accesses the network, it sends one or more authentication requests from one 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, configure the number of times for rejecting access requests from non-HIGH-STAs.



For example, a HIGH STA accesses the WLAN 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 an 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) If *N* is smaller than to *M*, the STA accesses a non-HE radio.

  In this scenario, M or N authentication requests (whichever is smaller) will be rejected or ignored. Therefore, it takes a long time for some STAs to access the WLAN. The delayed varies with the STA. For example, if a STA sends authentication requests every 100 ms and four authentication requests are ignored, the 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 feature, 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 steer STAs during STA access and has a low priority. When this function conflicts with other functions, other functions are preferred.

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. For example, 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 congested 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 associations on HE radios and non-HE radios. Based on STA access and channel load of radios, the AP adjusts the selection policy to ensure effectiveness of this function.

1.4 Configuration

Configuration	Description and Command	
Configuring HE Radio Selection	(Mandatory) It is used to enable the HE radio selection function for an AC.	
	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 working parameters of the HE radio selection function.	
	band-select acceptable-rssi	Configures the lower limit of the STA RSSI 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 scan cycle count.
	(Optional) It is used to configure working parameters of the HE radio selection function.	
	show ac-config client radio he-status	Displays STA access distribution of a radio.

1.4.1 Configuring HE Radio Selection

Configuration Effect

- Enable the HE radio selection function on an AP and steer HIGH STAs to HE radios.

Notes

N/A

Configuration Steps

Enabling HE Radio Selection for an AP

- Mandatory.
- Configure it on the AC 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	AC: AP configuration mode or AP group configuration mode (the AP configuration mode has a higher priority than AP group configuration mode)
Usage Guide	N/A

Configuring the Usage Mode of HE Radio Selection

- Optional. Configure it when HE radio selection needs to be adjusted.
- Configure it on the AC 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 STA load of a radio. **fixed**: Forcibly steer 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 on the AC unless otherwise specified.
-

Command	band-optimize he-radio mode { 11axonly | 11ac_11ax }
Parameter Description	**11axonly**: Steers only 802.11ax STAs to HE radios. **11ac_11ax**: Steers only 802.11ac and 802.11ax STAs to HE radios.
Defaults	The default mode is **11axonly**.
Command Mode	AC + Fit AP: AP configuration mode or AP group configuration mode (the AP configuration mode has a higher priority than the AP group configuration mode)
Usage Guide	N/A

Configuring the Number of Times That HE Radio Selection Rejects a STA

- Optional. Configure the number of times that an 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 a 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 on the AC unless otherwise specified.

- The larger the number of times that a radio rejects a STA, the more difficult and more time it takes for the STA to access the radio.

Command	**band-select he-radio access-denial** *access-denial-time*
Parameter Description	*access-denial-time*: Indicates the number of times for rejecting a STA. The value range is 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 a STA

- Optional. Configure the number of times that an 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 on the AC unless otherwise specified.
- A longer STA information aging time indicates a longer STA information lifecycle and less sensitive to radio switching of a STA. A shorter STA information aging time indicates a shorter STA information lifecycle and more sensitive to radio switching of a STA.

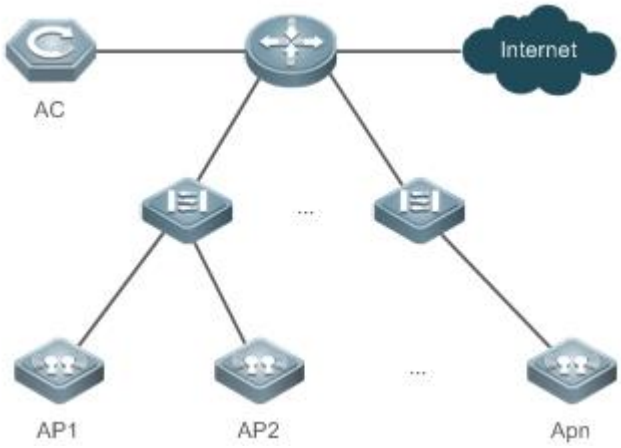
Command	**band-select he-radio probe-count** *probe-count*
Parameter Description	*probe-count*: Indicates the number of times that a non-HE radio rejects probe requests from a HIGH STA. The value range is from 0 to 10.
Defaults	2
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show band-select configuration** command to display HE radio selection parameter configuration on the AC.
- Run the **show running-config** command to check whether the HE radio selection function is enabled in WLAN configuration mode.
- After a period of time, run the **show band-select statistics** command to display running statistics on the AC.
- Obtain packets to confirm whether HE radio selection controls the proactive scanning process.
- After the STA accesses the network, run the **show ac-config client radio he-status** command to display STA access distribution on radios of the AC.

Configuration Example

Configuring HE Radio Selection in the Fit AP Architecture

Scenario **Figure 1-2**	 The preceding figure shows a typical wireless network with the fit AP architecture. ● AC is the wireless network controller. ● AP1, AP2. …AP*n* are tri-radio APs. ● The AC connects to the APs through a Layer 2 switch and Layer 3 router. ● The HE radio selection function is enabled, the WLAN is WLAN 99, the SSID is **wlan-bandoptimize**, and the WLAN maps to three RF interfaces of all tri-radio APs.
Configuration Steps	● Configure parameters for the HE radio selection function on the AC (optional). ● Enable HE radio selection for WLAN 99 on the AC.

AC	`AC# configure terminal`
	`AC(config)# ap-group 11axap_bandoptimize`
	`AC(config-group)# band-optimize he-radio enable`

Verification	Connect a HIGH STA to WLAN **wlan-bandselect**. ● The STA accesses an HE radio. (The HE radio selection may take ineffective, and the STA accesses a non-HE radio.) ● Check that the HE radio selection running statistics on the AC increase.

AC	`A# 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 parameters are not configured properly.
- The HE radio selection function is disabled.
- One of the two 5G RF interfaces of a tri-radio AP is disabled.

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show band-select statistics	Displays HE radio selection running statistics.
show ac-config client radio he-status	Displays STA distribution to radios of an AP connected to the AC to display STA distribution of HE radios.

Debugging

N/A

1 Configuring Radio Scheduling

1.1 Overview

Radio resources mentioned in this document include radios of an Access Point (AP) as well as the wireless local area network (WLAN) that provides access services.

Radio scheduling can perform automatic management of radio resources.

Radio scheduling can be used to disable the radio of an AP or a WLAN at the specified interval to realize the following functions:

- Reduce network traffic, saving network resources and preventing waste or abuse of network resources.
- Reduce radio interference and save energy.
- Disable access services in a certain period to reduce potential security risks.

Radio scheduling can be used in the scenarios where wireless access services are required in fixed time cycles.

1.2 Applications

Application	Description
AP RF Scheduling	In a Fit AP architecture, enables and disables AP RF as scheduled.
WLAN Scheduling	In a Fit AP architecture, enables and disables a WLAN as scheduled.

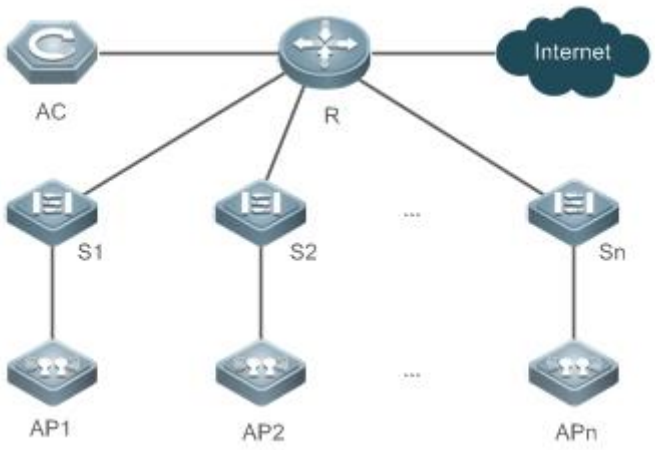
1.2.1 AP RF Scheduling

Scenario

In the scenario where access services need to be provided to stations (STAs) in a specific period, AP radio scheduling can be used to disable radios in the period when no STAs access the WLAN, thereby preserving network resources and saving energy.

The following figure shows the deployment of a WLAN in a teaching building of a university, with the Fit AP architecture. AP1, AP2,…, and AP*n* are located in different places of the building. In the daytime, wireless services need to be provided to students and teachers, but such services are disabled in the nighttime. By using AP radio scheduling, radios of the entire building will be disabled automatically in the nighttime, and enabled again in the daytime. In this way, wireless services are available as scheduled, saving network resources and energy.

Figure 1-1



Deployment

In a Fit AP architecture, you can configure AP radio scheduling on an AC.

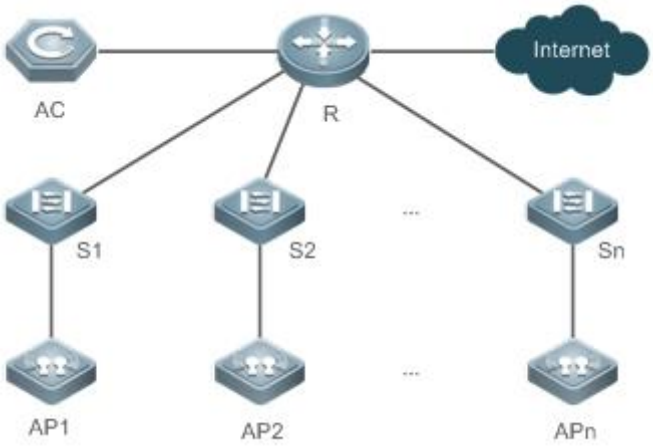
1.2.2 WLAN Scheduling

Scenario

Some specified WLANs should be enabled with radio scheduling as needed to reduce radio interference and ensure security.

The following figure shows the WLAN deployment of a bank business hall. The Fit AP architecture is used. AP1, AP2,…, and AP*n* are located in different places of the hall to provide free wireless access to customers. Typically, this WLAN does not require a password and is available only during business hours. When WLAN scheduling is applied, the WLAN is automatically enabled during business hours and disabled after work. In this way, the free customer-use WLAN is disabled, while other WLANs can continue to serve bank employees who are still working in the office.

Figure 1-2



Deployment

In a Fit AP architecture, configure WLAN scheduling on an AC.

1.3 Features

Basic Concepts

Scheduling Session

A scheduling session indicates a time interval for a radio resource. A simple scheduling session contains only one interval in a certain day, while a complex scheduling session contains many duplicate intervals in different days. One scheduling session supports eight identical or different 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 an AP	Applies a scheduling session to an AP radio to enable or disable the AP radio periodically.
Scheduling WLAN	Applies a scheduling session to a WLAN to enable or disable the WLAN periodically.

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 interface 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 a 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-work 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 an AP Radio

Enable or disable the AP radio periodically.

Working Principle

Before using the scheduling function, create a scheduling session and specify the time for radio scheduling. Then you can apply the scheduling session to an AP RF interface.

When the scheduling session starts or ends, the system sends a scheduling message. The RF interface of an AP or the RF interfaces of an AP group where this scheduling session is applied is enabled or disabled.

Applying a Scheduling Session to an RF Interface

After a scheduling session is created, it must be applied to the corresponding AP RF interface so that the scheduling can take effect.

You can specify an AP RF interface in the following several ways:

- Based on all APs
- Based on an AP group
- Based on a single AP

In the preceding several approaches, you can specify a radio ID for scheduling. If a radio ID is not specified, the scheduling will be applied to all radios of the AP.

In the example of the teaching building, the AP radio needs to be specified as needed.

If all APs in this scenario are in the same group or distributed in a few groups, the AP group-based configuration is recommended. If all the APs are located in the teaching building, the configuration based on all APs is also recommended. As the last choice, you can specify the AP RF interface based on a single AP.

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: scheduling state, including entering and exiting from the scheduling session

The handling of a scheduling message covers all APs. The system will determine whether to start scheduling based on the scheduling session ID configured for a single AP, AP group, and all APs in descending order of priority.

Scheduling priority: The priority of a session ID configured for a single AP, AP group, and all APs is in descending order. That is, when a session ID is configured for an AP, the AP group-based session ID and all APs-based session ID will not take effect on this AP. If no session ID is configured for an AP, the AP group-based session ID will take effect. If no AP group-based session ID is configured for an AP, the all APs-based session ID will take effect.

If the effective scheduling session ID of this AP radio is the same as that in the message, the message type will be checked. In scheduling state, the radio of this 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, create a scheduling session and 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. The WLAN where this scheduling session is applied to is enabled or disabled.

Applying a Scheduling Session on an RF Interface

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 the WLAN is in scheduling state, the WLAN will be disabled. Otherwise, the WLAN 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 interval, and apply the scheduling session to an AP or AP group.	
	schedule session	Creates a scheduling session.
	schedule session time-range	Specifies the 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 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 radio scheduling.

Configuration Steps

Creating a Scheduling Session

- Mandatory.
- A scheduling session must have been created.
- The command must be run on the AC where scheduling needs to be enabled.

Command	**schedule session** *session-id*
Parameter Description	*session-id*: Indicates the session ID. The value range is from 1 to 64 on an AC.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Interval for a Scheduling Session

- Mandatory.
- The function must be applied on the AC to enable scheduling.

Command	**schedule session** *session-id* **time-range** *time-range-num* **period** { *day1* [**to** *day2*] | **everyday** } **time** { *hh1:mm1* **to** *hh2:mm2* | **all-day** }
Parameter Description	*session-id*: Indicates the session ID. The value range is from 1 to 64 on an AC. *time-range-num*: Indicates the number of an interval. The value range is from 1 to 8. *day1*: Indicates the start date of the scheduling session cycle, which can be set to { sun | mon | tue | wed | thu | fri | sat }. **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, no scheduling interval or cycle is configured.

Command Mode	Global configuration mode
Usage Guide	N/A

Applying a Scheduling Session

- Mandatory.
- The function must be applied on the AC where scheduling needs to be enabled.
- In AP configuration mode, run the **schedule session** *session-id* command to specify the session ID for APs or a single AP.
- In AP group configuration mode, run the **schedule session** *session-id* command to specify the session ID for an AP group.
- After a scheduling session is applied, if the message for the scheduling session is displayed, the specified AP RF interface will automatically enter or exit from the scheduling state as specified by the massage type.

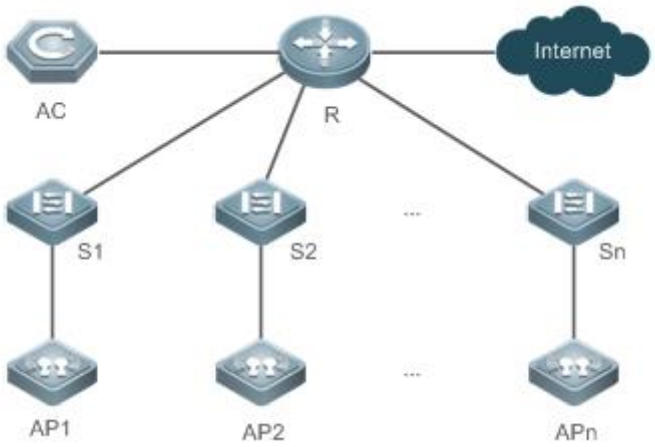
Command	**schedule session** *session-id* [**radio** *radio-id* | **slot** { *slot-id* | **all** }]
Parameter Description	*session-id*: Indicates the session ID. The value range is from 1 to 64 on an AC. *radio-id*: Indicates the ID of a radio on which the session is to be applied or deleted. The value range is from 1 to the number of radios on the AP. By default, the value is set to the number of radios on an AP. *slot-id*: Indicates ID of a slot on which the scheduling session is to be applied or deleted. The value range is from 1 to 24. **all**: Indicates all radios or all slots.
Defaults	By default, no scheduling session is applied to a single AP, an AP group, or all APs.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	N/A

Verification

- Run **show schedule session** to display the RF scheduling configuration.
- Check whether scheduling is still performed for an AP radio after a scheduling session expires.

Configuration Example

Providing WLAN Services to a Teaching Building of a University Only in the Daytime

Scenario **Figure 1-3**	 As shown in the figure, the Fit AP architecture is used in this scenario, and only one AC is applied. All the APs in the teaching buildings belong to the same AP group, whose group ID is **class-room**.
Configuration Steps	● Create a scheduling session on the AC. ● Specify the scheduling interval as the nighttime. ● On the AC, apply the scheduling session to AP group **class-room**.

AC	`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`
	`Hostname(config)# ap-group class-room`
	`Hostname(config-ap-group)# schedule session 1`

Verification	● On the AC, run the **show running-config** command to display the configuration. ● Display the state of AP RF in the scheduling interval. ● Display the state of AP RF beyond the scheduling interval.

AC	`Hostname# show running-config`
	`.....`
	`schedule session 1`
	`schedule session 1 time-range 1 period Sun to Sat time 21:00 to 06:00`
	`.....`
	`ap-group class-room`
	`.....`
	`schedule session 1`
	`.....`

Common Errors

- No scheduling session is created.
- The interval of the scheduling session is incorrectly 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** *sid* command to specify the scheduling session ID of a WLAN.
- The command must be run on the AC where scheduling needs to be enabled.
- 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.

Command	**schedule session** *session-id*
Parameter Description	*session-id*: Indicates the session ID. The value range is from 1 to 64 on an AC.
Defaults	By default, no scheduling session is applied to a WLAN.
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Time Interval for a Scheduling Session

- Mandatory.
- The function must be applied on the AC to enable scheduling.

Command	**schedule session** *session-id* **time-range** *time-range-num* **period** { *day1* [**to** *day2*] **| everyday** } **time** { *hh1:mm1* **to** *hh2:mm2* **| all-day** }
Parameter Description	*session-id*: Indicates the session ID. The value range is from 1 to 64 on an AC. *time-range-num*: Indicates the number of an interval. The value range is from 1 to 8. **period** *day1*: Indicates the start date of the scheduling session cycle, which can be set to

	{ sun | mon | tue | wed | thu | fri | sat }. **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	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Applying a Scheduling Session

- Mandatory.
- The function must be applied to the AC where scheduling needs to be enabled.

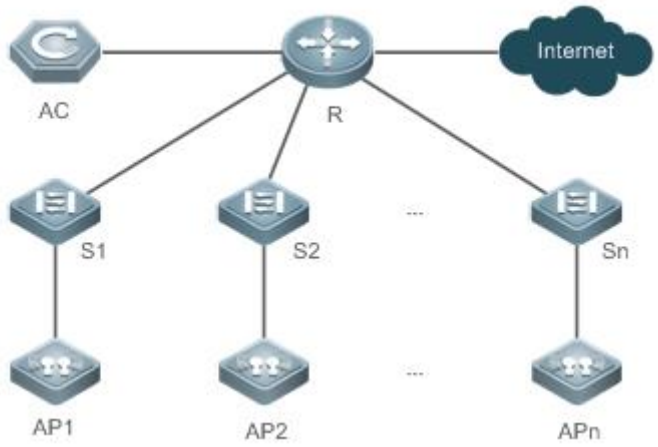
Command	**schedule session** *session-id*
Parameter Description	*session-id*: Indicates the session ID. The value range is from 1 to 64 on an AC.
Defaults	By default, no scheduling session is configured. No scheduling session is applied to a WLAN or radio.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run **show running-config** to display the RF scheduling configuration.
- Check whether scheduling is still performed for a WLAN after a scheduling session expires.

Configuration Example

Providing WLAN Services to Customers in a Bank Only in the Daytime of Workdays

Scenario **Figure 1-4**	 As shown in the figure, the Fit AP architecture is used, and only one AC is applied. WLAN 99 is the customer-use WLAN, and the scheduling session ID is **wlan bank-free**. The APs include AP1, AP2, …, and AP*n*.
Configuration Steps	● Create a scheduling session on the AC. ● On the AC, specify the scheduling intervals as the nighttime of workdays and the whole weekends. ● On the AC, apply the scheduling session to WLAN 99.

AC	`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)# wlan-config 99`
	`Hostname(config-wlan)# schedule session 1`

Verification	● On the AC, run the **show running-config** command to display the configuration. ● Display the state of the WLAN in the scheduling interval. ● Display the state of the WLAN beyond the scheduling interval.

AC	`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`
	`.....`
	`wlan-config 99 wlan-bank-free`

	…… schedule session 1 ……

Common Errors

- No scheduling session is created.
- The interval of the scheduling session is incorrectly configured.

1.5 Monitoring

Displaying

Command	Description
show schedule session [*session-id*]	Display the scheduling session configuration.

1 Configuring RRM

1.1 Overview

Radio resource management (RRM) is used on an access controller (AC) for managing radio resources of access points (APs).

RRM analyzes peripheral radio environments and adjusts the radio channel and power of APs based on specific algorithms to prevent signal interference between APs and ensure proper running of the wireless network.

When an AP has strong interference due to a complex radio environment, enabling RRM can improve user experience.

1.2 Features

Basic Concepts

STA, AP, and AC

- Station (STA): Is a device equipped with wireless network interface cards (NICs), for example, portable computer or mobile phone
- AP: Provides wireless signal access for STAs.
- AC: Manages APs and provides wireless network services.

RF Environment Information

- STA information: Includes the received signal strength indicator (RSSI) and signal-to-noise ratio (SNR) of STAs.
- Neighbor information: Includes the RSSI and working channels of neighboring APs.
- Noise: Indicates the noise value that affects 802.11 signal receiving, in dBm.
- Interference(%): Includes 802.11 signal interference and non-802.11 signal interference. The former indicates signal interference from other APs, and the latter indicates interference from other devices such as microwave ovens and Bluetooth devices.

Co-channel Interference

When two closely deployed APs work in the same channel, co-channel interference occurs, affecting 802.11 wireless packet receiving.

Overview

Feature	Description
Channel Adjustment	Based on the peripheral radio environment, the AC allocates a proper working channel to an AP to reduce co-channel interference and improve wireless access experience of users.
Power Control	When APs are closely deployed and the transmit power of an AP is high, the rest APs may be affected. Therefore, the transmit power of the AP needs to be lowered to reduce interference.
Automatic Coverage Hole Filling	When an AP is offline due to breakdown, the AC selects neighboring APs of the AP based on the neighbor relationship to increase the power and enlarge the coverage scope, so as to eliminate the signal coverage hole caused by the faulty AP.

To perform RRM 2.0 channel adjustment and power control, APs need to support RRM 1.0 or RRM 2.0. Channel adjustment and power control are supported for APs that support RRM 1.0 after they interwork with ACs that support RRM 2.0. However, scanning results reported by APs are limited. When multiple interference signals exist (for example, interference from private APs), the adjustment effect may be affected.

To display RRM versions supported by online APs, run the **show rrm support** command on the AC.

1.2.1 Channel Adjustment

From the perspective of an AP, channel adjustment prevents the AP from serious interference in a working channel.

From the perspective of the global radio environment, proper channel allocation to each AP reduces interference between APs and improves the spectrum resource utilization and user experience.

Working Principle

When two closely deployed APs work in the same channel, a wireless signal conflict or interference occurs, affecting wireless user experience.

The ADCA algorithm comprehensively analyzes various environment factors and allocates the optimized working channels to all APs, preventing channel conflicts.

For example, if two APs work in the same channel or two channels with overlapping spectrum resources, the ADCA algorithm will reallocate non-overlapping channels to optimize spectrum resources.

1.2.2 Power Control

Power control is used to lower the transmit power of an AP to reduce signal interference between APs.

Working Principle

When an AP is powered on for the first time, it uses the allowed maximum transmit power according to national or regional regulations. A higher transmit power indicates a larger signal coverage. If signal coverage of adjacent APs overlaps and the APs are in the same frequency band, strong co-channel interference exists. The Automatic Transfer Power Control (ATPC) algorithm determines whether to increase or reduce the transmit power of an AP based on neighbor information of the AP. When co-channel interference between APs is strong and overlapping channels cannot be avoided, the transmit power of APs needs to be lowered to reduce co-channel interference. If there is no co-channel interference between APs, increase the transmit power to expand the signal coverage area.

If both channel adjustment and power control are enabled, RRM 2.0 preferentially adjusts the channel and then the power. If overlapping channels can be avoided, the transmit power does not need to be lowered. Therefore, the ATPC algorithm is executed following the ADCA algorithm.

1.2.3 Automatic Coverage Hole Filling

After automatic coverage hole filling is enabled, if an AP is offline due to breakdown, the AC selects neighboring APs of the AP based on the neighbor relationship to increase the power and enlarge the coverage scope, so as to eliminate the signal coverage hole caused by the faulty AP.

Working Principle

When this function is enabled or network optimization is conducted on an AP through RRM, the neighbor relationship of the AP is recorded. When an AP goes offline abnormally, the AC selects neighboring APs of the AP to increase the power and enlarge the coverage scope, so as to eliminate the signal coverage hole caused by the offline AP. After the AP is restored and goes online, the AC reduces the increased power of the neighboring APs to their original power and reduce their coverage scope.

1.3 Configuration

Configuration	Description and Command	
Configuring Channel Adjustment	(Optional) It is used to configure channel adjustment parameters.	
	rrm [**2.4g** | **5g** | **6g**] **mode enable**	Enables automatic radio adjustment for newly deployed APs.
	rrm [**2.4g** | **5g** | **6g**] **channel dynamic enable**	Enables dynamic channel adjustment.
	rrm [**2.4g** | **5g** | **6g**] **channel bandwidth** { **current** | **optimal** | { **appoint 20** | **40** | **80** | **160** } }	Selects the channel bandwidth policy during channel adjustment.
	rrm [**2.4g** | **5g** | **6g**] **update** [**ap-group** *group-name*] **channel**	Manually enables channel planning.
	rrm [**2.4g** | **5g** | **6g**] **appoint** *date time* [**ap-group** *group-name*]	Reserves the time to adjust the channel and power for all online APs.
Configuring Power Control	(Optional) It is used to configure parameters related to power control.	
	rrm [**2.4g** | **5g** | **6g**] **mode enable**	Enables automatic RF adjustment for newly deployed APs.
	rrm [**2.4g** | **5g** | **6g**] **update** [**ap-group** *group-name*] **txpower**	Manually enables power planning.
	rrm [**2.4g** | **5g** | **6g**] **appoint** *date time* [**ap-group** *group-name*]	Reserves the time to adjust the channel and power for all online APs.
Enabling Automatic Coverage Hole Filling	**rrm** [**2.4g** | **5g** | **6g**] **blind enable**	Enables automatic coverage hole filling.
	rrm [**2.4g** | **5g** | **6g**] **scan** [**ap-group** *group-name*]	Configures scanning to obtain neighbor information.

1.3.1 Configuring Channel Adjustment

Configuration Effect

- After channel adjustment is enabled, the AC allocates proper working channels to APs based on their radio environments to improve the wireless network experience.

Configuration Steps

Configuring Channel Adjustment

- Optional. To enable the AC to allocate proper working channels to APs, configure the channel adjustment function.
- Run the **rrm** [**2.4g** | **5g** | **6g**] **mode enable** command to enable automatic channel adjustment for newly deployed APs.
- Run the **rrm** [**2.4g | 5g** | **6g**] **channel bandwidth** { **current** | **optimal** | { **appoint 20** | **40** | **80** | **160** } } command to configure a channel bandwidth policy.
- Run the **rrm** [**2.4g** | **5g** | **6g**] **channel dynamic enable** command to enable dynamic channel adjustment.
- Run the **rrm** [**2.4g** | **5g** | **6g**] **update** [**ap-group** *group-name*] **channel** command to enable channel planning for online APs within the specified range.
- Run the **rrm** [**2.4g** | **5g** | **6g**] **appoint** *date time* [**ap-group** *group-name*] command to reserve a time to adjust the channel and power for online APs within the specified range.

Command	**rrm** [**2.4g**	**5g**	**6g**] **mode enable**
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. **6g**: Indicates the 6 GHz network.
Defaults	Automatic power adjustment is disabled for newly deployed APs on all frequency bands by default.
Command Mode	Global configuration mode or AP group configuration mode
Usage Guide	● When a newly deployed AP goes online, radio adjustment is performed for the AP. The original configuration is retained for existing APs when they go online. ● If no frequency band is specified, the configuration takes effect on all frequency bands. ● If the function is configured in global configuration mode, it will take effect globally. If the function is configured in AP group configuration mode, it will only take effect for the AP group. The configuration in AP group configuration mode takes precedence over that in global configuration mode. ● The channel and power of newly deployed APs in the same range and frequency band are adjusted simultaneously. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Command	**rrm** [**2.4g**	**5g**	**6g**] **channel bandwidth** { **current**	**optimal**	{ **appoint 20**	**40**	**80**	**160** } }
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. **6g**: Indicates the 6 GHz network.

	current: Indicates that the current channel bandwidth configuration is selected during channel planning. **optimal**: Indicates that the channel bandwidth configuration is selected automatically during channel planning. **appoint:** Specifies the channel width configuration. Except the 2.4 GHz radio, the available channel width for other radios includes 20 MHz, 40 MHz, 80 MHz, and 160 MHz.
Defaults	The optimal channel bandwidth policy is configured for all frequency bands by default.
Command Mode	Global configuration mode
Usage Guide	1. The channel bandwidth configuration is selected automatically based on radio types of APs and effective channel ranges. The selection rules are as follows: (1) Use 20 MHz channel width for the 2.4 GHz frequency band. (2) Use 40 MHz channel width for the 5 GHz frequency band without channel limitations. (3) Use 40 MHz channel width for radios that are limited to channels 36 to 64. (4) Use 20 MHz channel width for radios that are limited to channels 149 to 165. (5) Use 20 MHz channel width for the 5G radio of the i-Share+ AP. (6) Use 80 MHz channel width for the 6G radio. 2. If no frequency band is specified, the configuration takes effect on all frequency bands. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Command	**rrm** [**2.4g** | **5g** | **6g**] **channel dynamic enable**
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. **6g**: Indicates the 6 GHz network.
Defaults	Dynamic channel adjustment is disabled for all frequency bands by default.
Command Mode	Global configuration mode or AP group configuration mode
Usage Guide	1. When dynamic channel adjustment is enabled, RRM 2.0 checks channel interference of APs every 5 minutes. If the channel interference exceeds the threshold, RRM 2.0 triggers channel adjustment for the APs. 2. The adjusted channel configuration will overwrite original channel and channel bandwidth configuration (when the optimal policy is selected) of APs in AP configuration mode. In addition, STAs may be disconnected due to channel switching during adjustment. 3. If no frequency band is specified, the configuration takes effect on all frequency bands. 4. If the function is configured in global configuration mode, it will take effect globally. If the function is configured in AP group configuration mode, it will only take effect for the AP group. The configuration in AP group configuration mode takes precedence over that in global configuration mode. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Command	**rrm** [**2.4g** | **5g** | **6g**] **update** [**ap-group** *group-name*] **channel**
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. **6g**: Indicates the 6 GHz network. *group-name*: Performs RF adjustment for the specified AP group. **channel**: Enables automatic channel adjustment for APs.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	1. If no frequency band is specified, the configuration takes effect on all frequency bands. 2. If **ap-group** is not configured, RF planning is performed for online APs on the entire network. Otherwise, it is performed only for online APs in the AP group. 3. If **channel** is configured, only the channel and bandwidth (when the optimal policy is selected) of APs are planned and the power configuration remains unchanged. 4. After adjustment is completed, automatic radio adjustment is enabled for newly deployed APs in the corresponding frequency band automatically. If **ap-group** is not configured, automatic radio adjustment is enabled on the entire network. Otherwise, it will only be enabled for online APs in the AP group. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Command	**rrm** [**2.4g** | **5g** | **6g**] **appoint** *date time* [**ap-group** *group-name*]
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. **6g**: Indicates the 6 GHz network. *date*: Specifies the reservation date, in the format of yyyy-mm-dd. *time*: Specifies the reservation time, in the format of hh:mm:ss. *group-name*: Reserves radio adjustment for online APs in the specified AP group.
Defaults	By default, no reservation time is set.
Command Mode	Global configuration mode
Usage Guide	1. If the reservation time is configured, the AC will adjust the channel and power for online APs in a specific frequency band and range at the specified time. 2. If no frequency band is specified, the configuration takes effect on all frequency bands. 3. If **ap-group** is not configured, the AC will adjust the channel and power for online APs on the entire network. Otherwise, the AC will adjust the channel and power for online APs in the specified AP group. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Verification

- Run the **show rrm** [**2.4g** | **5g** | **6g**] **summary** command to display the channel adjustment status.
- Run the **show ap-config summary** command to display channel adjustment results of APs.

Configuration Example

Configuring Channel Adjustment Parameters

Configuration Steps	Enable automatic channel planning for newly deployed APs on the entire network.

AC	`Hostname# configure terminal`
	`Hostname(config)# rrm mode enable`
	`Hostname(config)# exit`

Verification	Display the channel adjustment status.

AC	`Hostname# show rrm 2.4g summary`
	`Radio Resource Management`
	`Radio Type..... 2.4G`
	`RRM Enable Mode..... Enable`
	`Channel Width Strategy..... Optimal`
	`Channel Dynamic Enable Mode..... Enable`
	`Run Status..... Finish`

1.3.2 Configuring Power Control

Configuration Effect

- After power control is enabled, the AC configures the transmit power for APs based on their radio environments to reduce co-channel interference between the APs.

Notes

- Power control is used to reduce co-channel interference of an AP to other APs. The ATPC algorithm needs to obtain the co-channel interference from other APs to determine whether to control the power.

Configuration Steps

Configuring Power Control

- Optional. To control APs' transmit power to prevent co-channel interference between APs, configure the power control function.
- Run the **rrm** [**2.4g** | **5g** | **6g**] **mode enable** command to enable automatic power adjustment for newly deployed APs.
- Run the **rrm** [**2.4g** | **5g** | **6g**] **update** [**ap-group** *group-name*] **txpower** command to manually enable power adjustment for online APs within the specified range.

- Run the **rrm** [**2.4g** | **5g** | **6g**] **appoint** *date time* [**ap-group** *group-name*] command to reserve a time to adjust the channel and power for online APs within the specified range.

Command	**rrm** [**2.4g** | **5g** | **6g**] **mode enable**
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. **6g**: Indicates the 6 GHz network.
Defaults	By default, automatic power adjustment is disabled.
Command Mode	Global configuration mode or AP group configuration mode
Usage Guide	1. When a newly deployed AP goes online, RF adjustment is performed for the AP. The original configuration is retained for existing APs when they go online. 2. If no frequency band is specified, the configuration takes effect on all frequency bands. 3. If the function is configured in global configuration mode, it will take effect globally. If the function is configured in AP group configuration mode, it will only take effect for the AP group. The configuration in AP group configuration mode takes precedence over that in global configuration mode. 4. The channel and power of newly deployed APs in the same range and frequency band are adjusted simultaneously. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Command	**rrm** [**2.4g** | **5g** | **6g**] **update** [**ap-group** *group-name*] **txpower**
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. **6g**: Indicates the 6 GHz network. *group-name*: Performs RF adjustment for online APs in the specified AP group.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	1. If no frequency band is specified, the configuration takes effect on all frequency bands. 2. If **ap-group** is not configured, radio adjustment is performed for online APs on the entire network. Otherwise, radio adjustment is performed for only online APs in the specified AP group. 3. If **channel** is configured, only the channel and bandwidth (when the optimal policy is selected) of APs are planned and the power configuration remains unchanged. If **txpower** is configured, only the power of the APs is planned and the channel and bandwidth configurations remain unchanged. If **channel** or **txpower** is not configured, the channel and bandwidth (when the optimal policy is selected) as well as the power of APs are planned. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Command	**rrm** [**2.4g** | **5g** | **6g**] **appoint** *date time* [**ap-group** *group-name*]
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. **6g**: Indicates the 6 GHz network. *date*: Specifies the reservation date, in the format of yyyy-mm-dd. *time*: Specifies the reservation time, in the format of hh:mm:ss. *group-name*: Reserves RF adjustment for a specified AP group.
Defaults	By default, no reservation time is set.
Command Mode	Global configuration mode
Usage Guide	1. If the reservation time is configured, RRM 2.0 will adjust the channel and power for online APs in a specific frequency band and range at the specified time. 2. If no frequency band is specified, the configuration takes effect on all frequency bands. 3. If **ap-group** is not configured, the AC will adjust the channel and power for online APs on the entire network. Otherwise, the AC will adjust the channel and power for online APs in the specified AP group. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Verification

- Run the **show rrm** [**2.4g** | **5g** | **6g**] **summary** command to display the power adjustment status.
- Run the **show ap-config summary** command to display channel adjustment results of APs.

Configuration Example

Configuring Power Control Parameters

Configuration Steps	Enable the power adjustment function on the entire network.

AC	`Hostname# configure terminal`
	`Hostname(config)# rrm mode enable`
	`Hostname(config)# exit`

Verification	Display the power control status.

AC	`Hostname# show rrm 2.4g summary`
	`Radio Resource Management`
	`Radio Type..... 2.4G`
	`RRM Enable Mode..... Enable`
	`Channel Width Strategy..... Optimal`
	`Channel Dynamic Enable Mode..... Enable`

	Run Status..... Finish

1.3.3 Enabling Automatic Coverage Hole Filling

Configuration Effect

After the coverage hole filling function is enabled, when an AP goes offline abnormally, the AC selects neighboring APs of the AP to increase the power and enlarge the coverage scope, so as to eliminate the signal coverage hole caused by the offline AP. After the AP is restored and goes online, the AC reduces the increased power of the neighboring APs to their original power and reduce their coverage scope.

Notes

Ensure that other APs are deployed around an abnormal AP, and they work in the same frequency band as the abnormal AP.

Configuration Steps

↘ Enabling Automatic Coverage Hole Filling

- Optional. To ensure high reliability of a wireless network, configure coverage hole filling.
- Run the **rrm** [**2.4g** | **5g** | **6g**] **blind enable** command to enable coverage hole filling.
- Run the **rrm** [**2.4g** | **5g** | **6g**] **scan** [**ap-group group-name**] command to issue a scanning request to radios in a specified band or AP group.

Command	**rrm** [**2.4g** | **5g** | **6g**] **blind enable**
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network.
Defaults	By default, automatic coverage hole filling is disabled.
Command Mode	Global configuration mode or AP group configuration mode
Usage Guide	1. If no frequency band is specified, the configuration takes effect on all frequency bands. 2. If the function is configured in global configuration mode, it will take effect globally. If the function is configured in AP group configuration mode, it will only take effect for the AP group. The configuration in AP group configuration mode takes precedence over that in global configuration mode. After the APs are offline, there are two prerequisites for improving the effect of coverage hole filling of neighboring APs: (1) Other APs are deployed around the AP and they operate in the same frequency band. (2) The power configuration value of neighboring APs is less than 100%. 3. To maximize the networking experience, you are advised to enable automatic coverage hole filling in the following two scenarios: (1) When network-wide APs are online, you are advised to configure channel adjustment and power control to optimize the wireless network once, and then enable automatic coverage hole filling.

(2) You can also conduct network optimization manually or by using the WIS. Then, enable the automatic coverage hole filling and run the **rrm scan** command to scan the neighbor relationship of an AP.

4. Re-scanning is required when the AP goes online for the first time, the AP location is changed, or the AP RF band is changed.
5. Do not adjust the AP power randomly after automatic coverage hole filling takes effect. If the AP power must be adjusted, re-enable automatic coverage hole filling after adjustment.

⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Command	**rrm** [**2.4g** | **5g** | **6g**] **scan** [**ap-group** *group-name*]
Parameter Description	**2.4g**: Indicates the 2.4 GHz network. **5g**: Indicates the 5 GHz network. *group-name:* Conducts radio adjustment for a specified AP group.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	1. If no frequency band is specified, the configuration takes effect on all frequency bands. 2. If **ap-group** is not configured, scanning is performed on RF interfaces of online APs on the entire network. Otherwise, scanning is only conducted on online APs in that AP group. 3. After scanning is triggered, it takes some time for RF interfaces of APs to conduct scanning. You can run the **show rrm neighbor** command to display the acquired neighbor information about the AP. 4. Re-scanning is required when the AP goes online for the first time, the AP location is changed, or the AP RF band is changed. ⚠ Support for the 6 GHz frequency band depends on local rules and regulations in different countries and regions. In countries and regions where the 6 GHz frequency band is not supported, 6 GHz signals are unavailable even if related commands are executed.

Verification

- Run the **show rrm** [**2.4g** | **5g** | **6g**] **summary** command to display the status of the coverage hole filling function.
- Run the **show rrm** [**2.4g** | **5g** | **6g**] **neighbor** command to display information about neighbors of an online AP.

Configuration Example

↘ Enabling Coverage Hole Filling

Configuration	Enable automatic coverage hole filling on the entire network.

Steps

AC

```
Hostname# configure terminal
Hostname(config)# rrm blind enable
Hostname(config)# exit
```

Verification Display the channel adjustment status.

AC

```
Hostname# show rrm 2.4g summary
Radio Resource Management
  Radio Type.....  2.4G
  RRM Enable Mode.....  Enable
  Channel Width Strategy.....  Optimal
  Channel Dynamic Enable Mode.....  Enable
  Blind Mode.....  Enable
  Run Status.....  Finish
```

Triggering Scanning

Configuration Steps Enable automatic coverage hole filling on the entire network.

AC

```
Hostname# configure terminal
Hostname(config)# rrm scan
Hostname(config)# exit
```

Verification Display the channel adjustment status.

AC

```
Hostname# show rrm 2.4g neighbor
AP Neighbors ------------------------ 2.4G
(0085.0020.0025::1)
        (00d0.f822.3114::1)  RSSI:-12
        (00d0.f822.3344::1)  RSSI:-23
 (00d0.f822.3114::1)
        (0085.0020.0025::1)  RSSI:-37
        (00d0.f822.3344::1)  RSSI:-23
(00d0.f822.3344::1)
        (00d0.f822.3114::1)  RSSI:-36
```

```
(0085.0020.0025::1)  RSSI:-37
```

Common Errors

N/A

1.4 Monitoring

Displaying

Command	Description
show rrm [**2.4g** | **5g** | **6g**] **summary**	Displays basic RRM configuration.
show rrm support	Displays RRM versions supported by online APs.
show rrm [**2.4g** | **5g** | **6g**] **neighbor**	Displays the information about neighbors of an AP.

1 Configuring 802.11kv

1.1 Overview

The 802.11k protocol revises radio resource measurement (RRM) of the 802.11 protocol, which enables access points (APs) and stations (STAs) to obtain RRM data of each other. The 802.11v protocol revised wireless network management (WNM) of the 802.11 protocol. The 802.11k or 802.11v protocol enables access controllers (ACs) to manage wireless network resources better and supports the load balancing function.

On wireless networks, STAs are often unable to proactively connect to low-utilization channels, centrally connect to an AP, or have poor STA signals because they are unable to detect the load of APs. 802.11kv can help realize load balancing, including channel load balancing and load balancing between radios. With the increasing mobile office scenarios, there are higher roaming requirements of STAs. To minimize the impact of 802.11k on STA services and enable immediate switching with 802.11v, the AI radio-based devices have added the roaming enhancement function. This guides STAs to switch to APs with better signals when the signal quality is poor, thereby improving STA service experience and wireless channel performance.

Protocols and Standards

- IEEE 802.11k-2008: Amendment 1: Radio Resource Measurement of Wireless LANs
- IEEE 802.11v-2011: Amendment 8: IEEE 802.11 Wireless Network Management

1.2 Applications

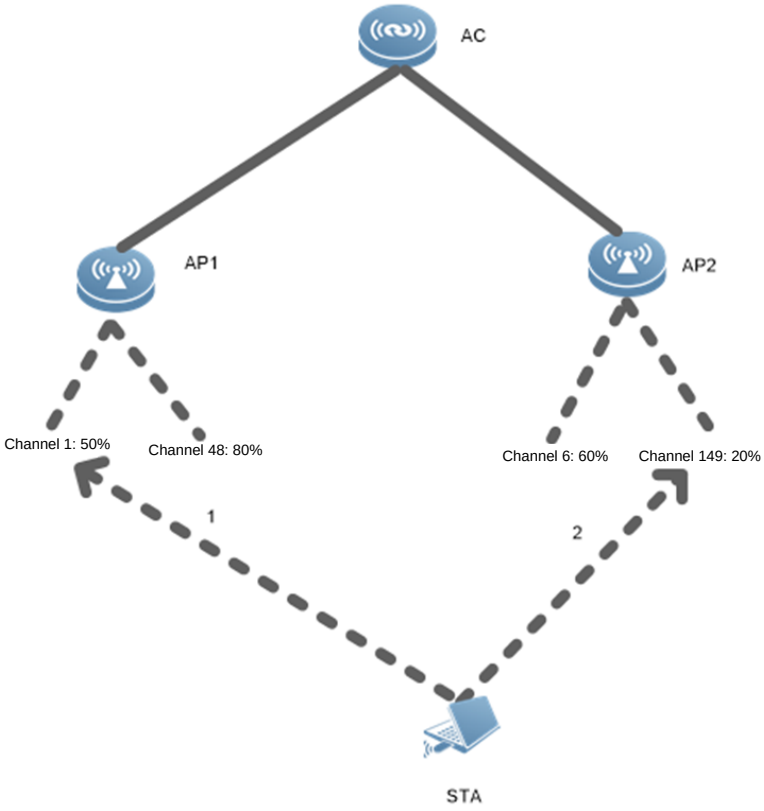
Application	Description
Channel Utilization Balancing	Uses Fit AP networking with at least one AC and two APs.
STA Balancing Between Radios	Uses Fit AP networking with at least one AC and two APs.
Guided Roaming for STAs with the Poor Signal Quality	Uses Fit AP networking with at least one AC and two APs. The 802.11v-based guided roaming is applied to STAs of associated APs that support 802.11v and enter areas with poor signal quality.

1.2.1 Channel Utilization Balancing

Scenarios

On a wireless network, especially in high-density STA deployment scenarios, channel utilization is unbalanced due to various reasons. Because STAs cannot detect channel utilization, they may select a channel with the higher utilization. Therefore, channel utilization balancing is required to migrate STAs to channels with low utilization within 2s to 10s after STAs go online, to improve user experience.

Figure 1-1



Deployment

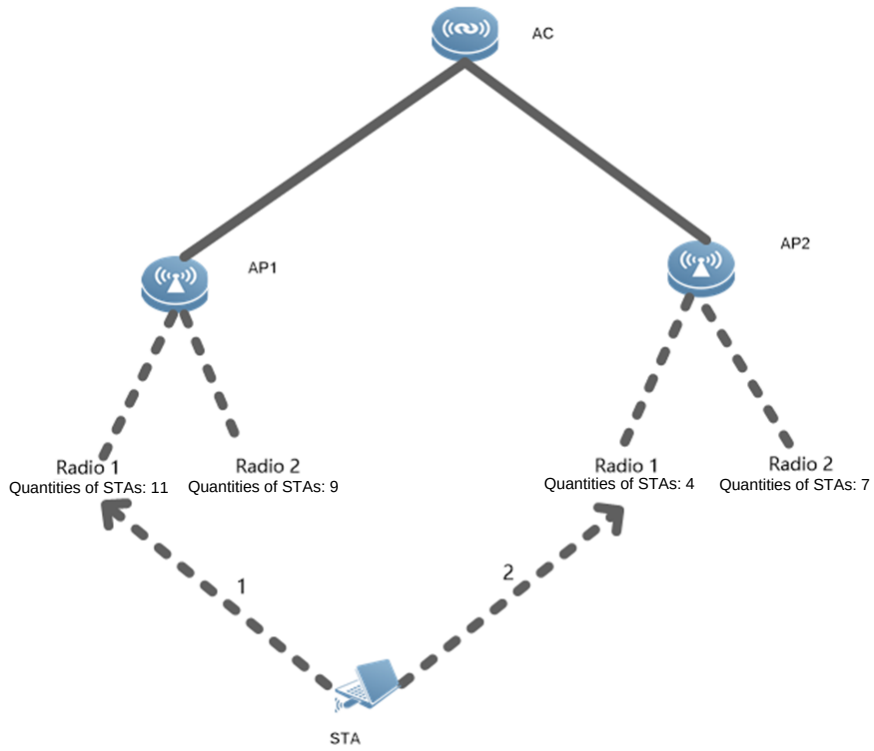
- Set the load balancing mode to channel utilization balancing on the AC.
- Set load balancing parameters on the AC.

1.2.2 STA Balancing Between Radios

Scenarios

When APs are deployed densely, multiple STAs may connect to the same AP. As a result, STA quantities on APs are unbalanced.

Figure 1-2



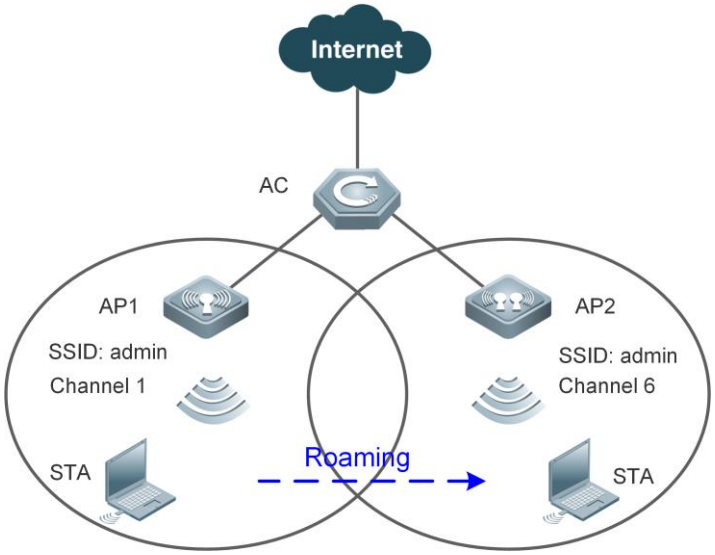
Deployment

- Set the load balancing mode to STA quantity balancing between radios on the AC.
- Set parameters of STA quantity balancing between radios on the AC.

1.2.3 Guided Roaming for STAs with the Poor Signal Quality

Scenario

On a wireless network, some STAs may have poor roaming aggressiveness, meaning they stay connected to their initially associated AP even when they are far away from the AP, experiencing weak signals, low communication rates, and high channel utilization of the AP. These STAs do not proactively roam to closer APs with stronger signals and lower channel utilization. To address this issue, introduce guided roaming for these STAs when 802.11v is supported, to improve the STAs' user experience and overall wireless channel performance.



Deployment

- Select the sensitivity of the roaming enhancement mode on the AC.
- Conduct 802.11v-based guided roaming for STAs with the poor signal quality on the AC based on the roaming sensitivity.

1.3 Features

Basic Concepts

Channel Utilization

Channel utilization is an important indicator that affects the STA connection quality. In scenarios where there are high levels of service traffic, a large number of connected STAs, or strong RF interference, the channel utilization of APs may be high. When a STA associates with a wireless network, it typically selects the strongest signal from multiple BSSIDs with the same Wi-Fi name. However, the strongest signal may come from an AP with high channel utilization.

Overview

Feature	Description
802.11kv-based Load Balancing	Improves the STA connection quality and balances the AP load.
802.11kv-based Guided Roaming	Steers STAs with the poor signal quality to connect to an AP with stronger signals.

1.3.1 802.11kv-based Load Balancing

Load balancing can steer STAs to evenly distribute themselves across different channels or RF interfaces when accessing Wi-Fi signals, in order to achieve better connectivity experience.

Working Principle

When a STA that supports the 802.11k protocol associates with an AC, the AC can obtain an available BSSID list from the STA in real time. Each BSSID is accompanied by a signal strength value. If the STA does not support the 802.11k protocol, the available BSSID list is obtained through probe frames from the STA.

When 802.11kv-based load balancing is enabled, the following two scenarios may occur:

1. Channel utilization balancing

If a STA is on a channel with 70% or higher utilization, the AC selects a BSSID from the available BSSID list that has 20% less channel utilization than the current channel and the highest signal strength of no less than –63 dBm. The AC then steers the STA to switch to this new BSSID, which balances channel utilization.

2. Load balancing between radios

If the number of STAs on the current radio is greater than 10, the AC selects a BSSID from the available BSSID list with five fewer STAs than the current channel and the highest signal strength of no less than –63 dBm. The AC then steers the STA to switch to this BSSID, achieving radio load balancing.

1.3.2 802.11kv-based Guided Roaming

Guided roaming can guide poorly performing STAs to switch to better APs through BSTM packets sent by APs through 802.11v. This is particularly helpful when STAs do not roam automatically or promptly, resulting in an enhanced STA service experience and improved wireless channel performance.

Working Principle

Based on BSSID information of neighboring APs reported by APs, the AC establishes a neighbor AP relationship table for each AP. When a STA moves away from the associated AP, the AP reports the STA's RSSI, association rate, channel utilization, and other information to the AC periodically. The AC processes the reported information and determines whether the STA is in an area with the poor signal quality.

When the STA is in an area with the poor signal quality, the AC distributes the STA information to neighboring APs of the associated AP. The neighboring APs start scanning the status of the STA through AI radio and report it to the AC. The AC selects multiple candidate APs suitable for the STA, generates an ordered list, and notifies the STA through BSTM packets. The STA detects the candidate APs based on its own strategy and switches to a suitable AP after finding one.

1.4 Configuration

Configuration	Description and Command	
Configuring Channel Utilization Balancing	(Optional) It is used to enable 802.11kv interaction.	
	802.11kv enable	Enables 802.11k/802.11v.
Configuring STA Balancing Between Radios	(Mandatory) It is used to set the load balancing mode.	
	802.11kv load-balance mode channel-utilization	Sets the load balancing mode to channel utilization balancing.
	802.11kv load-balance mode station-number	Sets the load balancing mode to STA balancing between radios.
	802.11kv load-balance mode none	Disables load balancing.

Configuring Guided Roaming for STAs with the Poor Signal Quality	(Mandatory) It is used to set the load balancing mode.	
	802.11kv roam-e mode disable	Disables the roaming enhancement mode.
	802.11kv roam-e mode sensitivity-high	Configures the high roaming sensitivity, indicating that it is easier to trigger the roaming function. This is suitable for scenarios with high requirements for roaming experience, such as situations where the STA has low receive and transmit sensitivity.
	802.11kv roam-e mode sensitivity-middle	Configures the medium roaming sensitivity, which is the default configuration mode (recommended).
	802.11kv roam-e mode sensitivity-low	Configures the low roaming sensitivity, meaning that it is less likely to trigger the roaming enhancement function. This is suitable for scenarios where roaming requirements are not high but STA's tendency to stick to a particular AP during association needs to be minimized.

1.4.1 Configuring Channel Utilization Balancing

Configuration Effect

When a STA that supports the 802.11v protocol connects to the wireless network, if the channel corresponding to the RF interface has a utilization higher than the preset value and another channel with lower utilization is available (the difference value is lower than the preset gain value), the STA will be migrated to the available channel.

Notes

- Load balancing takes effect only for the STAs that support 802.11k and 802.11v.
- If most STAs do not support 802.11k, roaming stickiness can be enabled for the corresponding AP group. This function is used to learn probe frames sent before a STA is associated, to determine the STA location.

Configuration Steps

Enabling 802.11kv

- Mandatory.
- Run the **802.11kv enable** command to enable 802.11k and 802.11v interaction in global configuration mode on the AC.

Command	**802.11kv enable**
Parameter Description	N/A
Defaults	By default, 802.11k and 802.11v interaction is disabled.
Command	Global configuration mode

Mode	
Usage Guide	N/A

Configuring the Load Balancing Mode Based on Channel Utilization

- Mandatory.
- Configure 802.11kv load balancing based on channel utilization in global configuration mode on the AC.

Command	**802.11kv load-balance mode channel-utilization**
Parameter Description	N/A
Defaults	By default, load balancing is not performed.
Command Mode	Global configuration mode
Usage Guide	Channel utilization balancing is triggered when a STA is associated with a channel with the utilization equal to or greater than 70% and there are neighboring channels with the utilization 20% less than the associated channel.

Verification

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

1.4.2 Configuring STA Balancing Between Radios

Configuration Effect

When a STA is associated with a radio on which the number of connected STAs is greater than or equal to the preset limit value and there is a neighboring radio on which the number of connected STAs is less than the preset limit value, the STA will be steered to associate with the neighboring radio.

Notes

Load balancing takes effect only for the STAs that support 802.11k and 802.11v.

Configuration Steps

Configuring the Load Balancing Mode Based on the Number of STAs Between Radios

- Mandatory.
- Enable 802.11k and 802.11v interaction in global configuration mode on the AC.

Command	**802.11kv enable**
Parameter Description	N/A
Defaults	By default, 802.11k and 802.11v interaction is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Load Balancing Mode Based on the Number of STAs Between Radios

- Mandatory.
- Configure the 802.11kv load balancing mode based on the number of STAs between radios in global configuration mode on the AC.

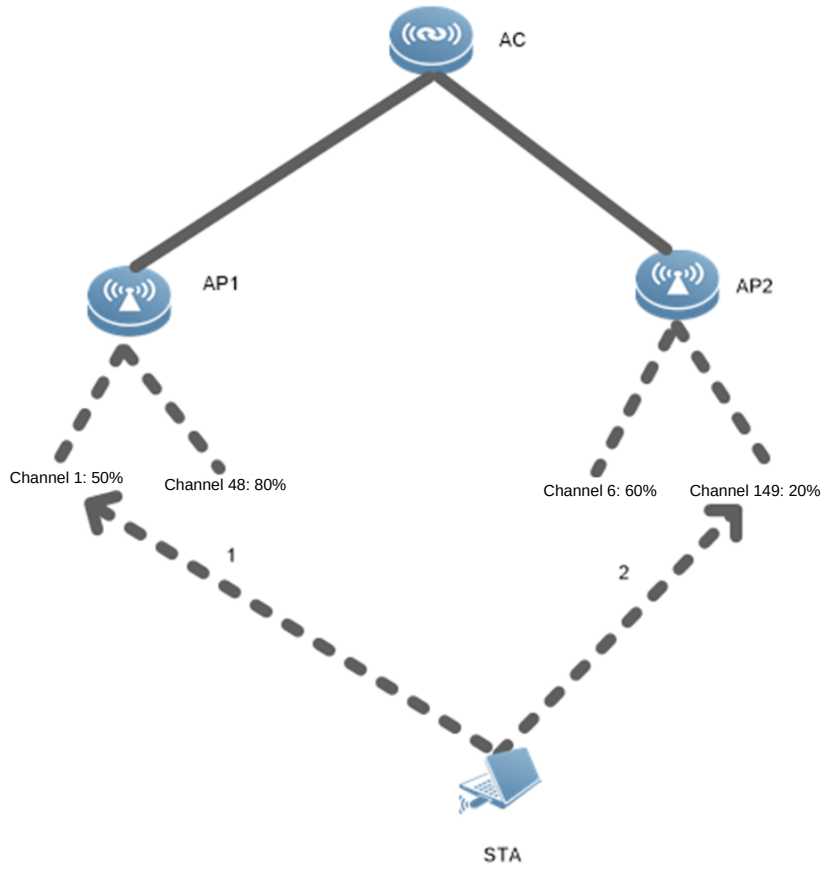
Command	**802.11kv load-balance mode station-number**
Parameter Description	N/A
Defaults	By default, load balancing is not performed.
Command Mode	Global configuration mode
Usage Guide	STA balancing between radios is triggered when a STA is associated with a radio on which the number of connected STAs is greater than 10 and there is a neighboring radio on which the number of connected STAs is less than 5.

Verification

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

Configuration Example

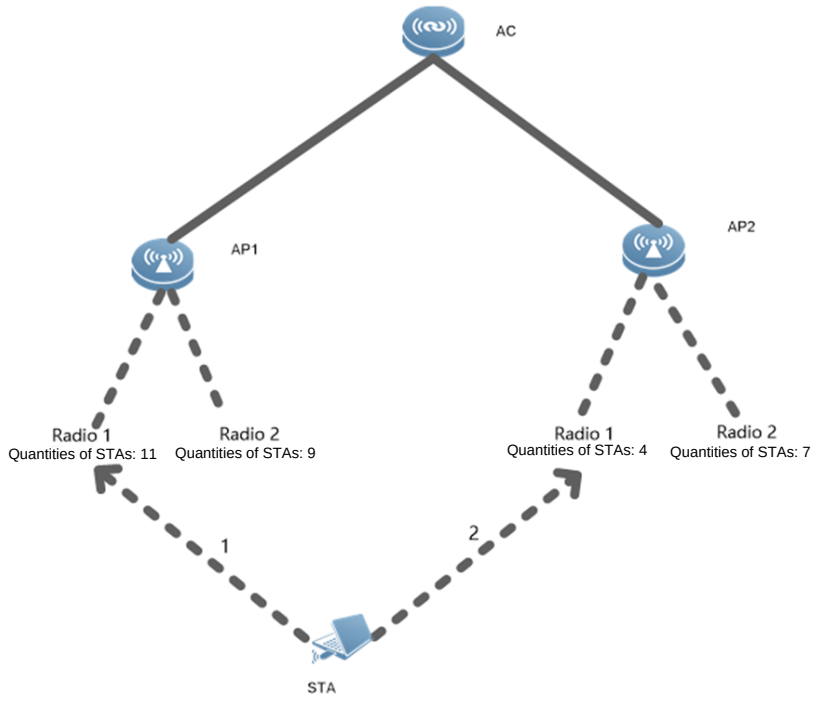
Configuring Channel Utilization Balancing

Scenario **Figure 1-3**	
Configuration Steps	Enable 802.11k and 802.11v interaction.

AC	`Hostname(config)# 802.11kv enable`
	Set the load balancing mode.
	`Hostname(config)# 802.11kv load-balance mode channel-utilization`
Verification	Run the **show running-config** command to display the configuration.

AC	`Hostname# show running-config | begin 802.11kv`
	`802.11kv enable`
	`802.11kv load-balance mode channel-utilization`

Configuring STA Balancing Between Radios

Scenario **Figure 1-4**	
Configuration Steps	Enable 802.11k and 802.11v interaction.
AC	`Hostname(config)# 802.11kv enable`
	Set the load balancing mode.
	`Hostname(config)# 802.11kv load-balance mode station-number`
Verification	Run the **show running-config** command to display the configuration.

AC	`Hostname# show running-config | begin 802.11kv`
	`802.11kv enable`
	`802.11kv load-balance mode station-number`

1.4.3 Configuring Guided Roaming for STAs with the Poor Signal Quality

Configuration Effect

For the STAs that support the 802.11v protocol, if they are associated with an AP and their signal quality falls into the poor signal quality interval, roaming enhancement can be introduced to steer the STAs to perform 802.11v-based roaming based on the configured roaming sensitivity. By doing so, the STAs can be associated with a better AP.

Notes

- Roaming enhancement only applies to the STAs that support 802.11v.
- Roaming enhancement is only supported on AR series APs.

Configuration Steps

Enabling 802.11kv

- Mandatory.
- Run the **802.11kv enable** command in global configuration mode on the AC.

Command	**802.11kv enable**
Parameter Description	N/A
Defaults	By default, 802.11k and 802.11v interaction is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Selecting the Sensitivity of the Roaming Enhancement Mode

- Mandatory.
- Run the **802.11kv roam-e mode** command in global configuration mode on the AC.

Command	**802.11kv roam-e mode** { **disable** | **sensitivity-high** | **sensitivity-low** | **sensitivity-middle** }
Parameter Description	**disable**: Disables the roaming enhancement mode. **sensitivity-high**: Sets the sensitivity of the roaming enhancement mode to high. **sensitivity-middle**: Sets the sensitivity of the roaming enhancement mode to medium. **sensitivity-low**: Sets the sensitivity of the roaming enhancement mode to low.
Defaults	The default mode is **sensitivity-middle**.
Command Mode	Global configuration mode
Usage Guide	1. When roaming enhancement is disabled, the AC will not execute roaming enhancement. Guided roaming will only be performed on STAs when roaming sensitivity is configured. 2. Layer 2 network connectivity between APs is required for using guided roaming.

Verification

Run the **show running-config** command to display 802.11kv-based association information.

1.5 Monitoring

Displaying

Command	Description
show 802.11kv all-bstms	Displays BSTM records sent by the AC to all STAs.
show 802.11kv bstms-per-station	Displays BSTM records sent by the AC to a specific STA.
show 802.11kv roam-e ap-info [*mac*]	Displays information about AR series APs under the AC.
show 802.11kv roam-e mode	Displays the roaming enhancement sensitivity configured on the AC.
show 802.11kv roam-e neighbor-ap [*mac*]	Displays information about neighboring APs of AR series APs on the AC.
show 802.11kv roam-e roam-station [*station-mac*]	Displays information about STAs that need to roam on the AC.
show 802.11kv roam-e roamed-station [*station-mac*]	Displays information about STAs that have already finished roaming on the AC.
show 802.11kv roam-e statistic	Displays statistics about roaming enhancement on the AC.

1 Configuring CorrectLink

1.1 Overview

CorrectLink provides an intelligent WLAN access solution to identify and guide access behaviors of stations (STAs), so that STAs can connect to access points (APs) with the optimal performance.

CorrectLink can perform guidance of 5 GHz preferred, remote association, and load balancing on STAs.

5 GHz preferred is to guide STAs with 5 GHz capabilities to associate with 5 GHz signals for better experience.

Remote association is to prevent STAs from associating with signals of low Received Signal Strength Indication (RSSI).

Load balancing is to make STAs connect to lower-load APs in the case of no remote association.

1.2 Applications

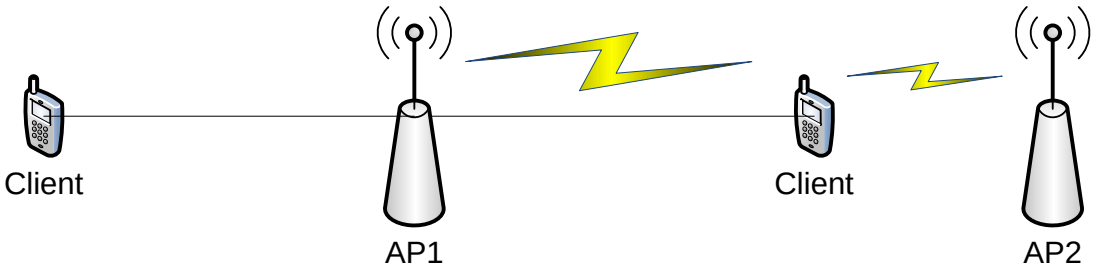
Application	Description
Remote Association	A STA is not connected to a near AP, but a far AP. In this case, the STA's uplink transmission rate is low with poor signals, resulting in poor wireless experience. Remote association can make the STA associate with a stronger-signal AP.
5 GHz Preferred	A dual-band STA does not select the 5 GHz frequency band, but the 2.4 GHz frequency band. The 2.4 GHz frequency band provides a small number of channels. It guarantees good user experience in idle time, but results in poor user experience in peak-load hours. 5 GHz preferred can guide STAs supporting 5 GHz to the 5 GHz frequency band.
Load Balancing	The excessive density of STAs is causing issues, restricting user experience due to access congestion. Even in an optimized network environment, where STAs are connected to the nearest APs and the 5 GHz frequency band is utilized, a high access density can compromise air interface service quality and ultimately impact the user experience.

1.2.1 Remote Association

Scenario

As shown in the following figure, a STA is not connected to a near AP, but a far AP. In this case, the STA's uplink transmission rate is low with poor signals, resulting in poor wireless experience. Remote association can make the STA associate with a stronger-signal AP.

Figure 1-1



Deployment

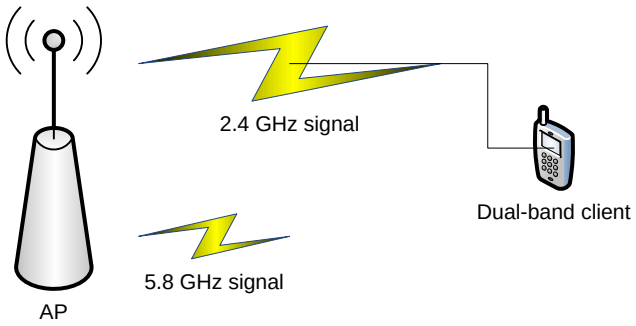
- Enable CorrectLink to resolve remote association issues.

1.2.2 5 GHz Preferred

Scenario

As shown in the following figure, a dual-band STA does not select the 5 GHz frequency band, but the 2.4 GHz frequency band. The 2.4 GHz frequency band provides a small number of channels. It guarantees good user experience in idle time, but results in poor user experience in peak-load hours. 5 GHz preferred can steer STAs supporting 5 GHz to the 5 GHz frequency band.

Figure 1-2



Deployment

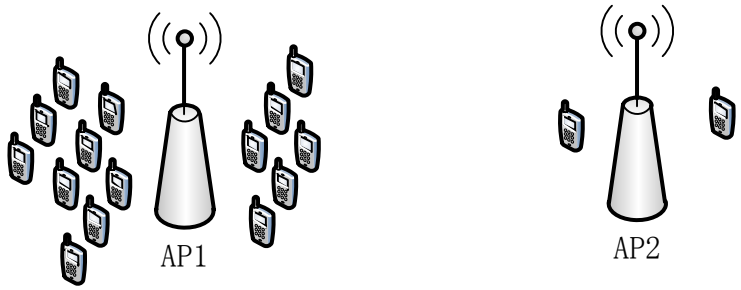
- Enable CorrectLink to resolve 5 GHz preferred issues.

1.2.3 Load Balancing

Scenario

As shown in the following figure, the distribution density of STAs is unmanageable, which is severely limiting their overall experience due to the high access density. Despite having optimal network optimization parameters and connecting to the nearest APs on the 5 GHz frequency band in a network environment, the air interface quality of service may suffer greatly from such high access density, causing a detrimental impact on the overall user experience.

Figure 1-3



Deployment

- Enable CorrectLink to resolve load balancing issues.

1.3 Features

Basic Concepts

CorrectLink

CorrectLink steers STAs to achieve optimal access, and provides functions of remote association, 5 GHz preferred, and load balancing.

Overview

Feature	Description
CorrectLink	Steers clients to achieve optimal access.

1.3.1 CorrectLink

During client access, perform guidance of remote association, 5 GHz preferred, and load balancing on clients, so that the clients achieve the optimal access state.

Working Principle

The AC determines whether a STA accesses the optimal AP based on the information detected during STA association and CorrectLink rules. If the STA fails to access the optimal AP, the AC steers the STA.

Access guidance rules:

If the difference between the detected RSSI of the AP and the highest RSSI is less than 10 dBm (default value), the set of APs is called an APset. If the load of an AP included in the APset is five (default value) fewer than that of the connected AP, a Cset exists.

If the connected AP does not belong to the APset, the STA cannot access the AP.

If the connected AP belongs to the APset but the Cset is not null, the STA cannot access the AP.

If the connected AP belongs to the APset and the Cset is null, the STA can access the AP.

1.4 Configuration

Configuration	Description and Command	
Configuring CorrectLink	(Optional) It is used to steer client access.	
	clink enable	Enables CorrectLink.
	clink rssi-delta-threshold	Configures the remote association RSSI difference threshold of CorrectLink.
	clink lb-client-threshold	Configures the load balancing determination threshold of CorrectLink.
	clink lb-client-delta-threshold	Configures the load balancing difference threshold of CorrectLink.
	clink bandsel-5g-rssi-threshold	Configures the 5G preferred RSSI threshold of CorrectLink.
	clink bandsel-5g-client-threshold	Configures the 5 GHz preferred load threshold of CorrectLink.
	clink max-fails	Configures the rate-limiting attempt threshold of CorrectLink.

1.4.1 Configuring CorrectLink

Configuration Effect

- Enable CorrectLink to identify and steer STAs based on CorrectLink rules.

Notes

- If APs in an area belong to different ACs and do not join the virtual AC group, CorrectLink takes effect only between APs connected to the same AC, but not across ACs. That is, CorrectLink ensures only STA steering between APs connected to the same AC.
- If CorrectLink is configured only on some AP groups, it takes effect only between APs in these AP groups. CorrectLink does not guarantee STA steering on the entire network.

Configuring CorrectLink

Enable CorrectLink in global configuration mode or AP group configuration mode.

Command	**clink enable**
Parameter Description	N/A
Defaults	Disabled
Command Mode	Global configuration mode or AP group configuration mode
Usage Guide	• When this function takes effect in global configuration mode, it is applied to all AP groups. • When configuring a single AP group, run the **show running** command to display the configuration of the AP group.

	When the function is configured in global configuration mode, it cannot be configured on a single AP group. If you need to configure the function on a single AP group, first disable the function globally.

Configuring the Remote Association RSSI Difference Threshold of CorrectLink

When the difference between the uplink associated RSSI of the client and the detected highest RSSI is greater than the configured remote association RSSI difference threshold, the STA is a remote one and cannot access the AP.

Command	**clink rssi-delta-threshold** *thrd*
Parameter Description	*thrd*: Indicates the remote association RSSI difference threshold. The value range is from 1 to 100.
Defaults	10
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Load Balancing Determination Threshold of CorrectLink

With load balancing enabled, when the load of STAs associated with the AP exceeds the load balancing determination threshold, the AC determines whether to perform load balancing.

Command	**clink lb-client-threshold** *thrd*
Parameter Description	*thrd*: Indicates the STA access threshold for dynamic load balancing. The value range is from 1 to 100.
Defaults	30
Command Mode	Global configuration mode
Usage Guide	The AC determines whether to perform load balancing when the number of STAs associated with an AP exceeds the configured load balancing threshold.

Configuring the Load Balancing Difference Threshold of CorrectLink

When a STA detects APs, if the difference between an AP's RSSI and the detected highest RSSI is less than the remote association RSSI threshold, the set of these APs is called an APset.

Command	**clink lb-client-delta-threshold** *thrd*
Parameter Description	*thrd*: Indicates the load balancing difference threshold. The value range is from 1 to 100.
Defaults	5
Command Mode	Global configuration mode
Usage Guide	Once the load balancing difference threshold is set, if the number of STAs associated with an AP surpasses the load balancing threshold and there is an APset containing an AP not currently linked to the STA, with fewer STAs connected to it compared to the current AP by at least the specified load balancing difference threshold, an imbalance is identified. This triggers the suppression of STA access to rectify the load imbalance issue.

Configuring the 5G Preferred RSSI Threshold of CorrectLink

- After the 5 GHz preferred RSSI threshold is configured, if a WLAN supports both the 2.4 GHz and 5 GHz frequency bands and the RSSI of 5 GHz signals is greater than the threshold on the WLAN, the STA cannot be associated with the WLAN in the 2.4 GHz frequency band.

Command	**clink bandsel-5g-rssi-threshold** *thrd*
Parameter Description	*thrd*: Indicates the 5 GHz preferred RSSI threshold. The value range is from 1 to 100.
Defaults	20
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the 5 GHz Preferred Load Threshold of CorrectLink

- After the 5 GHz preferred load threshold is configured, if a WLAN supports both the 2.4 GHz and 5 GHz frequency bands and load of 5 GHz signals is less than the threshold on the WLAN, the STA cannot be associated with the WLAN in the 2.4 GHz frequency band.

Command	**clink bandsel-5g-client-threshold** *thrd*
Parameter Description	*thrd*: Indicates the 5 GHz preferred load threshold. The value range is from 1 to 100.
Defaults	100
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Rate-limiting Attempt Threshold of CorrectLink

- After a STA is rate-limited for a certain number of times equal to the rate-limiting attempt threshold, stop rate limiting to guarantee access experience of the STA.

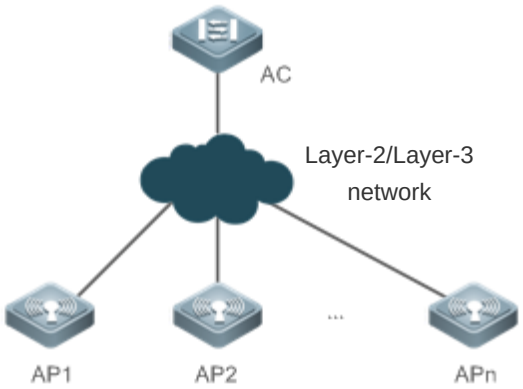
Command	**clink max-fails** *thrd*
Parameter Description	*thrd*: Indicates the rate-limiting attempt threshold. The value range is from 1 to 100.
Defaults	2
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Enabling CorrectLink and Configuring the Remote Association RSSI Difference Threshold as 7

Scenario **Figure 1-4**	
Configuration Steps	● Enable the global CorrectLink function on the AC. ● Configure the remote association RSSI difference threshold as 7 on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# clink enable`
	`Hostname(config)# clink rssi-delta-threshold 7`

Verification	Display the configuration after CorrectLink is enabled. ● Run the **show running** command to display the configuration.

	`Hostname# show running-config`
	`!`
	`clink enable`
	`clink rssi-delta-threshold 7`
	`!`

1.5 Monitoring

Displaying

Command	Description
show clink result	Displays the CorrectLink result.
show clink statistic	Displays CorrectLink statistics.
show clink probe	Displays probe information.

1 Configuring FSS

1.1 Overview

With Frequency Spectrum Scanning (FSS) enabled, an access point (AP) can operate in FSS mode and act as a wireless frequency spectrum sensor that is responsible for collecting and analyzing non-802.11 wireless signal frequency spectrum and sends results of frequency spectrum analysis to the frequency spectrum analysis server. Then the frequency spectrum analysis server shows frequency spectrum analysis results in intuitive forms such as graphic, list, and alarm.

FSS is used with RG-SNC to achieve frequency spectrum analysis.

1.2 Applications

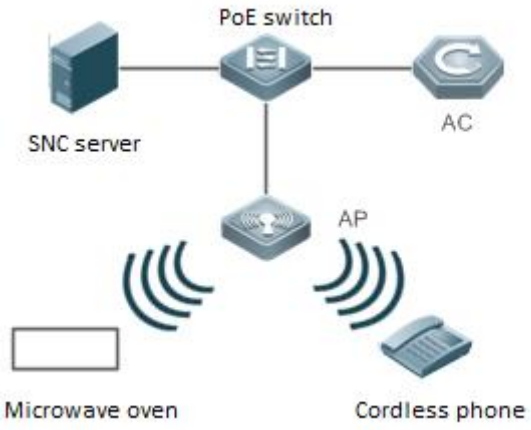
Application	Description
Providing Frequency Spectrum Analysis	FSS is used with RG-SNC to achieve frequency spectrum analysis.

1.2.1 Providing Frequency Spectrum Analysis with RG-SNC

Scenario

Non-802.11 wireless interference devices such as microwave ovens and cordless phones are deployed in the RF environment.

Figure 1-1



Remarks	A. RG-SNC is installed on the SNC server. B. The AC and AP constitute the wireless Fit AP system. C. There are interferences from microwave ovens and cordless phones in the RF environment.

Deployment

- Enable the frequency spectrum analysis function on the AC.
- Establish a connection between RG-SNC and the AC.

1.3 Features

Basic Concepts

Video Bridge Interference

A working video bridge may generate wireless signals that interfere with WLAN transmission. FSS enables an AP to recognize and send the video bridge interferences to RG-SNC for analysis.

Microwave Oven Interference

A working microwave oven may generate microwave leakage that interferes with WLAN transmission. FSS enables an AP to recognize and send the microwave interferences to RG-SNC for analysis.

Cordless Phone Interference

A working cordless phone may generate wireless signals that interfere with WLAN transmission. FSS enables an AP to recognize and send the cordless phone interferences to RG-SNC for analysis.

Bluetooth Interference

A working Bluetooth device may generate wireless signals that interfere with WLAN transmission. FSS enables an AP to recognize and send the Bluetooth device interferences to RG-SNC for analysis.

Continuous Wave

A continuous wave may generate wireless signals that interfere with WLAN transmission. FSS enables an AP to recognize and send the continuous wave interferences to RG-SNC for analysis.

Scanning Precision

The scanning precision indicates the serial number of the scanned characteristic waveform which is then determined as a specific interference source. Typically, a higher scanning precision leads to a higher probability of correct determination.

Scanning Duration

When performing frequency spectrum scanning, an AP cannot provide wireless services. The system regularly switches between wireless services and frequency spectrum scanning to balance them. A longer scanning duration leads to a higher probability of locating interferences.

Overview

Feature	Description

SNC Connecting to the AC for Frequency Spectrum Analysis	Through interaction between the SNC server and AC, non-802.11 interference sources such as microwave ovens, cordless phones, and Bluetooth devices are recognized in a wireless environment.

1.3.1 SNC Connecting to the AC for Frequency Spectrum Analysis

An AP recognizes non-802.11 interference sources such as microwave ovens, cordless phones, and Bluetooth devices in a wireless environment and sends them to RG-SNC for sort-out and display through the connection channel established between the AC and RG-SNC.

Working Principle

Frequency spectrum analysis is achieved through the interaction and SOCKET connection between the SNC server and AC. After FSS is enabled, an AP regularly collects non-802.11 interference information in the RF environment and performs Fast Fourier Transform (FFT). Then the AP classifies the information for processing, recognizes and sends specific interference sources to RG-SNC through the agreed protocol. After receiving information, RG-SNC sorts out and displays the interference information in various ways. For details, refer to the user manual for RG-SNC.

1.4 Configuration

Configuration	Description and Command	
Enabling FSS	⚠ (Mandatory) It is used to enable FSS.	
	spectral enable	Enable FSS.
Configuring the FSS Interference Recognition Precision	⚠ Optional.	
	spectral stability	Configures the interference recognition precision for FSS.
Configuring the FSS Duration	⚠ Optional.	
	spectral period	Configures the FSS duration.

1.4.1 Enabling FSS

Configuration Effect

- Enable FSS.

Notes

- FSS is enabled in the AP configuration mode.

Configuration Steps

↘ **Enabling FSS**

- (Mandatory) Run the **spectral enable** command to enable or disable FSS in AP configuration mode.
- Enable FSS for the target AP that is FSS-capable in AP configuration mode.

Command	**spectral enable**
Parameter Description	N/A
Defaults	By default, FSS is disabled.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

Run the **show ap-config running** *ap-name* command to verify that the FSS precision is configured on the target AP.

Configuration Example

Enabling FSS

Configuration Steps	• Enable FSS for a specified AP.

	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP0001`
	`Hostname(config-ap)# spectral enable`
	`Hostname(config)# end`

Verification	Run the **show ap-config running** *ap-name* command to verify that FSS is enabled on the target AP.
	`Hostname# show ap-config running AP0001` `spectral enable`

Common Errors

This function is configured in all-AP configuration mode.

1.4.2 Configuring the FSS Interference Recognition Precision

Configuration Effect

- Configure the recognition precision of non-802.11 frequency spectrum signals where a larger value leads to a higher precision.

Notes

- FSS must be enabled.

Configuration Steps

Configuring the FSS Interference Recognition Precision

- Optional
- The scanning precision is configured in AP configuration mode, and the default value can be used.

Command	**spectral stability** { **bth** *bth-num* | **bts** *bts-num* | **cph** *cph-num* | **cwa** *cwa-num* | **mwo** *mwo-num* | **vbr** *vbr-num* }
Parameter Description	*bth-num*: Configures the precision of Bluetooth recognition. The value range is 1 to 4 and the default value is 1. *bts-num*: Configures the precision of Bluetooth earphone recognition. The value range is 1 to 2 and the default value is 1. *cph-num*: Configures the precision of cordless phone recognition. The value range is 3 to 5 and the default value is 5. *cwa-num*: Configures the precision of continuous wave recognition. The value range is 4 to 10 and the default value is 8. *mwo-num*: Configures the precision of microwave recognition. The value range is 1 to 5 and the default value is 1. *vbr-num:* Configures the precision of video bridge recognition. The value range is 1 to 5 and the default value is 5.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	If there are no special requirements, the default value can be used.

Verification

Run the **show ap-config running** *ap-name* command to verify that the FSS precision is configured on the target AP.

Configuration Example

Configuring the FSS Precision

Configuration Steps	● Configure the FSS precision for video bridges as 2.

	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP0001`
	`Hostname(config-ap)# spectral enable`
	`Hostname(config-ap)# spectral stability vbr 2`
	`Hostname(config)# end`

Verification	Run the **show ap-config running** *ap-name* command to verify the FSS precision on the target AP.

	`Hostname# show ap-config running AP0001`
	`spectral enable`
	`spectral stability vbr 2`

Common Errors

- FSS is not enabled.
- This function is configured in all-AP configuration mode.

1.4.3 Configuring the FSS Duration

Configuration Effect

A longer scanning duration leads to a higher probability of locating interferences but greater influence on normal communication of the AP.

Notes

FSS must be enabled.

Configuring the FSS Duration

- Optional
- The scanning duration is configured in AP configuration mode. If there are no special requirements, the default value can be used.

Command	**spectral period** *num*
Parameter Description	*num*: Indicates the FSS duration. The value range is from 1 ms to 100 ms and the default value is 5 ms.
Defaults	5
Command Mode	AP configuration mode
Usage Guide	If there are no special requirements, the default value can be used.

Verification

Run the **show ap-config running** *ap-name* command to verify that the FSS duration is configured on the target AP.

Configuration Example

Configuring the FSS Duration as 10 μs

Configuration Steps	- Configure the FSS duration as 10 μs.

	Hostname# configure terminal Hostname(config)# ap-config AP0001 Hostname(config-ap)# spectral enable Hostname(config-ap)# spectral period 10 Hostname(config)# end
Verification	Run the **show ap-config running** *ap-name* command to verify the FSS duration configured on the target AP.
	Hostname# show ap-config running AP0001 spectral enable spectral period 10

Common Errors

- FSS is not enabled.
- This command is configured in all-AP configuration mode.

1 Configuring Wireless Location

1.1 Overview

The wireless location function uses IEEE 802.11-compliant wireless signals to locate stations (STAs). It is supported on all 802.11 a/b/g/n-compliant STAs, such as portable computers, Mobile Units (MUs), and special Radio Frequency Identifications (RFIDs, referred to as TAGs). By analyzing and summarizing IEEE 802.11-compliant wireless signals sent from these STAs, this function can be used to locate STAs through software on the location server and to intuitively display STA locations in the form of maps, tables, or reports.

Wireless location has the following characteristics:

- Indoor and outdoor deployment
- Two algorithms supported: Received Signal Strength Indication (RSSI) and Time Difference of Arrival (TDOA) location
- Location of two types of devices: 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

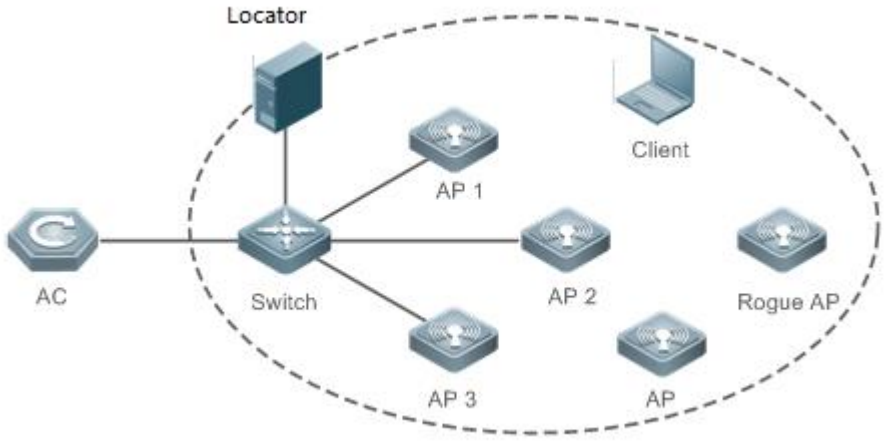
Scenario

On a WLAN in Fit AP mode where Access Points (APs) are managed uniformly by the Access Controller (AC), the IEEE 802.11-compliant STAs can be located by a location server or locator, under the condition that the following special requirements are met:

- Direct access is required between APs and the locator. Therefore, ensure that the ping operation between them is successful.
- The APs must support wireless location.
- It is necessary to deploy three APs for accurate location.

The following figure shows an example where AP 1, AP 2 and AP 3 can communicate with the locator. Each AP sends received STA information to the locator which then works out the STA locations.

Figure 1-1



Deployment

- The AC is responsible for wireless location configuration management and delivery.
- The APs are responsible for collecting STA information and sending the information 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 performed by the administrator.

1.3 Features

Basic Concepts

A location system contains three parts: target or source to be located, receiver, and 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, IEEE 802.11-complicant wireless STAs which regularly transmit wireless signals.

Receiver

The receiver can be a 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 types of graphic programs.

Features

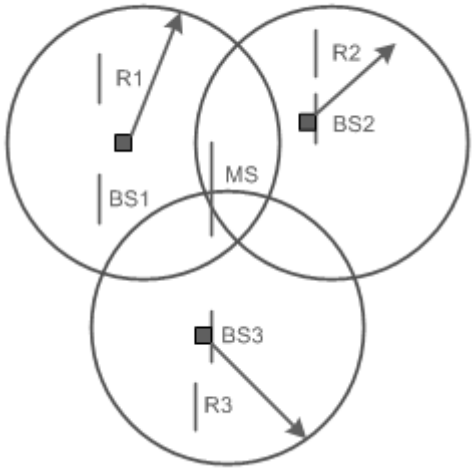
Feature	Description
Wireless Location	Enable wireless location for APs.

1.3.1 Wireless Location

Working Principle

Based on the RSSI from an MU received by a base station (BS) and the channel transmission model, the distance between the MU and BS can be estimated, indicated by the letter d. 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 errors are the multipath effect generated during signal transmission and the shadow effect generated during obstacle crossing. More accurate location can be achieved in an 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 Basic Functions of Wireless Location	(Mandatory) It is used to enable wireless location.	
	wlocation enable	Enables wireless location 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.
	(Optional) It is used to optimize wireless location transmission.	
	wlocation compound enable	Enables the WL aggregation.
	wlocation send-mu-time	Configures the interval for sending MU location information on a specified AP.

Configuration	Description and Command	
	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 Basic Functions of Wireless Location

Configuration Effect

Enable wireless location to provide basic location services.

Notes

N/A

Configuration Steps

↘ Enabling Wireless Location on an AP

- Mandatory.
- Run the **wlocation enable** command to enable wireless location on an AP.
- On wireless networks where the location function is required, you are advised to enable the wireless location function on all APs that meet location conditions.

Command	**wlocation enable** [**radio** *radio-id*]
Parameter Description	*radio-id*: Indicates that the wireless location function is enabled on the designated RF interface.
Defaults	By default, wireless location is disabled.
Command Mode	AP configuration mode
Usage Guide	If **radio** is not configured, the wireless location function is enabled or disabled for the AP. If **radio** is configured, the wireless location function is enabled or disabled for a specified radio of the AP.

↘ Configuring the IP Address and Interface Number for the Locator

- Mandatory.
- The interface number has a default value depending on the configuration of a specific locator. You can modify the interface number of the locator on the device synchronously.
- The wireless location function of an AP is used only with the locator. Therefore, the IP address and interface number of the locator needs to be configured to guarantee communication with the AP.
- After the correct IP address and interface number are configured, the AP can normally enable the wireless location function.

Command	**wlocation ae-ip** *ip-address*
Parameter	*ip-address*: Indicates the IP address of the locator.

Description	
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	N/A

Command	**wlocation ae-port** *port*
Parameter Description	*port*: Indicates the interface number of the locator.
Defaults	The default interface number is 12092.
Command Mode	AP configuration mode
Usage Guide	N/A

Enabling MU or TAG Location

- Mandatory.
- To enable wireless location on an AP, you need to enable wireless location 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	AP configuration mode
Usage Guide	Both MU and TAG locations can be enabled simultaneously.

Command	**wlocation tag enable**
Parameter Description	N/A
Defaults	By default, TAG location is disabled.
Command Mode	AP configuration mode
Usage Guide	Both MU and TAG locations can be enabled simultaneously.

Configuring Aggregated Transmission of Wireless Location Information

- Optional.
- Enable aggregated transmission of wireless location information to reduce the network overhead for transmitting location information through information aggregation.

Command	**wlocation compound enable**
Parameter Description	N/A
Defaults	By default, this function is enabled.

Command Mode	AP configuration mode on the AC
Usage Guide	N/A

Configuring the Interval for Sending MU or TAG Location Information

- Optional.
- It is used to adjust the interval for sending location information. Unless otherwise specified, the default value is used.
- In the scenarios where a lot of STAs need to be located, reduce the interval to avoid information loss. (An AP can cache 500 to 700 pieces of location information.)

Command	**wlocation send-mu-time** *interval*
Parameter Description	*interval*: Indicates the interval for sending MU location information on a specified AP. The value range is from 100 to 5000, in milliseconds.
Defaults	The default interval is 300 ms.
Command Mode	AP configuration mode
Usage Guide	N/A

Command	**wlocation send-tag-time** *interval*
Parameter Description	*interval*: Indicates the interval for sending TAG location information on a specified AP. The value range is from 100 to 5000, in milliseconds.
Defaults	The default interval is 300 ms.
Command Mode	AP configuration mode
Usage Guide	N/A

Enabling MU Location Report

- Optional.
- The locator does not communicate with APs which directly send collected MU location information, for example, through the NAT network. Unless otherwise specified, the default value is used.

Command	**wlocation mu report enable**
Parameter Description	N/A
Defaults	By default, this function is disabled.
Command Mode	AP configuration mode
Usage Guide	After this function is enabled, the AP will skip the protocol handshake process with the locator, which is applicable to NAT scenarios.

Enabling TAG Location Report

- Optional.

- After this function is enabled, the AP only sends summarized location information to the locator, reducing the bandwidth and traffic consumed by large amounts of location information that may affect user experience.

Command	wlocation tag report enable
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	Enabling the function of summarizing MU location information will reduce the bandwidth occupied by location information. This function is only applicable to scenarios where a locator of a specified vendor (such as Ruijie) is deployed on a network.

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.

Command	wlocation mu report reduce enable
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	Enable the function of simplifying MU location information to reduce traffic. This function is used only when the deployed locator is developed by Ruijie Networks.

Filtering Beacon Packets Sent by APs

- Optional.
- Use this command when traffic bandwidth needs to be reduced.

Command	wlocation ignore beacon enable
Parameter Description	N/A
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	Enable the function of filtering Beacon packets sent by APs to reduce bandwidth.

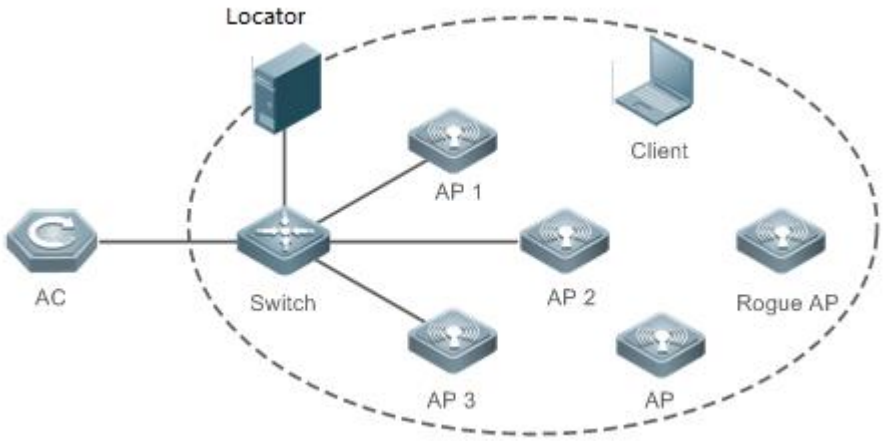
Verification

On a network, enable STAs to send wireless packets.

- Verify that APs receive wireless location information.
- Verify that the locator receives location information.

Configuration Example

Enabling Wireless Location

Scenario **Figure 1-3**	
Configuration Steps	● Enable wireless location. ● Configure the IP address of the locator. ● Enable MU location as required. ● Enable TAG location as required. ● Assuming that AP1 is named **ap1-1**, run the following commands to enable wireless location for this AP.

AP1	`Hostname# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# ap-config ap1-1`
	`Hostname(ap-config)# wlocation enable`
	`Hostname(ap-config)# wlocation ae-ip 1.1.1.1`
	`Hostname(ap-config)# wlocation mu enable`
	`Hostname(ap-config)# wlocation tag enable`

Verification	● Run the **show ap-config** command to display the configuration of each AP and verify the wireless location configuration. ● Assuming that AP1 is named **ap1-1**, run the following commands to verify the wireless location configuration for this AP.

AP1	`Hostname# show ap-config running`
	`ap-config ap1-1`
	`wlocation enable`
	`wlocation ae-ip 1.1.1.1`
	`wlocation mu enable`

	wlocation tag enable

Common Errors

N/A

1 Configuring Smart Antennas

1.1 Overview

A smart antenna, also known as an adaptive antenna array, is composed of the antenna array, beam forming network, and beam forming algorithm. By adopting algorithms meeting certain criteria, the smart antenna adjusts the weighted amplitude and phase of each array signal and thereby adjusts the radiation pattern of the antenna array to enhance required signals and suppress interference signals.

Smart antennas can solve network interference and signal fading, and increase system capacity.

Smart antennas are typically used in a complex environment where a lot of obstacles or certain interferences exist.

1.2 Applications

Application	Description
Obstacle Environment	Obstacles exist in a wireless network environment.

1.2.1 Obstacle Environment

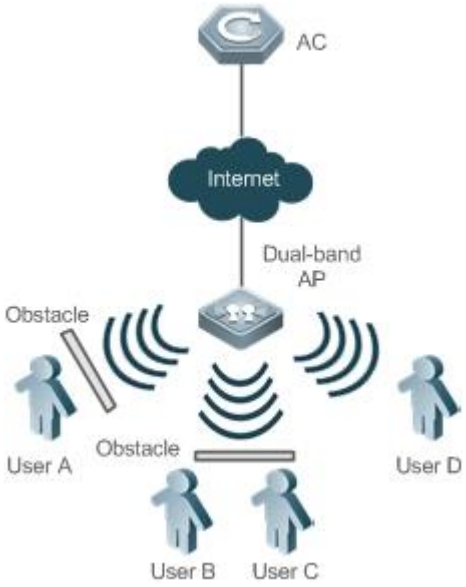
Scenario

Obstacles, such as load bearing walls and glass windows, exist in a wireless network environment.

The networking topology is shown in the following figure, where:

- Stations (STAs) are evenly distributed around the access point (AP).
- The smart antenna function is enabled by default.
- Obstacles exist between STAs and the AP.

Figure 1-1 Networking Topology of Smart Antennas



Deployment

- The AP performs downlink wireless packet training and collects data required by smart antennas.
- Based on the collected data for smart antennas, the AP executes the beam forming algorithm to compute an antenna path for each STA.
- The AP sends data to each STA along the computed path.

1.3 Features

Basic Concepts

Smart Antenna

Based on beamwidth, antennas are classified into omni-directional and directional antennas. Omni-directional antennas usually provide a wide coverage but a narrow distance, which is contrary to directional antennas. Smart antennas combine advantages of both omni-directional and directional antennas. They can cover 360 degrees of horizontal radiation with a longer distance at each angle.

Wireless Packet Training

Smart antennas sample STA communication packets for training. When a STA transmits downlink traffic, the direction of packet transmission is changed by setting the transmitting antennas. The associated AP extracts the rates of packet loss in different antenna directions for evaluation, and finally computes a path for antenna transmission based on the beam forming algorithm.

Overview

Feature	Description
Smart Antenna Path Selection	Finds an optimal transmission path between the AP and STAs for better user experience.

1.3.1 Smart Antenna Path Selection

With the smart antenna is enabled, the AP can find an optimal transmission path for each STA.

Working Principle

Through downlink packet training and sampling by an AP, an optimal transmission path can be found to avoid interferences and obstacles

1.4 Configuration

Configuration	Description and Command	
Configuring Antennas	⚠ Optional.	
	smartant enable radio	Configures smart antennas.

1.4.1 Configuring Smart Antennas

Configuration Effect

- Configure the smart antenna status.

Notes

- If the AP does not support smart antennas, the configuration cannot take effect.

Configuration Steps

Configuring the Smart Antenna for a Specified Radio of a Specified AP

- Optional.
- The smart antenna is configured on per-radio and per-AP basis.

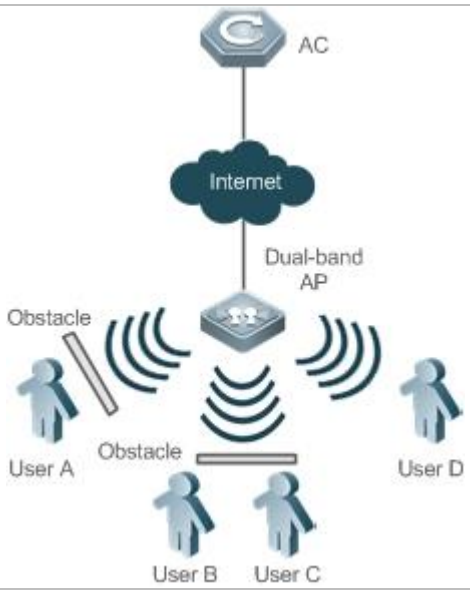
Command	**[no] smartant enable radio** *radio-id*
Parameter Description	*radio-id*: Indicates the ID of a radio to be configured with the smart antenna.
Defaults	By default, the smart antenna is enabled.
Command Mode	AP configuration mode
Usage Guide	This command is used to enable or disable the smart antenna function. For smart antenna-incapable devices, the configuration cannot take effect.

Verification

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

Configuration Example

Configuring the Smart Antenna for a Specified Radio of a Specified AP

Scenario **Figure 1-2**	

Configuration Steps	● Configure the smart antenna for a specified radio of a specified AP.
	Hostname# configure terminal Hostname(config)# ap-config ap320 Hostname(config-ap)# smartant enable radio 1
Verification	After the smart antenna function is configured for the specified radio of the specified AP, check the configuration through the following ways. ● Run the **show running** *ap-name* command to display the configuration. Because the smart antenna is enabled by default, no configuration will not be displayed. When the smart antenna function is disabled, the disabled configuration can be displayed.
	Hostname# show ap-config running ap320 ! ap-config ap320 ... ... no smartant enable radio 2 ... ... !

1.5 Monitoring

N/A

Configuring WLAN 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 on 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 obtained only by intended 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
- 802.11r This amendment specifies the extensions to IEEE Std 802.11-2007 for wireless local area networks (WLANs) providing mechanisms for fast basic service set (BSS) transition

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 home 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.
802.11r Fast Roaming	Fast BSS Transition (FT) is defined to reduce network delay caused by roaming.

1.2.1 WEP Encryption

Scenario

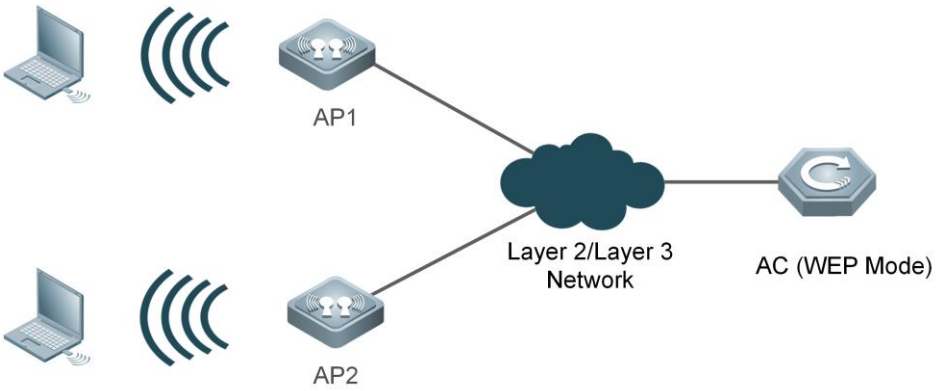
On a small WLAN that has a lower requirement for security, WEP encryption can be used.

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 clients cannot go online.

Figure 1-1 shows the scenario of static WEP encryption.

Figure 1-1



Deployment

- Configure a WLAN on the AC.
- Configure WEP encryption in WLAN security configuration mode.
- Deliver the WLAN configuration to APs.

1.2.2 PSK Access Authentication

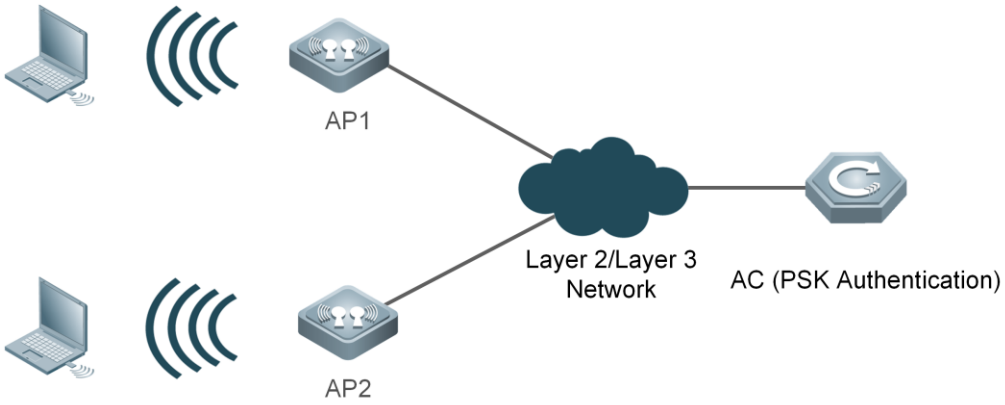
Scenario

Small and medium-sized enterprise networks or home users can use the Wi-Fi Protected Access (WPA) or WPA2 standard to enhance WLAN security. The simplest method is using pre-shared key authentication (WPA-PSK and WPA2-PSK, respectively). In this case, WPA is similar to Wired Equivalent Privacy (WEP), and can achieve higher security based on IEEE 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 access device to establish connection and communication. No additional authentication server is required.

Figure 1-2 shows the scenario of PSK authentication.

Figure 1-2



Deployment

- Configure a WLAN on the AC.
- Configure PSK authentication in WLAN security configuration mode.
- Deliver the WLAN configuration to APs.
- Use this authentication with web authentication to support web-based authentication and accounting.

1.2.3 802.1X Access Authentication

Scenario

In a scenario that has a higher requirement for security, 802.1X authentication can be used.

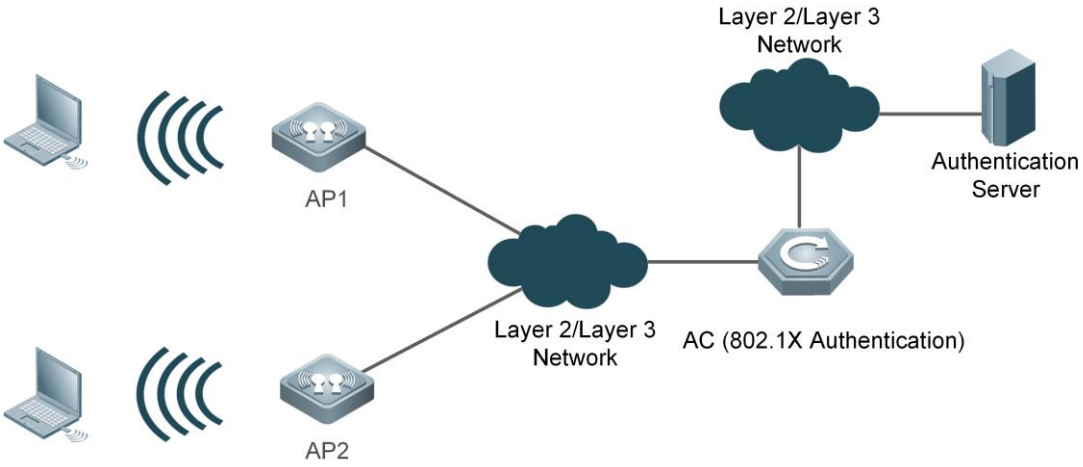
802.1X is a port-based network access control protocol. This authentication mode is used to authenticate and control STAs at the port level of WLAN access devices. STAs connected to the ports can access WLAN resources if they pass the authentication. Otherwise, the STAs cannot access WLAN resources.

Authentication client software needs to be installed on terminals to perform 802.1X authentication. However, in some cases, some client devices cannot be installed with the software, for example, wireless printers. For the sake of network management and security, although these client devices have no 802.1X authentication client software, administrators need to control the access of these client devices. MAC Authentication Bypass (MAB) provides a solution for this application.

After the MAB function is deployed for a WLAN, a wireless device can automatically detect the MAC address of a connected client device and use the MAC address to initiate a request to the authentication server.

Figure 1-3 shows the scenario of 802.1X authentication.

Figure 1-3



Deployment

- Configure a WLAN on the AC.
- Configure an authentication server on the AC.
- Configure 802.1X authentication in WLAN security configuration mode.
- Deliver the WLAN configuration to APs.

1.2.4 802.11r Fast Roaming

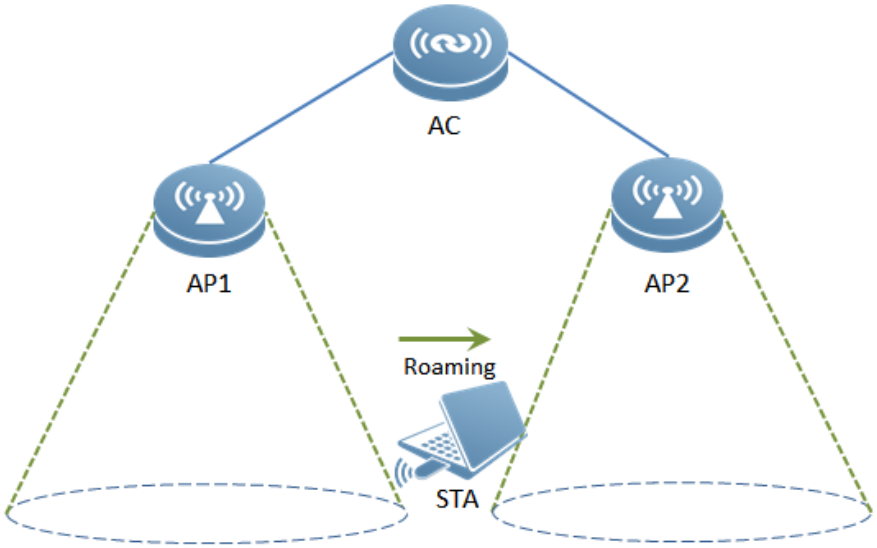
Scenario

For applications that are sensitive to network delay, such as Voice over Wi-Fi and video, minimizing roaming authentication time is crucial. The 802.11r standard defines the FT roaming mode. In this mode, 802.1X authentication and the 4-way handshake are not required, thereby reducing the roaming handoff time.

FT provides the Over-the-Air and Over-the-DS methods. Currently, only Over-the-Air is supported. When Over-the-Air is used, STAs directly connect to a new AP for authentication in roaming scenarios.

Figure 1-4 shows the Over-the-Air scenario.

Figure 1-4



Deployment

- Configure a WLAN on the AC.
- In WLAN security configuration mode, set the authentication mode to RSN, Authentication and Key Management (AKM) to PSK or 802.1X, and encryption mode to AES.
- Deliver the WLAN configuration to APs.
- Simulate a scenario in which a STA roams from AP1 to AP2. If the 802.11r function is enabled, the STA directly connects to AP2 for FT authentication.

1.3 Features

Basic Concepts

WPA

Wi-Fi Protected Access (WPA) is a wireless security draft defined by the Wi-Fi Alliance. The IEEE 802.11i standard is compatible with this draft.

RSN

The IEEE 802.11i standard defines the concept of Robust Security Network (RSN): and makes many improvements against various defects of the WEP encryption mechanism. RSN is equivalent to WPA2 launched by the Wi-Fi Alliance in terms of functions.

TKIP

The Temporal Key Integrity Protocol (TKIP) enhances security compared with WEP. TKIP provides per-packet key mixing, message integrity check, and key re-generation mechanism, thereby eliminating 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 next-generation encryption standard AES.

CCMP

Counter Mode with CBC-MAC Protocol (CCMP) uses AES, which is more secure 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 require users to enter authentication information, and STAs and APs negotiate temporary PMKs.

Overview

Feature	Description
Link Authentication	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 Authentication

Link authentication refers to 802.11 authentication, which is a low-level authentication mechanism. Link authentication is performed when a STA associates with an AP according to the 802.11 standard, which is earlier than access authentication. Before a STA accesses a WLAN, 802.11 authentication must be performed. 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 link-layer authentication modes:

- 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. That is, if the authentication mode is set to open-system authentication, all STAs that request authentication can pass the authentication.

The process of open-system link authentication is as follows:

Step 1: An STA requests authentication. The STA sends an authentication request that contains the ID (typically 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 two-way authentication.

Figure 1-5



Shared-Key Link Authentication

Shared-key link authentication is another authentication mechanism in addition to 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 open-system link authentication is available in all the other modes.

The process of shared-key link authentication is as follows:

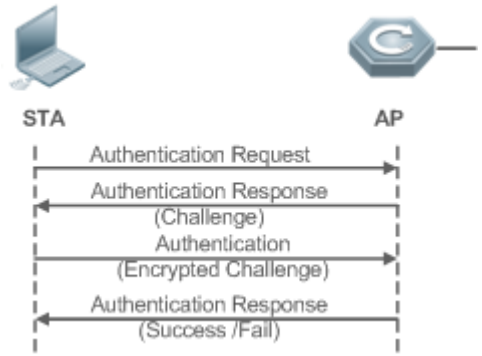
Step 1: A STA sends an authentication request to an AP.

Step 2: The AP generates a Challenge packet (a random string) 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 1-6



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 modes:

- PSK access authentication
- 802.1X access authentication

Working Principle

PSK Access Authentication

Pre-shared Key (PSK) is an 802.11i authentication mode that performs authentication with pre-defined static keys. This authentication mode 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 mode is used to authenticate and control the STAs at the port level of WLAN access devices. STAs connected to the ports can access resources on a WLAN if they pass the authentication. Otherwise, the STAs cannot access resources on the WLAN.

A WLAN system with the 802.1X authentication function must provide the following elements to implement port-based authentication and authorization for network access control:

- Authentication client

Authentication client is typically installed on the STA. To access a WLAN, a user needs to activate the client program and enter the username and password. Then, the client program sends a connection request.

- Authenticator

An authenticator is an AP or a communication device functioning as an AP. It is responsible for uploading and delivering 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 identity information (username and password), and delivers the port enabling or disabling status 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. In this case, client devices do not need to install the client software.

1.3.3 Wireless Data Encryption

Compared with a wired network, a wireless network is prone to higher 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 threats to WLAN access security.

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 protect the privacy of data exchanged between authorized users on a WLAN and prevent the data from being stolen.

WEP uses the RC4 algorithm to protect data privacy and implements authentication by using a shared key. WEP does not specify a key management scheme. Typically, keys are configured and maintained manually. WEP that does not provide a key distribution mechanism is called manual WEP or static WEP.

A WEP key contains 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 actual implementation, the 104-bit WEP keys are widely used to replace the 40-bit WEP keys. WEP using 104-bit keys is called WEP-104. Although WEP-104 increases the security of WEP encryption, WEP encryption is prone to security risks due to limitations of the RC4 encryption algorithm and manually configured keys. WEP encryption cannot guarantee the confidentiality and integrity of data or implement access authentication.

TKIP Encryption

Temporal Key Integrity Protocol (TKIP) is a temporary transitional solution created by the IEEE 802.11 organization for fixing the WEP encryption mechanism. Similar to WEP encryption, TKIP encryption also uses the RC4 algorithm. However, compared with WEP encryption, TKIP encryption can provide more secure 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 anti-replay function.

AES Encryption

The Counter Mode with CBC-MAC Protocol (AES-CCMP) is the most advanced wireless security protocol for the public.

The IEEE 802.11i standard requires that CCMP be used to provide four security services, namely, authentication, confidentiality, integrity, and anti-replay services. CCMP uses the 128-bit AES to guarantee confidentiality and uses CBC-MAC to ensure data integrity and perform 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 next-generation encryption technology that replaces WEP and provides more powerful security protection for WLANs.

The IEEE 802.11r standard requires that CCMP be used to encrypt EAPOL packets. Therefore, before enabling the 802.11r function, configure the AES-CCMP encryption mode.

1.3.4 Management Frame Encryption

Wireless management frames, such as authentication, de-authentication, association, disassociation, beacon, and probe frames, are transmitted using plaintext in the air. In this case, these frames may be used by unauthorized devices to attack wireless clients associated with APs. The Protected Management Frame (PMF) defined by the IEEE 802.11w standard 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 on air interfaces. 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 rogue 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 Wi-Fi encryption protocol released by the Wi-Fi Alliance. WPA3 is available in WPA3-Enterprise, WPA3-Personal, and OWE editions. WPA3-Enterprise provides WPA3-Enterprise only and WPA3-Enterprise 192-bit modes.

- WPA3-Personal Edition

Compared with WPA2-Personal, WPA3-Personal introduces Simultaneous Authentication of Equals (SAE) for management frame authentication. When a STA attempts to connect to the device enabled with WPA3-Personal, SAE adds an SAE handshake before the original WPA/WPA2-PSK 4-way handshake to dynamically negotiate a pairwise master key (PMK) using random variables and passwords through calculation. The PMK is used for the WPA/WPA2-PSK 4-way handshake, enhancing access security for WPA3.

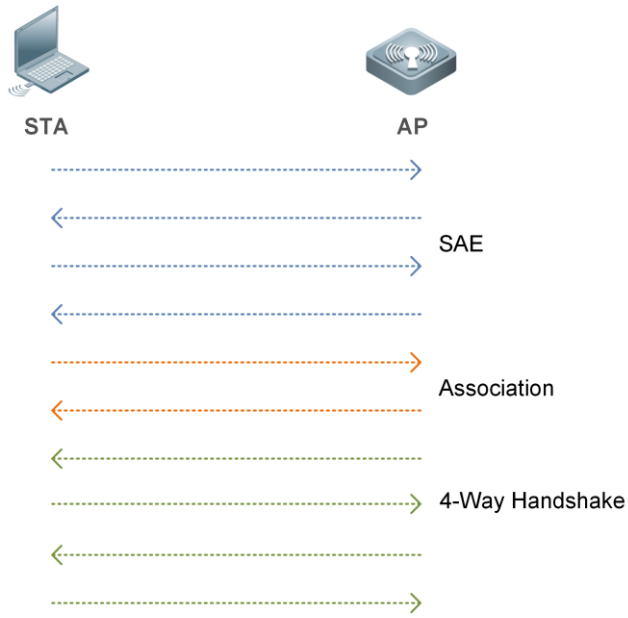
There are three WPA3 SAE encryption options available:

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 1-7 Mutual Authentication of WPA3-Personal Edition



- WPA3-Enterprise Edition

Based on WPA2-Enterprise, the WPA3-Enterprise only mode introduces management frame protection. That is, 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 air interfaces to enhance security.

An enhanced encryption suite is used for 4-way handshake in the WPA3-Enterprise 192-bit mode.

  - This suite increases the key length from 128 bits to 192 bits, enhancing data protection.
  - 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 replace CCMP, thereby protecting multicast management frames.

- OWE Authentication

OWE authentication, also known as Enhanced Open network authentication, does not require users to enter authentication information. The packets exchanged between STAs and APs are still encrypted, providing a certain level of privacy and defense against packet sniffing. In a scenario where OWE authentication is enabled, STAs that do not support OWE authentication are allowed to access in open authentication mode.

1.4 Configuration

Configuration	Description and Command	
Configuring Static WEP	(Mandatory) It is used to enable static WEP encryption.	
	wlansec	Enters the security configuration mode of the specified WLAN.
	security static-wep-key encryption	Enables static WEP for a WLAN and configures a static WEP key.

Configuration	Description and Command	
	(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 for 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 anti-jitter time in WEB authentication.	
	authtimeout forbidcount	Configures the association forbidding count after 4-way handshake key interaction fails.
	authtimeout forbidtime	Configures the association forbidding interval after 4-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

Configuration	Description and Command	
		key negotiation packets.
	webauth prevent-jitter	Configures the anti-jitter time of web authentication.
Configuring 802.11r	**security rsn dot11r enable**	Enables the 802.11r fast roaming protocol.
	security rsn dot11r reassoc-timeout	Modifies the 802.11r re-association timeout duration.
Configuring Management Frame Encryption	**security pmf** { **disable | mandatory** | **optional** }	Configures management frame encryption.
Configuring WPA3 Authentication	**security wpa3 mode**	Sets the WPA3 authentication mode.
	security wpa3 personal passphrase	Sets a key for WPA3-Personal authentication.
	security wpa3 personal pwe	Sets a WPA SAE encryption mode.
	security wpa3 enhanced-open paired-wlan	Sets an equivalent WLAN for WPA3 authentication in enhanced-open mode.
Configuring the Response Delay Mode for Authentication Packets	**rsna lazy-response enable**	Enables or disables the response delay for authentication packets.
	rsna lazy-response time	Configures the response delay timeout for authentication packets.
Configuring PPSK	**security sta-psk enable**	Configures Private Pre-Shared Key (PPSK).
	security sta-psk external enable	Configures PPSK external authentication.

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 can be configured only when static WEP encryption is enabled.
- In the security configuration mode of a WLAN, static WEP encryption cannot be configured together with other authentication and encryption modes.
- 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 AC.

Command	**security static-wep-key encryption** *key-length* { **ascii** | **hex** } *key-index key*
Parameter Description	*key-length*: Indicates the key length, which can be 40 bits or 104 bits. **ascii**: Specifies that the WEP key is in ASCII format. **hex**: Specifies that the WEP key is in hexadecimal format.

	key-index: Indicates the key index. The range is from 1 to 4. *key*: Indicates key data.
Defaults	Static WEP is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to configure a static WEP key and enable static WEP encryption. This command can be configured repeatedly, but only the last configuration takes effect. The key length must be the same as the value of 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.
- Enable static WEP encryption in security configuration mode on the AC first.
- The link authentication mode can be configured only after static WEP encryption is enabled. After configuring the shared-key link authentication mode, set the link authentication mode to shared-key link authentication on the STA. Otherwise, the STA cannot access the WLAN.

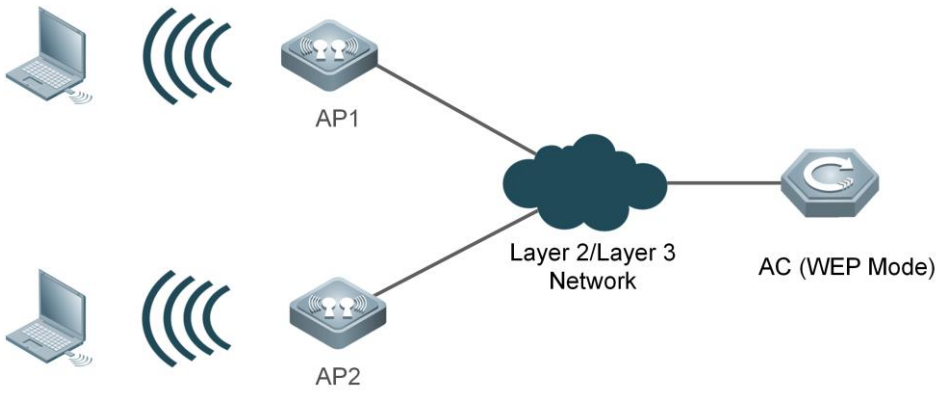
Command	**security static-wep-key authentication** { **open** | **share-key** }
Parameter Description	**open**: Configures open-system link authentication. **share-key**: Configures shared-key link authentication.
Defaults	A STA accesses a WLAN by using open-system link authentication.
Command Mode	WLAN security configuration mode
Usage Guide	Configure the link authentication mode after configuring a static WEP key. The link authentication mode can be configured only for static WEP encryption, but cannot configured for other security configuration modes.

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 Shared-Key Link Authentication for WLAN 1

Scenario **Figure 1-8**	 In a fit AP environment, configure WLAN 1 on the AC and configure the security policies as follows:

	1. Enable static WEP encryption. 2. Configure shared-key link authentication.
Configuration Steps	● Enter 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.

AC	`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** *wlan_id* command to check whether the configuration takes effect.

AC	`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 key length specified in the command.
- Static WEP encryption is configured for multiple WLANs.
- The link authentication mode is configured before static WEP encryption 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 configuration mode of a WLAN, WPA authentication and WEP authentication cannot be configured simultaneously.

Configuration Steps

↘ Configuring WPA Authentication

- Mandatory.
- Enable WPA authentication in WLAN security configuration mode on the AC.

Command	**security wpa** { **enable** | **disable** }

Parameter Description	**enable**: Enables WPA authentication. **disable**: Disables WPA authentication.
Defaults	WPA authentication is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode for WPA authentication can be configured only when 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 only 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 WPA Authentication

- Mandatory.
- Enable WPA authentication in WLAN security configuration mode on the AC first.
- The encryption mode of WPA authentication can be configured only when WPA authentication is enabled. The AES and TKIP encryption modes can be enabled simultaneously in the security configuration mode of a WLAN. After an encryption mode is configured for a WLAN, communication data of a STA that accesses 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 for WPA authentication. **disable**: Disables the encryption mode for WPA authentication.
Defaults	No encryption mode is configured.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable an encryption mode for WPA authentication, which can be AES or TKIP. The AES and TKIP encryption modes can be enabled simultaneously in the security configuration mode of a WLAN.

Configuring the Access Authentication Mode for WPA authentication

- Mandatory.
- Enable WPA authentication in WLAN security configuration mode on the AC first.
- The access authentication mode can be configured only when WPA authentication is enabled. Only one access authentication mode can be enabled in the security configuration mode of a WLAN. 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 for WPA authentication. **disable**: Disables the access authentication mode for WPA authentication.

Defaults	No access authentication mode is configured.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only when WPA authentication is enabled. Only one access authentication mode can be enabled in the security configuration mode of a WLAN.

Configuring a Shared Key for WPA Authentication

- Optional. It must be configured when WPA PSK authentication is enabled.
- Enable WPA PSK authentication in WLAN security configuration mode on the AC first.

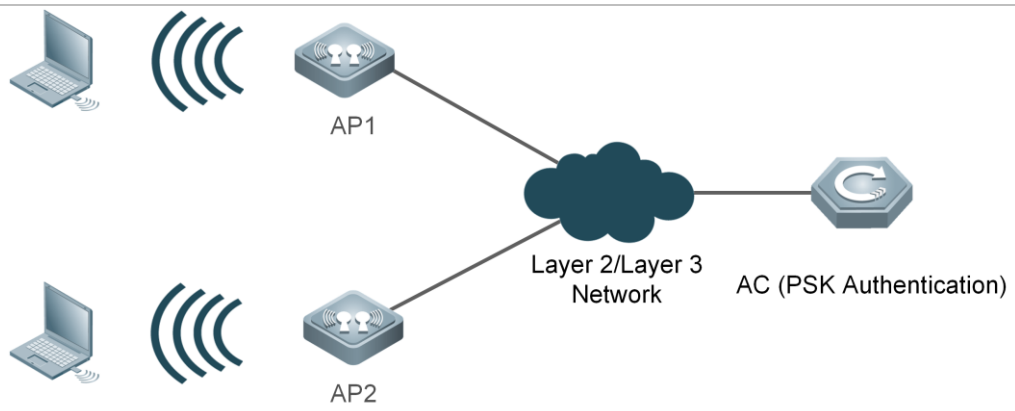
Command	**security wpa akm psk set-key** { **ascii** [**0** | **7**] *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is in ASCII format. **0**: Optional. Configures a cleartext password. **7**: Optional. Configures a ciphertext password. The password must meet encryption specifications. *ascii-key*: Indicates a key in ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is in hexadecimal format. *hex-key*: Indicates a key in 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. ● If you configure a cleartext password by using the **security wpa akm psk set-key ascii 0** *ascii-key* command, the configured password is converted into and saved as a ciphertext password, and command is displayed as **security wpa akm psk set-key ascii 7** *ascii-key*. ● If you configure a cleartext password by using the **security wpa akm psk set-key ascii** *ascii-key* command, the configured password is not converted into and saved as a ciphertext password.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring WPA PSK Authentication

Scenario **Figure 1-9**	

	In a fit AP environment, configure the security policies on the AC as follows: 1. Configure the WPA PSK authentication mode for WLANs 1, 2, and 3. 2. Configure the AES encryption mode for WLANs 1, 2, and 3. 3. Set the shared password to 12345678 for WLAN 1, the shared cleartext password to password@123 for WLAN 2, and the shared ciphertext password to $10$27c$8Wu2G++qd4mBlYzO$ for WLAN 3.
Configuration Steps	1. Enter the security configuration mode of WLANs 1, 2, and 3. 2. Enable the WPA authentication mode. 3. Set the data encryption mode of WPA authentication to AES. 4. Set the access authentication mode of WPA authentication to PSK. 5. Set the PSK password to 12345678 for WLAN 1, the PSK cleartext password to password@123 for WLAN 2, and the PSK ciphertext password to $10$27c$8Wu2G++qd4mBlYzO$ for WLAN 3.

AC	`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`
	`Hostname(config-wlansec)#exit`
	`Hostname(config)#wlansec 2`
	`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 0 password@123`
	`Hostname(config-wlansec)#exit`
	`Hostname(config)#wlansec 3`
	`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 7`
	`$10$27c$8Wu2G++qd4mBlYzO$`
	`Hostname(config-wlansec)#exit`

Verification	● Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

AC	`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`
	`!`
	`wlansec 2`

	security wpa enable security wpa ciphers aes enable security wpa akm psk enable security wpa akm psk set-key ascii 7 $10$27c$8Wu2G++qd4mBlYzO$! wlansec 3 security wpa enable security wpa ciphers aes enable security wpa akm psk enable security wpa akm psk set-key ascii 7 $10$27c$8Wu2G++qd4mBlYzO$!

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 is shorter than 8 characters or longer 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 configuration mode of a WLAN, RSN authentication and WEP authentication cannot be configured simultaneously.

Configuration Steps

↘ Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC.

Command	**security rsn** { **enable** | **disable** }

Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode for RSN authentication can be configured only when 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 only 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.
- Enable RSN authentication in WLAN security configuration mode on the AC first.
- The encryption mode for RSN authentication can be configured only when RSN authentication is enabled. The AES and TKIP encryption modes can be enabled simultaneously in the security configuration mode of a WLAN. After an encryption mode is configured for a WLAN, communication data between a STA that accesses 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.
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 simultaneously in the security configuration mode of a WLAN.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC first.
- The access authentication mode for RSN authentication can be configured only when RSN authentication is enabled. Only one access authentication mode can be enabled in the security configuration mode of a WLAN. 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.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only when RSN authentication is enabled. Only one access authentication mode can be enabled in the security configuration mode of a WLAN.

Configuring a Shared Key for RSN Authentication

- Optional. It must be configured when RSN PSK authentication is enabled.
- Enable RSN PSK authentication in WLAN security configuration mode on the AC first.

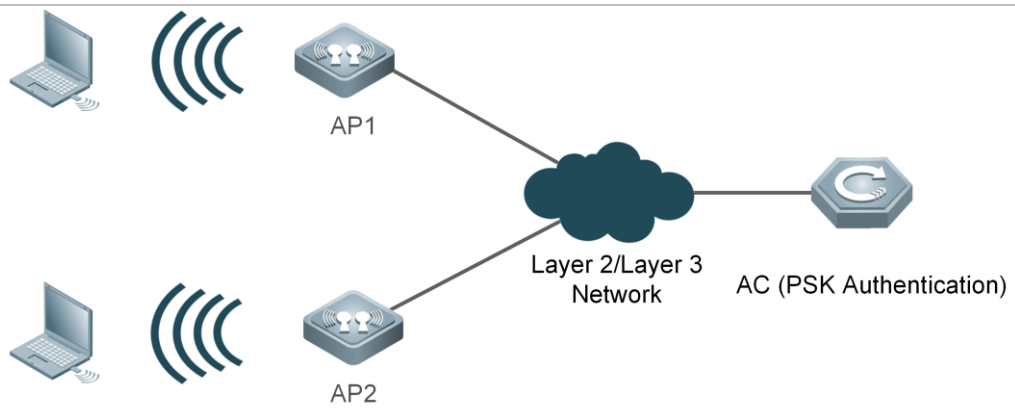
Command	**security rsn akm psk set-key** { **ascii** [**0** | **7**] *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is in ASCII format. **0**: Optional. Configures a cleartext password. **7**: Optional. Configures a ciphertext password. The password must meet encryption specifications. *ascii-key*: Indicates a key in ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is in hexadecimal format. *hex-key*: Indicates a key in 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. ● If you configure a cleartext password by using the **security rsn akm psk set-key ascii 0** *ascii-key* command, the configured password is converted into and saved as a ciphertext password, and command is displayed as **security rsn akm psk set-key ascii 7** *ascii-key*. ● If you configure a cleartext password by using the **security rsn akm psk set-key ascii** *ascii-key* command, the configured password is not converted into and saved as a ciphertext password.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Configuring RSN PSK Authentication

Scenario **Figure 1-10**	

	In a fit AP environment, configure the security policies on the AC as follows: 1. Configure the RSN PSK authentication mode for WLANs 1, 2, and 3. 2. Configure the AES encryption mode for WLANs 1, 2, and 3. 3. Set the shared password to 12345678 for WLAN 1, the shared cleartext password to password@123 for WLAN 2, and the shared ciphertext password to $10$27c$8Wu2G++qd4mBlYzO$ for WLAN 3.
Configuration Steps	1. Enter the security configuration mode of WLANs 1, 2, and 3. 2. Enable the RSN authentication mode. 3. Set the data encryption mode of RSN authentication to AES. 4. Set the access authentication mode of RSN authentication to PSK. 5. Set the PSK password to 12345678 for WLAN 1, the PSK cleartext password to password@123 for WLAN 2, and the PSK ciphertext password to $10$27c$8Wu2G++qd4mBlYzO$ for WLAN 3.

AC	`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)#exit`
	`Hostname(config)#wlansec 2`
	`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 0 password@123`
	`Hostname(config-wlansec)#exit`
	`Hostname(config)#wlansec 3`
	`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 7`
	`$10$27c$8Wu2G++qd4mBlYzO$`
	`Hostname(config-wlansec)#exit`

Verification	● Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

AC	`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`
	`!`
	`wlansec 2`

```
 security rsn enable
 security rsn ciphers aes enable
 security rsn akm psk enable
 security rsn akm psk set-key ascii 7 $10$27c$8Wu2G++qd4mBlYzO$
!
wlansec 3
 security rsn enable
 security rsn ciphers aes enable
 security rsn akm psk enable
 security rsn akm psk set-key ascii 7 $10$27c$8Wu2G++qd4mBlYzO$
!
```

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 is shorter than 8 characters or longer 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 the security configuration 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 AC.
- 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.

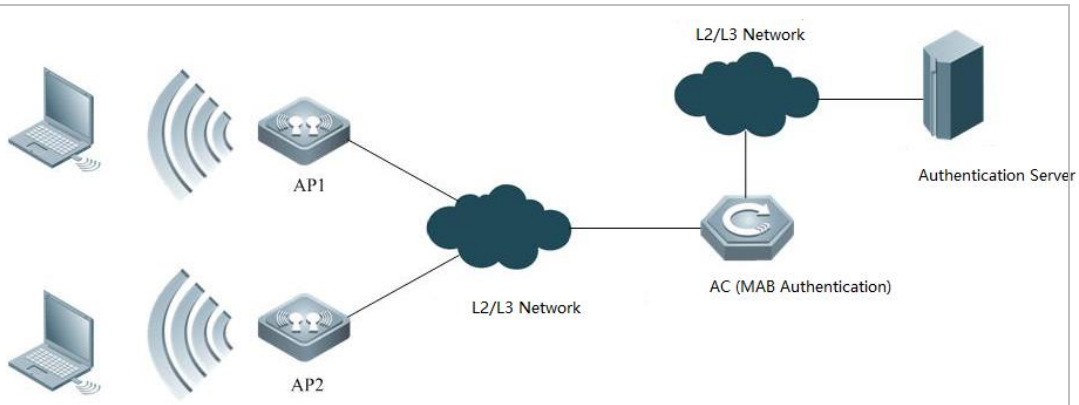
Command	[**no**] **dot1x-mab**
Parameter Description	**no**: Disables MAB authentication.
Defaults	MAB authentication is not configured.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable MAB authentication. MAB authentication can be used together with PSK access 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 1-11	 In fit AP mode, configure the security policy of WLAN 1 on the AC as follows: 1. Configure MAB authentication.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable MAB authentication.
AC	`Hostname(config)#wlansec 1` `Hostname(config-wlansec)#dot1x-mab`
Verification	● Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

AC	`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 anti-jitter time in web authentication.

Notes

- Key interaction parameters take effect only in PSK or 802.1X authentication.
- The anti-jitter time in web authentication can be configured only when web authentication is enabled.

Configuration Steps

↘ Configuring Key Interaction Parameters

- Optional. Typically, you do not need to configure key interaction parameters. You are advised to set the packet re-transmission count and timeout duration to large values for a poor WLAN environment.
- Enable PSK or 802.1X authentication in WLAN security configuration mode on the AC first.

Command	**authtimeout** { **forbidcount** *count* | **forbidtime** *time* | **groupcount** *count* | **grouptime** *timeout* | **paircount** *count* | **pairtime** *timeout* }
Parameter Description	**forbidcount** *count*: Configures the association forbidding count after 4-way handshake key interaction fails. **forbidtime** *time*: Configures the association forbidding interval after 4-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 4-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 1000 ms. The default unicast key negotiation packet re-transmission count is 4. The default timeout duration of unicast key negotiation packets is 1000 ms.
Command Mode	WLAN security configuration mode
Usage Guide	Key interaction parameters take effect only in PSK or 802.1X authentication.

↘ Configuring the Anti-jitter Time of Web Authentication

- Optional. The default anti-jitter time of web authentication is 300 seconds. You can configure the anti-jitter time based on actual requirements or disable the anti-jitter function of web authentication by setting the time to 0 seconds.

- Enable web authentication in WLAN security configuration mode on the AC first.

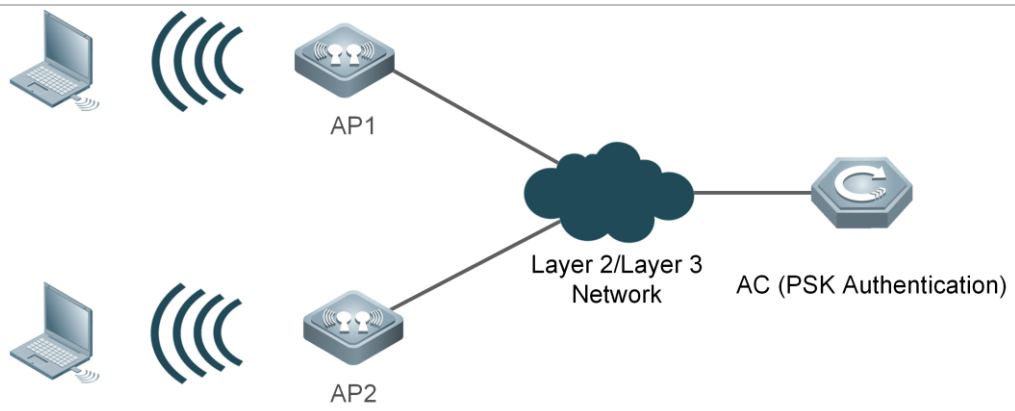
Command	**webauth prevent-jitter** *timeout*
Parameter Description	*timeout*: Configures the anti-jitter time of web authentication, in seconds. The range is from 0 to 86400. (The anti-jitter function of web authentication is disabled when this parameter is set to 0).
Defaults	The default anti-jitter time of web authentication is 300 seconds.
Command Mode	WLAN security configuration mode
Usage Guide	The anti-jitter time of web authentication can be configured only when web authentication is enabled.

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Setting the RSN PSK+Web Authentication Mode, the Unicast Key Negotiation Packet Re-transmission Count to 5 and the Anti-jitter Time of Web Authentication to 900 Seconds for WLAN 1

Scenario **Figure 1-12**	 In fit AP mode, configure the security policies of WLAN 1 on the AC as follows: 1. Configure RSN PSK authentication. 2. Enable web authentication.
Configuration Steps	● Enter 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 anti-jitter time of web authentication to 900 seconds.

AC	`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** *wlan_id* command to check whether the configuration takes effect.
AC	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 anti-jitter time of web authentication is configured before web authentication is enabled.

1.4.6 Configuring 802.11r

Whether this function is supported depends on the actual product version.

Configuration Effect

- If the 802.11r function is enabled for a WLAN, the 802.1X authentication and 4-way handshake are not required during fast roaming, thereby reducing network delay caused by roaming.

Notes

- 802.11r can be independently configured for RSN.
- The 802.11r function can be enabled for RSN only when the following conditions are met:
  - RSN authentication is enabled.
  - WPA authentication is disabled, that is, WPA and RSN cannot be enabled simultaneously.
  - The access authentication mode AKM is configured as PSK or 802.1X.
  - AES encryption is enabled.
  - TKIP encryption is disabled, that is, AES and TKIP cannot be enabled simultaneously.
- For roaming between an AC and a VAC and between ACs with the same SSID, the WLAN ID that corresponds to the SSID must be the same.
- The 802.1X LEAP authentication mode is not supported.
- 802.11r can be configured independently for RSN and WPA3.

Configuration Steps

Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode can be configured for RSN authentication only when 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 only 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.
- Enable RSN authentication in WLAN security configuration mode on the AC first.
- The encryption mode for RSN authentication can be configured only when RSN authentication is enabled. The AES and TKIP encryption modes can be enabled simultaneously in the security configuration mode of a WLAN. After an 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.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to enable the AES or TKIP encryption mode for RSN authentication. To use the 802.11r function, enable AES encryption first. In addition, TKIP encryption must be disabled. TKIP encryption is disabled by default.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC first.
- The access authentication mode for RSN authentication can be configured only when RSN authentication is enabled. Only one access authentication mode can be enabled in the security configuration mode of a WLAN. 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	**psk**: Sets the access authentication mode to pre-shared key authentication.

Description	**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.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only when RSN authentication is enabled. Only one access authentication mode can be enabled in the security configuration mode of a WLAN.

Configuring a Shared Key for RSN Authentication

- Optional. It must be configured when RSN PSK authentication is enabled.
- Enable RSN PSK authentication in WLAN security configuration mode on the AC first.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is in ASCII format. *ascii-key*: Indicates a key in ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is in hexadecimal format. *hex-key*: Indicates a key in 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 ASCII format consists of 8 to 63 characters. A key in hexadecimal format consists of 64 characters.

Enabling 802.11r for RSN

- Optional. This command is used to enable 802.11r fast roaming.

Command	**security rsn dot11r {disable | enable}**
Parameter Description	**disable**: Disables 802.11r fast roaming. **enable**: Enables 802.11r fast roaming.
Defaults	The 802.11r fast roaming function is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	When the 802.11r function is enabled, a judgment is made based on the conditions. For details about the conditions, see Notes. This command is valid only when AKM (802.1X or PSK) is enabled. This command is valid only when AES encryption is enabled.

Modifying 802.11r Re-association Timeout Duration

- Optional. This command is used to configure the re-association timeout duration (that is, the maximum interval for a client to send a re-association request after client authentication is completed).

Command	**security rsn dot11r reassoc-timeout** *timeout*
Parameter	*timeout:* Re-association timeout duration, in seconds. The range is from 1 to 120.

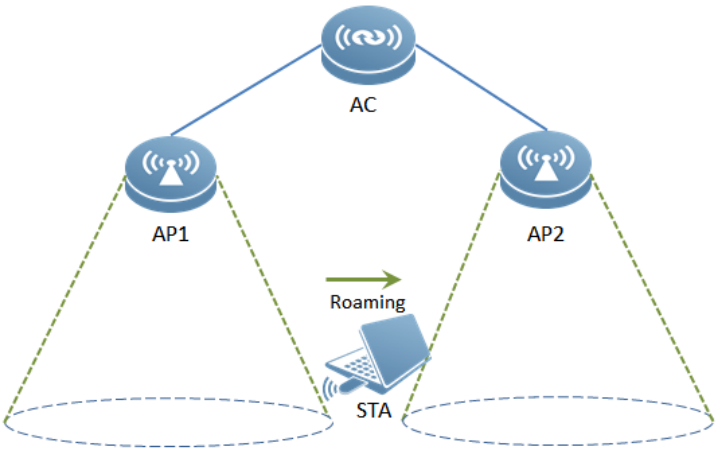
Description	
Defaults	The default re-association timeout duration is 20 seconds.
Command Mode	WLAN security configuration mode
Usage Guide	This command takes effect only when the 802.11r function is enabled. If the client does not initiate a re-association request within the re-association timeout duration, the roaming is stopped.

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 and Enabling 802.11r for WLAN 1

Scenario **Figure 1-13**	 In a fit AP environment, configure the following security policies for WLAN 1 on the AC: 1. Configure RSN PSK authentication. 2. Configure AES encryption. 3. Configure the shared key 12345678. 4. Enable 802.11r.
Configuration Steps	● Enter 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. ● Set the PSK key to 12345678. ● Enable 802.11r.

AC	`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 rsn dot11r enable`
Verification	● Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

AC	`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 rsn dot11r enable`
	`!`

Common Errors

- 802.11r is enabled when RSN authentication is disabled or both RSN and WPA are enabled.
- 802.11r is enabled when the access authentication mode (802.1X or PSK) is not configured.
- 802.11r is enabled when AES encryption is disabled or both AES encryption and TKIP encryption are enabled.
- The SSIDs of ACs are the same but the WLAN IDs are different, causing FT roaming failures.

1.4.7 Configuring Management Frame Encryption

Configuration Effect

- Transmit partial management frames through air interfaces in ciphertext.

Notes

- Only WPA2 supports management frame encryption. If the WLAN uses the open, WEP-40, WEP-104, or AES/TKIP (WPA authentication) mode for encryption, the management frame encryption function cannot be enabled.
- The operating systems of some STAs do not support management frame encryption.

Configuration Steps

↘ Configuring RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC.

Command	**security rsn** { **enable** | **disable** }
Parameter Description	**enable**: Enables RSN authentication. **disable**: Disables RSN authentication.
Defaults	RSN authentication is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	The encryption mode and access authentication mode for RSN authentication can be configured only

	when 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 only 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.
- Enable RSN authentication in WLAN security configuration mode on the AC first.
- The encryption mode for RSN authentication can be configured only when RSN authentication is enabled. The AES and TKIP encryption modes can be enabled simultaneously in the security configuration mode of a WLAN. 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.
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 simultaneously in the security configuration mode of a WLAN.

Configuring the Access Authentication Mode for RSN Authentication

- Mandatory.
- Enable RSN authentication in WLAN security configuration mode on the AC first.
- The access authentication mode for RSN authentication can be configured only when RSN authentication is enabled. Only one access authentication mode can be enabled in the security configuration mode of a WLAN. 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.
Command Mode	WLAN security configuration mode
Usage Guide	The access authentication mode can be configured only when RSN authentication is enabled. Only one access authentication mode can be enabled in the security configuration mode of a WLAN.

Configuring a Shared Key for RSN Authentication

- Optional. It must be configured when RSN PSK authentication is enabled.
- Enable RSN PSK authentication in WLAN security configuration mode on the AC first.

Command	**security rsn akm psk set-key** { **ascii** *ascii-key* | **hex** *hex-key* }
Parameter Description	**ascii**: Specifies that the PSK key is in ASCII format. *ascii-key*: Indicates a key in ASCII format, consisting of 8 to 63 ASCII characters. **hex**: Specifies that the PSK key is in hexadecimal format. *hex-key*: Indicates a key in 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 ASCII format consists of 8 to 63 characters. A key in hexadecimal format consists of 64 characters.

Enabling Management Frame Encryption

- Mandatory.
- Enable management frame encryption on an AC.
- Management frame encryption can be configured only when RSN authentication is enabled.

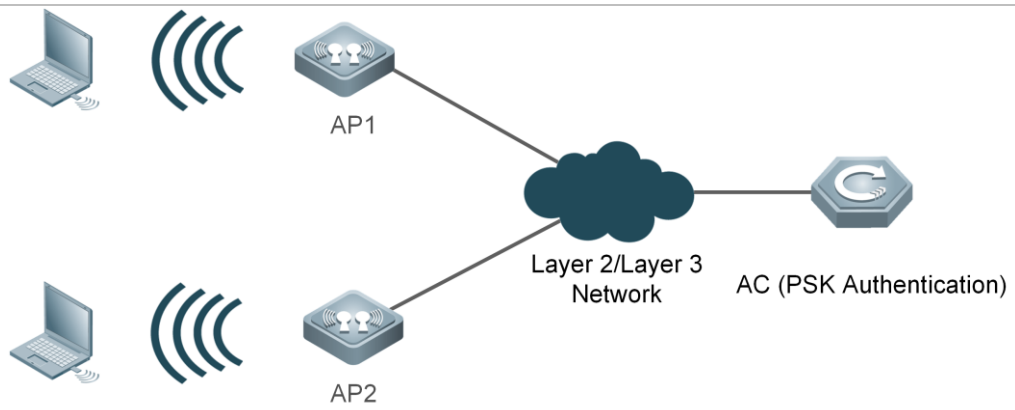
Command	**security pmf** { **disable | mandatory** | **optional** }
Parameter Description	**disable**: Disables management frame encryption. **mandatory**: Sets management frame encryption to mandatory mode. In this mode, STAs must support management frame encryption. **optional**: Sets management frame encryption to optional mode. In this mode, STAs do not need to support management frame encryption.
Defaults	Management frame encryption is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Verification

Run the **show running-config** | **begin wlansec** *wlan_id* command to check whether the configuration takes effect.

Configuration Example

Enabling RSN PSK Authentication and Management Frame Encryption for WLAN 1

Scenario **Figure 1-14**	 In a fit AP environment, configure the following security policies for WLAN 1 on the AC: 1. Configure RSN PSK authentication. 2. Enable management frame encryption.
Configuration Steps	● Enter 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. ● Set the PSK key to 12345678. ● Enable management frame encryption.

AC	`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** *wlan_id* command to check whether the configuration takes effect.

AC	`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

- If an encryption mode is configured for WPA, management frame encryption cannot be enabled.
- If a STA cannot go online when **mandatory** is configured, the STA may not support management frame encryption.

1.4.8 Configuring WPA3 Authentication

Whether this function is supported depends on the actual product version.

Configuration Effect

- Enable the WPA3 authentication mode on a WLAN.

Notes

- WPA3-Personal can only be used with WPA2 for authentication. The encryption mode for WPA2 must be AES.
- WPA3-Enterprise cannot be used with WPA2 simultaneously.
- WPA3 relies on management frame encryption. Therefore, enable management frame encryption before configuring WPA3.
- WPA3 cannot be used with 802.11r.
- In scenarios where WPA3-Enterprise authentication is used, STAs that do not support WPA3 cannot access a WLAN.

Configuration Steps

Enabling Management Frame Encryption

- Mandatory.
- Configure it in WLAN security configuration mode on an AC.

Command	**security pmf** { **disable** | **optional** | **mandatory** }
Parameter Description	**disable**: Disables management frame encryption. **mandatory**: Sets management frame encryption to mandatory mode. In this mode, STAs must support management frame encryption. **optional**: Sets management frame encryption to optional mode. In this mode, STAs do not need to support management frame encryption.
Defaults	Management frame encryption is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	● When WPA3-Enterprise or OWE is used for authentication, management frame encryption must be set to mandatory mode. Otherwise, STAs may fail to access a WLAN. ● When WPA3 and WPA2 are used for authentication simultaneously, if management frame encryption is set to optional mode, STAs that support WPA2 or SAE are allowed to access a WLAN; if management frame encryption is set to mandatory mode, only WPA2 STAs that support PMF are allowed to access a WLAN.

Configuring the WPA3 Mode

- Mandatory.
- Configure the WPA3 mode in WLAN security configuration mode.

Command	**security wpa3 mode** { **enhanced-open** | **enterprise** [**ccmp-128** | **gcmp-256**] | **none** | **personal** }
Parameter	**enhanced-open**: Configures OWE authentication.

Description	**enterprise**: If the **ccmp-128** and **gcmp-256** parameters are not configured, GCMP-256 is used for encryption by default. **enterprise ccmp-128**: Configures CCMP-128 for WPA3-Enterprise authentication. **enterprise gcmp-256**: Configures GCMP-256 for WPA3-Enterprise authentication. **none**: Disables the WPA3 function. **personal**: Configures WPA3-Personal authentication**.**
Defaults	WPA3 is disabled.
Command Mode	WLAN security configuration mode
Usage Guide	● WPA3-Personal can only be used with WPA2 for authentication. The encryption mode for WPA2 must be AES. ● WPA3-Enterprise cannot be used with WPA2simultaneously. ● WPA3 cannot be used with WPA simultaneously.

Configuring an Equivalent WLAN for OWE Authentication

- Optional. It must be used together with OWE authentication. After configuration, if a STA supports OWE authentication, it accesses the WLAN using OWE authentication; if a STA does not support OWE authentication, it accesses the WLAN using open authentication.

Command	**security wpa3 enhanced-open paired-wlan** { **none** | *wlan-id* }
Parameter Description	**none**: Clears the configuration of equivalent WLANs for OWE authentication. *wlan-id*: Indicates the WLAN ID of the equivalent WLAN to be configured with OWE authentication.
Defaults	N/A
Command Mode	WLAN security configuration mode
Usage Guide	● To enable OWE authentication, an equivalent WLAN using the open authentication mode must be configured first. ● The QoS, schedule, and other configurations of the equivalent WLAN to be configured with OWE authentication must be consistent with those for OWE authentication. ● After configuring an equivalent WLAN, set the OWE authentication signal to the hidden mode. ● An equivalent WLAN can be associated with only one OWE authentication signal.

Configuring an Authentication Key for WPA3-Personal

- The configuration is optional when WPA2 PSK authentication is enabled. It is mandatory only when WPA3-Personal authentication is enabled.
- If WPA3-Personal and WPA2 are used for authentication simultaneously, all STAs use the WPA2 PSK key to access a WLAN.

Command	**security wpa3 personal passphrase** { **none** | **ascii** [**0** | **7**] *password* }
Parameter Description	**none**: Clears the key. **ascii**: Configures an ASCII password. **0**: Optional. Configures a cleartext password. **7**: Optional. Configures a ciphertext password. The password must meet encryption specifications. *password*: Indicates a key in ASCII format, consisting of 8 to 63 ASCII characters.
Defaults	No key is configured for WPA3-Personal authentication.

Command Mode	WLAN security configuration mode
Usage Guide	● If you configure a cleartext password by using the **security wpa3 personal passphrase ascii 0** *password* command, the configured password is converted into and saved as a ciphertext password, and command is displayed as **security wpa3 personal passphrase ascii 7** *password*. ● If you configure a cleartext password by using the **security wpa3 personal passphrase ascii** ***password*** command, the configured password is not converted into and saved as a ciphertext password.

Configuring WPA3 SAE Encryption Mode

- Mandatory.
- In WLAN security configuration mode, set the WPA3 SAE encryption mode.

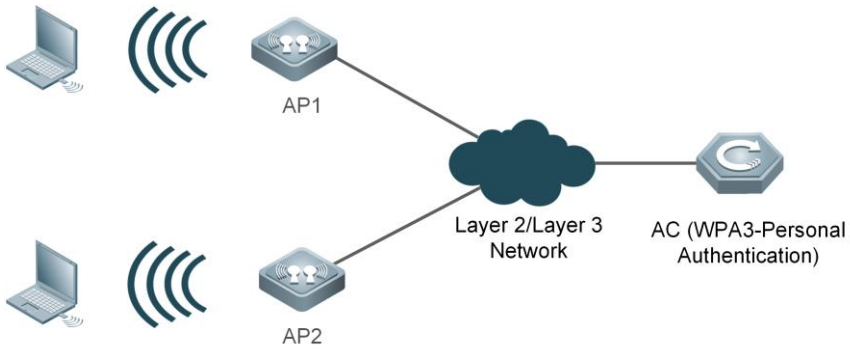
Command	**security wpa3 personal pwe** { **hnp** | **h2e** | **both** }
Parameter Description	**hnp**: Configures HnP for WPA3 SAE authentication. **h2e**: Configures H2E for WPA3 SAE authentication. **both**: Configures both HnP and H2E for WPA3 SAE authentication. The device determines the encryption 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

Scenario **Figure 1-15**	 In a fit AP environment, configure the following security policies for WLAN 1 on the AC: 1. Configure the WPA3-Personal authentication mode (RSN disabled) for WLANs 1, 2, and 3.

	2. Set the shared password to 12345678 for WLAN 1, the shared cleartext password to password@123 for WLAN 2, and the shared ciphertext password to $10$27c$8Wu2G++qd4mBlYzO$ for WLAN 3. 3. Set the WPA3 SAE encryption mode to H2E for WLAN 1.
Configuration Steps	1. Enter the security configuration mode of WLANs 1, 2, and 3. 2. Enable management frame encryption. 3. Set the WPA3 password to 12345678 for WLAN 1, the cleartext password to password@123 for WLAN 2, and the ciphertext password to $10$27c$8Wu2G++qd4mBlYzO$ for WLAN 3. 4. Set the WPA3 mode to Personal. 5. Set the WPA3 SAE encryption mode to H2E.

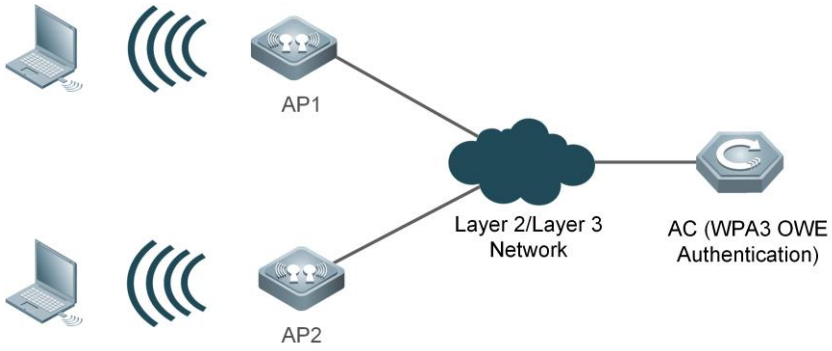
AC	`Hostname(config)#wlansec 1`
	`Hostname(config-wlansec)#security pmf mandatory`
	`Hostname(config-wlansec)#security wpa3 personal passphrase ascii 12345678`
	`Hostname(config-wlansec)#security wpa3 mode personal`
	`Hostname(config-wlansec)#security wpa3 personal pwe h2e`
	`Hostname(config-wlansec)#exit`
	`Hostname(config)#wlansec 2`
	`Hostname(config-wlansec)#security pmf mandatory`
	`Hostname(config-wlansec)#security wpa3 personal passphrase ascii 0 password@123`
	`Hostname(config-wlansec)#security wpa3 mode personal`
	`Hostname(config-wlansec)#exit`
	`Hostname(config)#wlansec 3`
	`Hostname(config-wlansec)#security pmf mandatory`
	`Hostname(config-wlansec)#security wpa3 personal passphrase ascii 7 $10$27c$8Wu2G++qd4mBlYzO$`
	`Hostname(config-wlansec)#security wpa3 mode personal`
	`Hostname(config-wlansec)#exit`

Verification	● Run the **show running-config | begin wlansec** *wlan_id* command to check whether the configuration takes effect.

AC	`Hostname#show running-config | begin wlansec 1`
	`wlansec 1`
	` security pmf mandatory`
	` security wpa3 personal passphrase ascii 12345678`
	` security wpa3 mode personal`
	` security wpa3 personal pwe h2e`
	`!`
	`wlansec 2`
	` security pmf mandatory`
	` security wpa3 personal passphrase ascii ascii 7 $10$27c$8Wu2G++qd4mBlYzO$`
	` security wpa3 mode personal`
	`!`
	`wlansec 3`
	` security pmf mandatory`

	security wpa3 personal passphrase ascii ascii 7 1007072e0f1b4f2d704078 security wpa3 mode personal !

Configuring OWE Authentication for WLAN 1, Configuring WLAN 2 as an Equivalent WLAN for OWE Authentication and Setting WLAN ID to 2

Scenario **Figure 1-17**	 In a fit AP environment, configure the following security policies for WLANs on the AC: 6. Configure OWE authentication (enhanced-open mode) for WLAN 1. 7. Configure open authentication for WLAN 2. 8. Set the SSID of WLAN 1 to the hidden mode.
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 for OWE authentication. ● Enter the configuration mode of WLAN 1. ● Set the SSID of WLAN 1 to the hidden mode.
AC	Hostname(config)#wlan-config 1 Open-SSID-OWE Hostname(config-wlan)#exit Hostname(config)#wlan-config 2 Open-SSID 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)#exit Hostname(config-wlan)#wlan-config 1 Hostname(config-wlan)#no enable-broad-ssid Hostname(config)#exit
Verification	● Run the **show running-config | begin wlansec** *wlan_id* 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 WPA3-Personal or WPA3-Enterprise is configured, when WPA authentication is enabled for the WLAN, a configuration failure occurs.
- If WPA3-Personal is configured, when WPA2 (RSNA) authentication and TKIP encryption are enabled for the WLAN, a configuration failure occurs.
- If WPA3-Enterprise is configured, when WPA2 (RSNA) authentication is enabled for the WLAN, a configuration failure occurs.

1.4.9 Configuring the Response Delay Mode for Authentication Packets

Whether this function is supported depends on the actual product version.

Configuration Effect

To prevent STAs from being attacked by repeated authentication packets during the onboarding process, a response delay mode for authentication packets is introduced. After the response delay mode is enabled, if association request packets are being processed within 1,000 ms (by default), the device discards newly received authentication packets and continues to process the previous association request packets. If the processing of association request packets has timed out (for example, exceeding 1,000 ms), the device discards the previous association request packets and processes newly received authentication packets.

Notes

N/A

Configuration Steps

Configuring the Response Delay Mode for Authentication Packets

This function is enabled by default.

Command	**rsna lazy-response enable**
Parameter Description	N/A
Defaults	This function is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Response Delay Timeout Duration for Authentication Packets

Command	[**default**] **rsna lazy-response timer** *timer*
Parameter Description	*timer*: Indicates the delay for the device to respond to authentication packets, in milliseconds. The range is from 0 to 2000. **default**: Restores the default configuration.

Defaults	The default value is 1000.
Command Mode	Global configuration mode
Usage Guide	N/A

1.4.10 Configuring PPSK

Configuration Effect

- Enable PPSK on the WLAN.
- Clients adopt PPSK authentication upon access.

Notes

- PPSK is a PSK allocated for each client, with which you can choose not to configure the WPA-PSK or RSN-PSK.
- The WLAN should be enabled with WPA authentication mode, RSN authentication mode, or a combination of the two modes, and the PSK authentication.

Configuration Steps

Configuring PPSK

- Mandatory.
- Enter the WLAN security configuration mode to enable PPSK on the AC.

Command	**security sta-psk** { **enable** | **disable** }
Parameter Description	**enable**: Enables PPSK. **disable**: Disables PPSK.
Defaults	PPSK is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	PPSK is a PSK allocated for each client, with which you can choose not to configure the WPA-PSK or RSN PSK. If you have configured both WPA-PSK and RSN-PSK, the PPSK takes precedence over them during authentication.

Configuring PPSK External Authentication

- Optional.
- Enter the WLAN security configuration mode to enable PPSK external authentication on the AC.
- Enable PPSK before you configure this function.

Command	**security sta-psk external** { **enable** | **disable** }
Parameter Description	**enable**: Enables PPSK external authentication. **disable**: Disables PPSK external authentication.
Defaults	PPSK external authentication is disabled by default.
Command Mode	WLAN security configuration mode

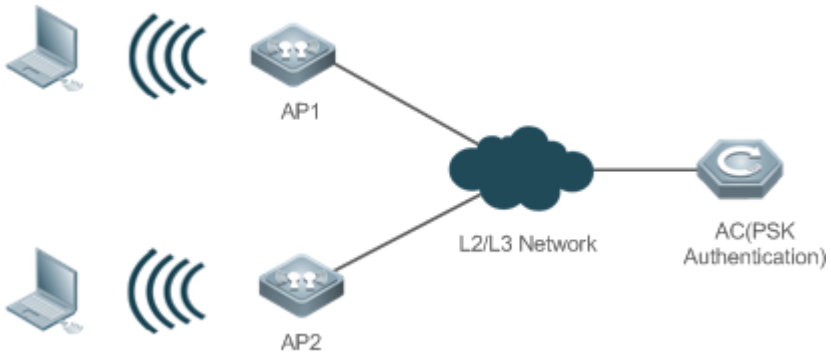
Usage Guide	This command must be used with the external authentication server.

Verification

Run the **show running-config | begin wlansec** *wlan_id* command to verify the configuration result.

Configuration Example

Enabling RSN-PSK Authentication, configuring AES Encryption, and Enabling External PPSK Authentication on WLAN 1

Scenario **Figure 1-1**	 In a Fit AP environment, configure the following security policies for WLAN 1 on the AC: Configuring RSN-PSK authentication. Configuring AES encryption. Configuring external PPSK authentication.
Configuration Steps	● Enter the security configuration mode of WLAN 1. ● Enable the RSN authentication mode. ● Configure AES encryption. ● Enable RSN-PSK authentication. ● Enable PPSK. ● Enable external PPSK authentication mode.

AC	`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 sta-psk enable`
	`Hostname(config-wlansec)# security sta-psk external enable`

Verification	Run the **show running-config	begin wlansec** *wlan_id* command to verify the configuration result.
AC	`Hostname# show running-config	begin wlansec 1` `wlansec 1` ` security rsn enable` ` security rsn ciphers aes enable` ` security rsn akm psk enable` ` security sta-psk enable` ` security sta-psk external enable` `!`

Common Errors

- The external authentication server is not configured before you enable external PPSK authentication.

1.5 Monitoring

Clearing

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

Command	Purpose
N/A	N/A

Displaying

Command	Purpose
show wlan security *wlan-id*	Displays security configuration of a WLAN.
show wclient security *mac-address*	Displays security configuration of a STA.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Purpose
N/A	N/A

1 Configuring STA Access Control Lists

1.1 Overview

STA access control lists indicate large-capacity static blocklists and allowlists and provide the following functions:

- Blocklist and allowlist for an access controller (AC), access point (AP), AP group, or service set identifier (SSID). The maximum number of blocklists or allowlists on an AC is the maximum number of STAs supported by the AC divided by two, and the maximum number of blocklists or allowlists on an AP is 4096.
- Blocklist and allowlist 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

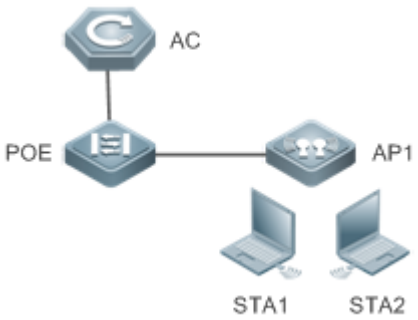
Application	Description
Fit AP Networking	Fit AP networking is adopted, including at least one AC and one AP.

1.2.1 Fit AP Networking

Scenario

On a wireless network, deploy an AC and enable the AC-based, AP-based, AP group-based, or SSID-based blocklist or allowlist on the AC, as shown in the following figure.

Figure 1-1



Remarks	AC: wireless access controller PoE: switch, used as the gateway of the AP

	AP: wireless access point STA1 and STA2: wireless stations

Deployment

- Enable AC-based blocklist on the AC to add MAC addresses of illegal STAs to the blocklist.
- Enable AP-based allowlist on the AC to allow STAs with specified MAC addresses to access this AP only.
- Enable AP group-based allowlist on the AC to allow STAs with specified MAC addresses to access APs in this AP group only.
- Enable SSID-based allowlist on the AC to allow STAs with specified MAC addresses to access this SSID only.

1.3 Features

Basic Concepts

N/A

Overview

Feature	Description
Configuring an AC-based Blocklist and Allowlist	Disallows STAs in the blocklist to access the networks of the AC and allows STAs in the allowlist to access the networks of the AC.
Configuring an AP-based Blocklist and Allowlist	Disallows STAs in the blocklist to access the specific AP and allows STAs in the allowlist to access the AP.
Configuring an AP Group-based Blocklist and Allowlist	Disallows STAs in the blocklist to access APs in the specific AP group and allows STAs in the allowlist to access APs in the AP group.
Configuring an SSID-based Blocklist and Allowlist	Disallows STAs in the blocklist to access the specific SSID and allows STAs in the allowlist to access the SSID.
Importing and Exporting Configurations	Exports configurations to a file or imports configurations from a file.

1.3.1 Configuring an AC-based Blocklist and Allowlist

You can add the MAC addresses of illegal STAs to the MAC address blocklist of the AC to prevent these STAs from accessing all the networks of the AC.

If the network users are fixed, you can add the MAC addresses of legal STAs to the MAC address allowlist of the AC. In this case, only STAs with these MAC addresses can access the networks of the AC.

To disallow or allow STAs of specific vendors to access the AC, add the OUIs of these STAs to the OUI blocklist or allowlist of the AC. In this case, STAs of these vendors are disallowed or allowed to access the networks of the AC.

Working Principle

If the MAC address or OUI of a STA is in the blocklist or not in the allowlist when it goes online, the AC rejects the association request of the STA and sends an association failure response to it.

1.3.2 Configuring an AP-based Blocklist and Allowlist

The AP-based blocklist/allowlist function allows a network administrator to configure different blocklist and allowlist policies for different APs to control access of STAs to APs.

AP-based blocklist/allowlist includes the following two types:

- AP-based MAC address blocklist/allowlist

  To disallow or allow a STA with the specified MAC address to access the specified AP without affecting access of the STA to other APs, add the MAC address of the STA to the MAC address blocklist or allowlist of the AP. In this case, the STA is disallowed or allowed to access all the SSIDs released by the specified AP and access to other APs is not affected.

- AP-based OUI blocklist/allowlist

  To disallow or allow STAs of specific vendors to access an AP, add the OUIs of these STAs to the OUI blocklist or allowlist of the AP. In this case, STAs of these vendors are disallowed or allowed to access the SSIDs released by the AP.

Working Principle

When a STA goes online through an AP, the AC checks whether a blocklist or allowlist is configured for the AP. If the MAC address or OUI of the STA is in the blocklist or not in the allowlist, the AC disallows the STA to access the wireless network and sends an association failure response to it.

1.3.3 Configuring an AP Group-based Blocklist and Allowlist

The AP group-based blocklist/allowlist function allows a network administrator to configure different blocklist and allowlist policies for different AP groups to control access of STAs to APs in an AP group.

AP group-based blocklist/allowlist includes the following two types:

- AP group-based OUI blocklist/allowlist

  To disallow or allow STAs of specific vendors to access APs in an AP group, add the OUIs of these STAs to the OUI blocklist or allowlist of the AP group. In this case, STAs of these vendors are disallowed or allowed to access all the SSIDs released by the APs in this AP group.

- AP group-based OUI blocklist/allowlist with the specified WLAN ID

  After the AP group-based OUI blocklist/allowlist with the specified WLAN ID is enabled, when a STA attempts to access an AP through the SSID corresponding to the WLAN ID, the AC disallows or allows the STA to go online based on the blocklist or allowlist policy for the WLAN ID.

Working Principle

When a STA goes online through an AP, the AC checks whether a blocklist or allowlist is configured for the AP group to which the AP belongs. If the OUI of the STA is in the blocklist or not in the allowlist, the AC rejects the association request from the STA and sends an association failure response to it.

1.3.4 Configuring an SSID-based Blocklist and Allowlist

Some SSIDs may only allow specific STAs to access. In this case, you can configure an SSID-based blocklist or allowlist to prevent STAs out of the control scope from accessing an SSID.

To disallow or allow STAs of specific vendors to access an SSID, add the OUIs of these STAs to the OUI blocklist or allowlist of the SSID. In this case, STAs of these vendors are disallowed or allowed to access the SSID.

Working Principle

When a STA goes online through an SSID, the AC checks whether a blocklist or allowlist is configured for the SSID. If the MAC address or OUI of the STA is in the blocklist or not in the allowlist, the AC rejects the association request from the STA and sends an association failure response to it.

1.3.5 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 separate file for backup or transfer it to another AC.

You can run the **import** command to import the backup configuration file to the AC 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 AC using the **copy** command for backup or transfer.

Import: Read the specified file and import the configuration commands to the AC. In overwriting mode, configurations on the AC 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 AC-based Blocklist	⚠ (Mandatory) It is used to add STAs to the AC-based blocklist.	
	blacklist mac *sta-mac*	Adds MAC addresses of STAs to the MAC address blocklist of the AC.
	blacklist vendor mac *sta-oui*	Adds OUIs of STAs to the OUI blocklist of the AC.
Configuring an AC-based Allowlist	⚠ (Mandatory) It is used to add STAs to the AC-based allowlist.	
	whitelist mac *sta-mac*	Adds MAC addresses of STAs to the MAC address allowlist of the AC.
	whitelist vendor mac *sta-oui*	Adds OUIs of STAs to the OUI allowlist of the AC.
Configuring an AP-based Blocklist	⚠ (Mandatory) It is used to add STAs to the AP-based blocklist.	
	blacklist mac *sta-mac* **in-ap** *ap-mac*	Adds MAC addresses of STAs to the MAC address blocklist of an AP.
	blacklist vendor mac *sta-oui* **in-ap** *ap-mac*	Adds OUIs of STAs to the OUI blocklist of an AP.
Configuring an AP-based	⚠ (Mandatory) It is used to add STAs to the AP-based allowlist.	

Allowlist	**whitelist mac** *sta-mac* **in-ap** *ap-mac*	Adds MAC addresses of STAs to the MAC address allowlist of an AP.
	whitelist vendor mac *sta-oui* **in-ap** *ap-mac*	Adds OUIs of STAs to the OUI allowlist of an AP.
Configuring an AP Group-based Blocklist	(Mandatory) It is used to add STAs to the AP group-based blocklist.	
	blacklist mac *sta-mac* **in-apg** *apg-name* [**wlan** *wlan-id*]	Adds MAC addresses of STAs to the MAC address blocklist of an AP group.
	blacklist vendor mac *sta-oui* **in-apg** *apg-name* [**wlan** *wlan-id*]	Adds OUIs of STAs to the OUI blocklist of an AP group. (A WLAN ID can be specified.)
	blacklist vendor mac *sta-oui* [**wlan** *wlan-id*] (AP group configuration mode)	Adds OUIs of STAs to the OUI blocklist of the current AP group. (A WLAN ID can be specified.)
Configuring an AP Group-based Allowlist	(Mandatory) It is used to add STAs to the AP group-based allowlist.	
	whitelist mac *sta-mac* **in-apg** *apg-name* [**wlan** *wlan-id*]	Adds MAC addresses of STAs to the MAC address allowlist of an AP group.
	whitelist vendor mac *sta-oui* **in-apg** *apg-name* [**wlan** *wlan-id*]	Adds OUIs of STAs to the OUI allowlist of an AP group. (A WLAN ID can be specified.)
	whitelist vendor mac *sta-oui* [**wlan** *wlan-id*] (AP group configuration mode)	Adds OUIs of STAs to the OUI allowlist of the current AP group. (A WLAN ID can be specified.)
Configuring an SSID-based Blocklist	(Mandatory) It is used to add STAs to the SSID-based blocklist.	
	blacklist mac *sta-mac* **in-ssid** *ssid-string*	Adds MAC addresses of STAs to the MAC address blocklist of an SSID.
	blacklist vendor mac *sta-oui* **in-ssid** *ssid-string*	Adds OUIs of STAs to the OUI blocklist of an SSID.
Configuring an SSID-based Allowlist	(Mandatory) It is used to add STAs to the SSID-based allowlist.	
	whitelist mac *sta-mac* **in-ssid** *ssid-string*	Adds MAC addresses of STAs to the MAC address allowlist of an SSID.
	whitelist vendor mac *sta-oui* **in-ssid** *ssid-string*	Adds OUIs of STAs to the OUI allowlist 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 AC-based Blocklist

Configuration Effect

- STAs added to the MAC address blocklist cannot access all the networks of the AC.
- STAs of vendors added to the OUI blocklist cannot access all the networks of the AC.

Notes

N/A

Configuration Steps

Adding MAC Addresses of STAs to the MAC Address Blocklist of the AC

- Mandatory. Configure it on the AC.

Command	**blacklist mac** *sta-mac* [**mnemonic** *string*]
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	● After a blocklist is configured, STAs that meet the conditions are not allowed to access the network. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. ● When the blocklist is enabled, an online STA that meets 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 blocklist and allowlist configurations.

Adding OUIs of STAs to the OUI Blocklist of the AC

- Mandatory. Configure it on the AC.

Command	**blacklist vendor mac** *sta-oui* [**mnemonic** *string*]
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI blocklist is used to match OUIs of STAs. STAs of vendors in the OUI blocklist are not

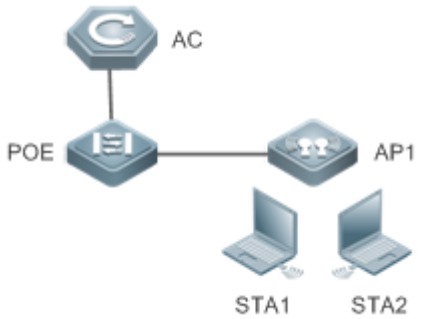
	allowed to access the network. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. ● When the blocklist is enabled, an online STA that meets 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list blacklist** command to display the information about STAs in the MAC address blocklist of the AC.
- Run the **show black-white-list blacklist vendor** command to display the vendor OUIs in the OUI blocklist of the AC.

Configuration Example

↘ Configuring a MAC Address Blocklist for the AC

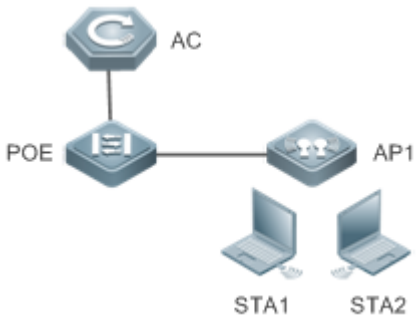
Scenario **Figure 1-2**	
Configuration Steps	● Configure a MAC address blocklist for the AC.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# blacklist mac 0069.6c3f.2baa`

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list blacklist** command. ● Check whether STAs added to the MAC address blocklist cannot associate with the AC.

AC	

Configuring an OUI Blocklist for the AC

Scenario Figure 1-3	
Configuration Steps	● Configure an OUI blocklist for the AC.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# blacklist vendor mac 0069.6c`
	`AC(black-white-list)# blacklist vendor mac 0c51.01`

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list blacklist vendor** command. ● Check whether STAs of vendors added to the OUI blocklist cannot associate with the AC.
AC	

Common Errors

- N/A

1.4.2 Configuring an AC-based Allowlist

Configuration Effect

- When there are entries in the MAC address allowlist, STAs not added to the allowlist cannot access any network of the AC.
- When there are entries in the OUI allowlist, STAs of vendors not added to the OUI allowlist cannot access any network of the AC.

Notes

- N/A

Configuration Steps

Adding MAC Addresses of STAs to the MAC Address Allowlist of the AC

- Mandatory. Configure it on the AC.

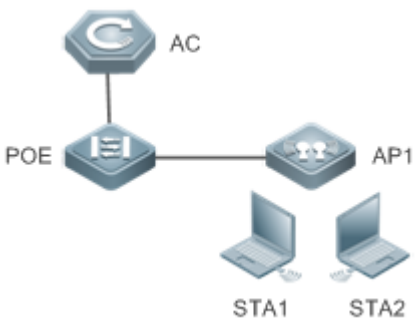
Command	**whitelist mac** *sta-mac* **[mnemonic** *string***]**
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	• After an allowlist is configured, only STAs that meet conditions are allowed to access the network. • If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the network. • Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. • The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. • Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. • When an entry is added to the allowlist, 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list whitelist** command to display information about the STAs in the MAC address allowlist of the AC.

Configuration Example

↘ Configuring a MAC Address Allowlist for the AC

Scenario **Figure 1-4**	

Configuration Steps	● Configure a MAC address allowlist for the AC.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# whitelist mac 0069.6c3f.2baa`
	`AC(black-white-list)# whitelist mac 0c51.016a.5d8e`

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list whitelist** command. ● Check whether STAs not added to the allowlist cannot associate with the AC.
AC	

Adding OUIs of STAs to the OUI Allowlist of the AC

- Mandatory. Configure it on the AC.

Command	**whitelist vendor mac** *sta-oui* **[mnemonic** *string***]**
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI allowlist is used to match the OUIs of STAs. STAs of vendors in the OUI allowlist are allowed to access the network. ● If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the network. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. ● When an entry is added to the allowlist, 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Configuration Steps

Adding OUIs of STAs to the OUI Allowlist of the AC

- Mandatory. Configure it on the AC.

Command	**whitelist vendor mac** *sta-oui* **[mnemonic** *string***]**

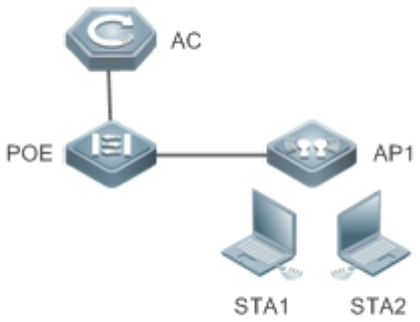
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI allowlist is used to match the OUIs of STAs. STAs of vendors in the OUI allowlist are allowed to access the network. ● If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the network. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. ● When an entry is added to the allowlist, 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list whitelist vendor** command to display the vendor OUIs in the OUI allowlist of the AC.

Configuration Example

↘ Configuring an OUI Allowlist for the AC

Scenario **Figure 1-5**	
Configuration	● Configure an OUI allowlist for the AC.

Steps	
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# black-white-list AC(black-white-list)# whitelist vendor mac 0069.6c AC(black-white-list)# whitelist vendor mac 0c51.01
Verification	● Run the **show black-white-list whitelist vendor** command to display the configuration entries. ● Check whether STAs of vendors not added to the OUI allowlist cannot associate with the AC.
AC	

Common Errors

- N/A

1.4.3 Configuring an AP-based Blocklist

Configuration Effect

- STAs added to the MAC address blocklist of an AP cannot access all the networks of the AP.
- STAs of vendors added to the OUI blocklist of an AP cannot access all the networks of the AP.

Notes

- N/A

Configuration Steps

↘ Adding MAC Addresses of STAs to the MAC Address Blocklist of the Specified AP

- Mandatory. Configure it on the AC.

Command	**blacklist mac** *sta-mac* **[in-ap** *ap-mac* **| mnemonic** *string***]**
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	● After a blocklist is configured, STAs that meet the conditions are not allowed to access the networks of the AP. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is

	added to allowlists of other types. ● When the blocklist is enabled, an online STA that meets 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list blacklist in-ap** *ap-mac* command to display information about the STAs in the MAC address blocklist of the AP.

Adding OUIs of STAs to the OUI Blocklist of the AP

- Mandatory. Configure it on the AC.

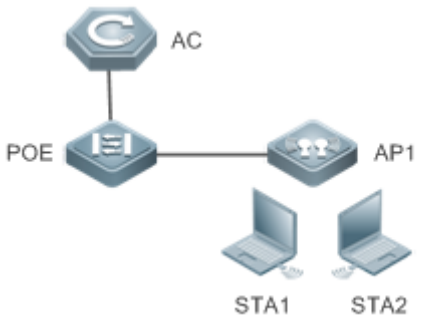
Command	**blacklist vendor mac** *sta-oui* **[in-ap** *ap-mac* **| mnemonic** *string* **]**
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI blocklist is used to match OUIs of STAs. STAs of vendors in the OUI blocklist are not allowed to access the network. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. ● When the blocklist is enabled, an online STA that meets 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list blacklist vendor** command to display the vendor OUIs in the OUI blocklist of the AP.

Configuration Example

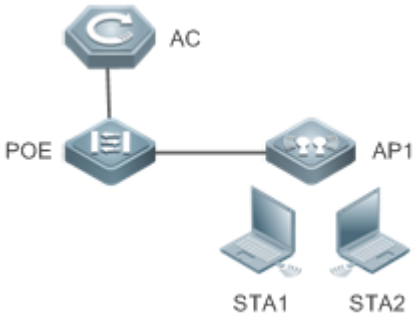
Configuring a MAC Address Blocklist for an AP

Scenario **Figure 1-6**	
Configuration Steps	● Configure a MAC address blocklist for AP1 with the MAC address 0074.9c06.9afa.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# blacklist mac 0069.6c3f.2baa in-ap 0074.9c06.9afa`

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list blacklist** command. ● Check whether STAs added to the MAC address blocklist cannot associate with the AP.
AC	

Configuring an OUI Blocklist for an AP

Scenario **Figure 1-7**	
Configuration Steps	● Configure an OUI blocklist for AP1 with the MAC address 0074.9c06.9afa.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# blacklist vendor mac 0069.6c in-ap 0074.9c06.9afa`
	`AC(black-white-list)# blacklist vendor mac 0c51.01 in-ap 0074.9c06.9afa`

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list blacklist vendor in-ap** *ap-mac* command.

	● Check whether STAs of vendors added to the OUI blocklist cannot associate with the AP.
AC	

Common Errors

- N/A

1.4.4 Configuring an AP-based Allowlist

Configuration Effect

- When there are entries in the MAC address allowlist of an AP, STAs not added to the allowlist cannot access any network of the AP.
- When there are entries in the OUI allowlist of an AP, STAs of vendors not added to the OUI allowlist cannot access any network of the AP.

Notes

- N/A

Configuration Steps

↘ Adding MAC Addresses of STAs to the MAC Address Allowlist of the Specified AP

- Mandatory. Configure it on the AC.

Command	**whitelist mac** *sta-mac* **in-ap** *ap-mac* [**mnemonic** *string*]
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	● After an allowlist is configured, only STAs that meet conditions are allowed to access the networks of the AP. ● If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the networks of the AP. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. ● When an entry is added to the allowlist, 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list whitelist in-ap** *ap-mac* command to display information about the STAs in the allowlist of the AP.

Adding OUIs of STAs to the OUI Allowlist of the Specified AP

- Mandatory. Configure it on the AC.

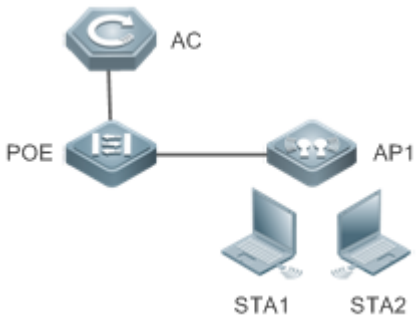
Command	**whitelist vendor mac** *sta-oui* **in-ap** *ap-mac* **[mnemonic** *string***]**
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	• The OUI allowlist is used to match the OUIs of STAs. STAs of vendors in the OUI allowlist are allowed to access the networks of the AP. • If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the network. • Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. • The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. • Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. • When an entry is added to the allowlist, 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

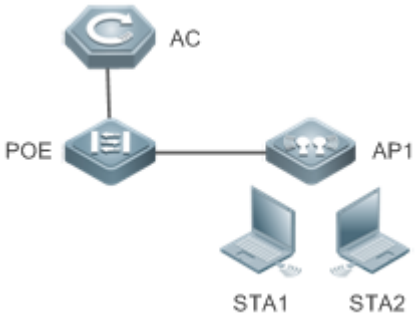
- Run the **show black-white-list whitelist vendor in-ap** *ap-mac* command to display the vendor OUIs in the OUI allowlist of the AP.

Configuration Example

Configuring a MAC Address Allowlist for an AP

Scenario **Figure 1-8**	
Configuration Steps	● Configure a MAC address allowlist for AP1 with the MAC address 0074.9c06.9afa.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# black-white-list AC(black-white-list)# whitelist mac 0069.6c3f.2baa in-ap 0074.9c06.9afa AC(black-white-list)# whitelist mac 0c51.016a.5d8e in-ap 0074.9c06.9afa
Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list whitelist in-ap** *ap-mac* command. ● Check whether STAs not added to the allowlist cannot associate with the AP.
AC	

Configuring an OUI Allowlist for an AP

Scenario **Figure 1-9**	
Configuration Steps	● Configure an OUI allowlist for AP1 with the MAC address 0074.9c06.9afa.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# black-white-list AC(black-white-list)# whitelist vendor mac 0069.6c in-ap 0074.9c06.9afa AC(black-white-list)# whitelist vendor mac 0c51.01 in-ap 0074.9c06.9afa

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list whitelist vendor in-ap** *ap-mac* command. ● Check whether STAs of vendors not added to the allowlist cannot associate with the AP.
AC	

Common Errors

N/A

1.4.5 Configuring an AP Group-based Blocklist

Configuration Effect

- STAs added to the MAC address blocklist of an AP cannot access all the networks of the AP group.
- STAs of vendors added to the OUI blocklist of an AP group cannot access all the networks of the AP group.

Notes

- AP groups support only the OUI blocklist and allowlist and do not support the MAC address blocklist and allowlist.
- Configurations in AP group configuration mode and STA access control list configuration mode with the **in-apg** parameter are the same. However, the **show running-config** command displays the configuration in AP group configuration mode. In a hierarchical AC scenario, the configuration can be synchronized from the central AC to a branch AC.
- A non-existent AP group name can be specified for the AP group-based OUI blocklist. The OUI of a STA is matched against the OUI blocklist only when the name of the AP group to which the AP that the STA accesses belongs is the same as the AP group name of the blocklist.
- When an AP group-based OUI blocklist with the specified WLAN ID is configured, a non-existent WLAN ID or a WLAN ID not added to the AP group can be specified. The WLAN ID range is from 1 to 4094.
- When the AP group-based OUI blocklist with the specified WLAN ID is configured, the OUI of the STA is matched against the OUI blocklist only when the STA accesses an AP in the AP group through the SSID corresponding to the WLAN ID. When no WLAN ID is specified, the OUI of the STA is matched against the OUI blocklist when the STA accesses an AP in the AP group through any SSID.
- The OUI blocklist is used to match OUIs of STAs. STAs of vendors in the OUI blocklist are not allowed to access the network.
- Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs.
- The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC.
- Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types.
- When the blocklist is enabled, an online STA that meets the conditions will be kicked offline immediately.

Configuration Steps

Adding MAC Addresses of STAs to the MAC Address Blocklist of the Specified AP group

- Mandatory. Configure it on the AC.

Command	**blacklist mac** *sta-mac* **in-apg** *apg-name* [**wlan** *wlan-id*] [**mnemonic** *string*]
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	• After a blocklist is configured, STAs that meet the conditions are not allowed to access the networks of the AP. • Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. • The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. • Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. • When the blocklist is enabled, an online STA that meets 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list blacklist in-ap** *ap-mac* command to display information about the STAs in the MAC address blocklist of the AP group.

Adding OUIs of STAs to the OUI Blocklist of an AP Group

- Mandatory. Configure it on the AC.

Command	**blacklist vendor mac** *sta-oui* **in-apg** *apg-name* [**wlan** *wlan-id*] [**mnemonic** *string*]
Parameter Description	*sta-oui*: OUI of a STA, in the format of hhhh.hh. If there are no parameters after *sta-oui*, the blocklist is configured for the AC. *apg-name*: Name of the AP group for which an OUI blocklist is configured. This parameter takes effect only on the AC. *wlan-id*: WLAN ID specified when an OUI blocklist is configured for an AP group. This parameter takes effect only on the AC. *string*: Mnemonic, which is displayed in the output of the **show** command to facilitate viewing.
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	In STA access control list configuration mode, run the **show black-white-list config** command to display the blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

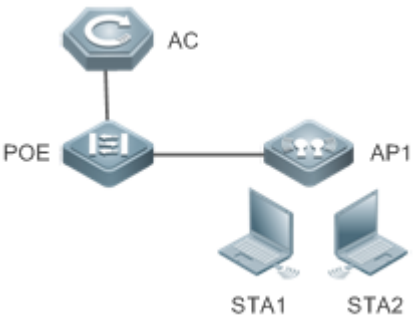
Command	**blacklist vendor mac** *sta-oui* [**wlan** *wlan-id*] [**mnemonic** *string*]
Parameter Description	*sta-oui*: OUI of a STA, in the format of hhhh.hh. If there are no parameters after *sta-oui*, the blocklist is configured for the AC. *apg-name*: Name of the AP group for which an OUI blocklist is configured. This parameter takes effect only on the AC. *wlan-id*: WLAN ID specified when an OUI blocklist is configured for an AP group. This parameter takes effect only on the AC. *string*: Mnemonic, which is displayed in the output of the **show** command to facilitate viewing.
Defaults	No entry is configured.
Command Mode	AP group configuration mode
Usage Guide	N/A

Verification

- Run the **show black-white-list blacklist vendor in-apg** *apg-name* [**wlan** *wlan-id*] command to display OUIs of vendors in the OUI blocklist of the AP group.

Configuration Example

Configuring an OUI Blocklist for an AP Group

Scenario Figure 1-10	
Configuration Steps	● Configure an OUI blocklist for AP group APG1.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# blacklist vendor mac 0069.6c in-apg APG1`
	`AC(black-white-list)# blacklist vendor mac 0069.6d in-apg APG1 wlan 1`
	`AC(black-white-list)# exit`
	`AC(config)# ap-group APG1`
	`AC(config-group)# blacklist vendor mac 0c51.01`
	`AC(config-group)# blacklist vendor mac 0c51.02 wlan 1`

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list blacklist vendor in-apg** *apg-name* [**wlan** *wlan-id*] command. (Note: If no WLAN ID is specified, the OUI blocklist of the AP group without WLAN ID specified is displayed.) ● Check whether STAs of vendors added to the OUI blocklist cannot associate with APs in the AP group.

Common Errors

N/A

1.4.6 Configuring an AP Group-based Allowlist

Configuration Effect

- When there are entries in the MAC address allowlist of an AP, STAs not added to the allowlist cannot access any network of the AP group.
- When there are entries in the OUI allowlist of the specified AP group, STAs of vendors not added to the OUI allowlist cannot access APs in this AP group.

Notes

- A non-existent AP group name can be specified for the AP group-based OUI allowlist. The OUI of a STA is matched against the OUI allowlist only when the name of the AP group to which the AP that the STA accesses belongs is the same as the AP group name of the allowlist.
- A non-existent WLAN ID or a WLAN ID not added to an AP group can be specified for an AP group-based OUI allowlist. The WLAN ID range is from 1 to 4094. When a WLAN ID is specified, the OUI of a STA is matched against the OUI allowlist only when the STA accesses an AP in the AP group through the SSID corresponding to the WLAN ID. When no WLAN ID is specified, the OUI of a STA is matched against the OUI allowlist when the STA accesses an AP in the AP group through any SSID.
- The OUI allowlist is used to match the OUIs of STAs. STAs of vendors in the OUI allowlist are allowed to access the network.
- If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the network.
- Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs.
- The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC.
- Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types.
- When an entry is added to the allowlist, other STAs will not be kicked offline.
- Configurations in AP group configuration mode and STA access control list configuration mode with the **in-apg** parameter are the same. However, the **show running-config** command displays the configuration in AP group configuration mode. In a hierarchical AC scenario, the configuration can be synchronized from the center AC to a branch AC.

Configuration Steps

Adding MAC Addresses of STAs to the MAC Address Allowlist of the Specified AP group

- Mandatory. Configure it on the AC.

Command	**whitelist mac** *sta-mac* **in-apg** *apg-name* [**wlan** *wlan-id*] [**mnemonic** *string*]
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	• After an allowlist is configured, only STAs that meet conditions are allowed to access the networks of the AP. • If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the networks of the AP. • Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. • The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. • Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. • When an entry is added to the allowlist, 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

Run the **show black-white-list whitelist in-ap** *ap-mac* command to display information about the STAs in the allowlist of the AP group.

Adding OUIs of STAs to the OUI Allowlist of the Specified AP Group

- Mandatory. Configure it on the AC.

Command	**whitelist vendor mac** *sta-oui* **in-apg** *apg-name* [**wlan** *wlan-id*] [**mnemonic** *string*]
Parameter Description	*sta-oui*: OUI of a STA, in the format of hhhh.hh. If there are no parameters after *sta-oui*, the allowlist is configured for the AC. *apg-name*: Name of the AP group for which an OUI allowlist is configured. This parameter takes effect only on the AC. *wlan-id*: WLAN ID specified when an OUI allowlist is configured for an AP group. This parameter takes effect only on the AC. *string*: Mnemonic, which is displayed in the output of the **show** command to facilitate viewing.
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode

Usage Guide	● In STA access control list configuration mode, run the **show black-white-list config** command to display the blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

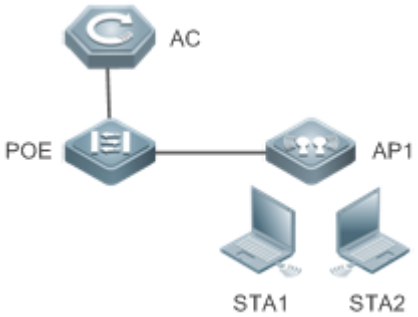
Command	**whitelist vendor mac** *sta-oui* [**wlan** *wlan-id*] **[mnemonic** *string***]**
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	AP group configuration mode
Usage Guide	N/A

Verification

- Run the **show black-white-list whitelist vendor in-apg** *apg-name* [**wlan** *wlan-id*] command to display the OUIs of vendors in the OUI allowlist of the AP group.

Configuration Example

Configuring an OUI Allowlist for an AP Group

Scenario Figure 1-11	
Configuration Steps	● Configure an OUI allowlist for AP group APG1.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# whitelist vendor mac 0069.6c in-apg APG1`
	`AC(black-white-list)# whitelist vendor mac 0069.6d in-apg APG1 wlan 1`
	`AC(black-white-list)# exit`
	`AC(config)# ap-group APG1`
	`AC(config-group)# whitelist vendor mac 0c51.01`
	`AC(config-group)# whitelist vendor mac 0c51.01 wlan 1`

Verification	● Configuration entries are displayed in the output of the **show black-white-list whitelist vendor in-apg** *apg-name* [**wlan** *wlan-id*] command. (Note: If no WLAN ID is specified, the OUI allowlist of the AP group without WLAN ID specified is displayed.) ● STAs of vendors not added to the allowlist cannot associate with APs in the AP group.

Common Errors

N/A

1.4.7 Configuring an SSID-based Blocklist

Configuration Effect

- STAs added to the MAC address blocklist of an SSID cannot access the SSID.
- When there are entries in the OUI blocklist of the specified SSID, STAs of vendors added to the OUI blocklist cannot access the SSID.

Notes

N/A

Configuration Steps

↘ Adding MAC Addresses of STAs to the MAC Address Blocklist of the Specified SSID

- Mandatory. Configure it on the AC.

Command	**blacklist mac** *sta-mac* **in-ssid** *ssid* [**mnemonic** *string*]
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	● After a blocklist is configured, STAs that meet the conditions are not allowed to access the network. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. ● When the blocklist is enabled, an online STA that meets 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list blacklist in-ssid** *ssid* command to display information about the STAs in the MAC address blocklist of the SSID.

Adding OUIs of STAs to the OUI Blocklist of the Specified SSID

- Mandatory. Configure it on the AC.

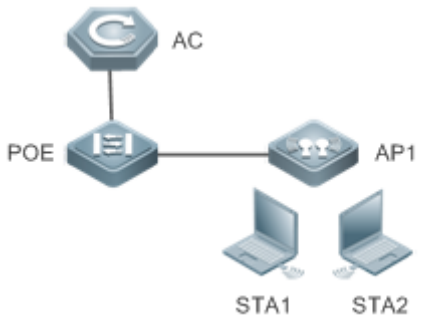
Command	**blacklist vendor mac** *sta-oui* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	• The OUI blocklist is used to match OUIs of STAs. STAs of vendors in the OUI blocklist are not allowed to access the network. • Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. • The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. • Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. • When the blocklist is enabled, an online STA that meets 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list blacklist vendor in-ssid** *ssid* command to display the OUIs of vendors in the OUI blocklist of the SSID.

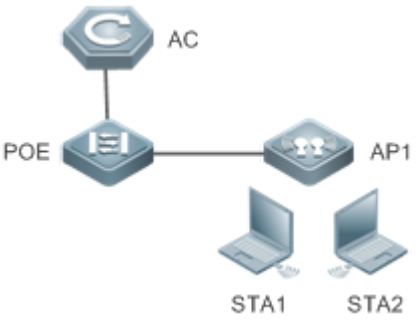
Configuration Example

Configuring a MAC Address Blocklist for an SSID

Scenario **Figure 1-12**	

Configuration Steps	● Configure a MAC address blocklist for SSID Hostname-web.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# black-white-list AC(black-white-list)# blacklist mac 0069.6c3f.2baa in-ssid Hostname-web
Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list blacklist in-ssid** *ssid-string* command. ● Check whether STAs added to the blocklist cannot associate with the SSID.
AC	

Configuring an OUI Blocklist for an SSID

Scenario **Figure 1-13**	
Configuration Steps	● Configure an OUI blocklist for SSID Hostname-web.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# black-white-list AC(black-white-list)# blacklist vendor mac 0069.6c in-ssid Hostname-web AC(black-white-list)# blacklist vendor mac 0c51.01 in-ssid Hostname-web
Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list blacklist vendor in-ssid** *ssid-string* command. ● Check whether STAs of vendors added to the blocklist cannot associate with the SSID.
AC	

Common Errors

- N/A

1.4.8 Configuring an SSID-based Allowlist

Configuration Effect

- When there are entries in the MAC address allowlist of the specified SSID, STAs not added to the MAC address allowlist cannot access the SSID.
- When there are entries in the OUI allowlist of the specified SSID, STAs of vendors not added to the OUI allowlist cannot access the SSID.

Notes

- N/A

Configuration Steps

Adding MAC Addresses of STAs to the MAC Address Allowlist of the Specified SSID

- Mandatory. Configure it on the AC.

Command	**whitelist mac** *sta-mac* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	N/A
Defaults	No entry is configured.
Command Mode	STA access control list configuration mode
Usage Guide	• After an allowlist is configured, only STAs that meet conditions are allowed to access the network. • If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the network. • Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. • The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. • Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. • When an entry is added to the allowlist, 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list whitelist in-ssid** *ssid* command to display information about the STAs in the MAC address allowlist of the SSID.

Adding OUIs of STAs to the OUI Allowlist of the Specified SSID

- Mandatory. Configure it on the AC.

Command	**whitelist vendor mac** *sta-oui* **in-ssid** *ssid* **[mnemonic** *string***]**
Parameter Description	N/A
Defaults	No entry is configured.

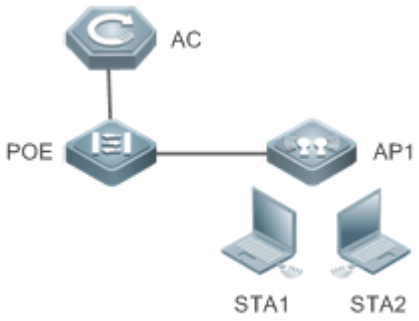
Command Mode	STA access control list configuration mode
Usage Guide	● The OUI allowlist is used to match the OUIs of STAs. STAs of vendors in the OUI allowlist are allowed to access the network. ● If the allowlist is empty, all STAs are allowed to access the network. If there is data in the allowlist, STAs not listed in the allowlist are immediately banned from accessing the network. ● Different types of blocklists and allowlists are complex in priority. You are advised to select a single type according to your needs. ● The MAC address allowlist and blocklist of the same type are mutually exclusive. For example, a MAC address added to the allowlist of an AC cannot be added to the blocklist of the AC. ● Blocklist has a higher priority than allowlist. For example, a STA added to any type of blocklist (MAC address or OUI blocklist of an AC, AP, AP group, or SSID) cannot go online even if it is added to allowlists of other types. ● When an entry is added to the allowlist, 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 blocklist and allowlist configurations. The **show running-config** command is not supported in this configuration mode.

Verification

- Run the **show black-white-list whitelist vendor in-ssid** *ssid* command to display the OUIs of vendors in the OUI allowlist of the SSID.

Configuration Example

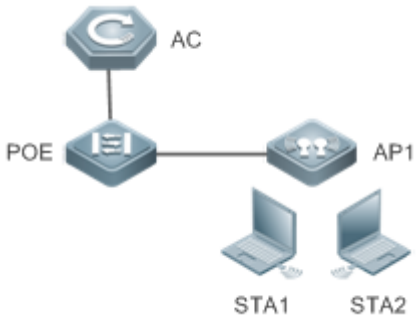
↘ Configuring a MAC Address Allowlist for an SSID

Scenario Figure 1-14	
Configuration Steps	● Configure a MAC address allowlist for SSID Hostname-web.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# whitelist mac 0069.6c3f.2baa in-ssid Hostname-web`
	`AC(black-white-list)# whitelist mac 0c51.016a.5d8e in-ssid Hostname-web`

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list whitelist in-ssid** *ssid-string* command. ● Check whether STAs not added to the MAC address allowlist cannot associate with the SSID.
AC	

↘ Configuring an OUI Allowlist for an SSID

Scenario **Figure 1-15**	
Configuration Steps	● Configure an OUI allowlist for SSID Hostname-web.

AC	`AC# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC(config)# black-white-list`
	`AC(black-white-list)# whitelist vendor mac 0069.6c in-ssid Hostname-web`
	`AC(black-white-list)# whitelist vendor mac 0c51.01 in-ssid Hostname-web`

Verification	● Check whether configuration entries are displayed in the output of the **show black-white-list whitelist vendor in-ssid** *ssid-string* command. ● Check whether STAs of vendors not added to the OUI allowlist cannot associate with the SSID.
AC	

Common Errors

- N/A

1.4.9 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. In overwriting mode, configurations on the AC will be cleared in advance. In merging mode, entries 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

- Optional. Configure it on the AC.
- 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

- Optional. Configure it on the AC.
- This command takes effect only once and is not saved.

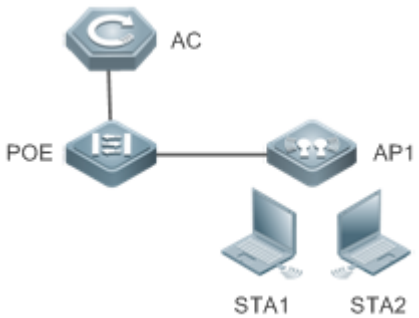
Command	**import** *filename* **{replace | append}**
Parameter Description	N/A
Defaults	N/A
Command Mode	STA access control list configuration mode
Usage Guide	N/A

Verification

- Run the **show black-white-list config** command to display the configurations.
- Run the **dir** command to display files in the flash memory.

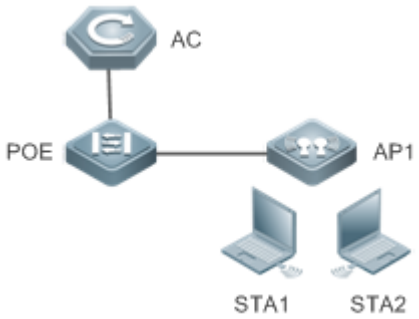
Configuration Example

Exporting the Current Configuration to a File

Scenario Figure 1-16	
Configuration	● Export the current configuration to the **black-white-list.csv** file.

Steps	
AC	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. Check whether the **black-white-list.csv** file is displayed in the command output. ● Run the **more black-white-list.csv** command. Check whether the file content is the STA access control list configuration.
AC	

↘ Importing the Configuration from a File

Scenario Figure 1-17	
Configuration Steps	● Import the configuration from the **black-white-list.csv** file and append it to the current configuration.
AC	AC# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC(config)# black-white-list AC(black-white-list)# import black-white-list.csv append
Verification	● Run the **show black-white-list config** command to display the configurations.
AC	

Common Errors

- N/A

1.5 Monitoring

Clearing

Command	Purpose

Command	Purpose
reset blacklist [**in-ap** *ap-mac* **| in-ssid** *ssid-string*]	Clears entries in the MAC address blocklist of an AC, AP, or SSID.
reset whitelist [**in-ap** *ap-mac* **| in-ssid** *ssid-string*]	Clears entries in the MAC address allowlist of an AC, AP, or SSID.
reset whitelist vendor [**in-ap** *ap-mac* **| in-apg** *apg-name* [**wlan** *wlan-id*] **| in-ssid** *ssid-string*]	Clears entries in the OUI allowlist of an AC, AP, AP group, or SSID.
reset blacklist vendor [**in-ap** *ap-mac* **| in-apg** *apg-name* [**wlan** *wlan-id*] | **in-ssid** *ssid-string*]	Clears entries in the OUI blocklist of an AC, AP, AP group, or SSID.

Displaying

Command	Purpose
show black-white-list summary	Displays basic information of a STA access control list.
show black-white-list config	Displays the STA access control list configuration.
show black-white-list conflict	Displays STAs in both the blocklist and allowlist.
show black-white-list sta-mac *sta-mac*	Displays the blocklist/allowlist configuration type of a specific STA.
show black-white-list blacklist [**in-ap** *ap-mac* **| in-ssid** *ssid-string*]	Displays entries in the MAC address blocklist of an AC, AP, or SSID.
show black-white-list blacklist vendor [**in-ap** *ap-mac* **| in-apg** *apg-name* [**wlan** *wlan-id*] **| in-ssid** *ssid-string*]	Displays entries in the OUI blocklist of an AC, AP, AP group, or SSID.
show black-white-list whitelist [**in-ap** *ap-mac* **| in-ssid** *ssid-string*]	Displays entries in the MAC address allowlist of an AC, AP, or SSID.
show black-white-list whitelist vendor [**in-ap** *ap-mac* | **in-apg** *apg-name* [**wlan** *wlan-id*] **| in-ssid** *ssid-string*]	Displays entries in the OUI allowlist of an AC, AP, AP group, or SSID.

Debugging

N/A

1 Configuring WIDS

1.1 Overview

Compared with wired networks, the wireless LAN (WLAN) has unparalleled advantages, such as convenient deployment, flexible use, efficient cost, and easy extension. These benefits contribute to the increasing popularity of WLAN. However, due to channel openness, WLAN is vulnerable to various network threats, such as rogue access points (APs), ad hoc networks, and different types of protocol attacks. Therefore, security becomes a major factor that hinders WLAN development.

Wireless Intrusion Detection System (WIDS) can detect malicious station (STA) attacks and intrusions in an early stage, helping network administrators proactively discover and defend against potential risks on networks in a timely manner.

1.2 Applications

Application	Description
Frame Filtering	When unauthorized STAs attempt to access the WLAN, WIDS frame filtering can control STA access.
User Isolation	When a STA intends to access other STAs on the WLAN, WIDS user isolation can isolate their direct communication.
IDS	Intrusion Detection System (IDS) can detect different types of attacks and intrusions on the WLAN.
Rogue Detection and Containment	WIDS rogue device detection and containment can monitor and contain unauthorized devices that compromise normal STAs and services by providing counterfeit services on the WLAN.

1.2.1 Frame Filtering

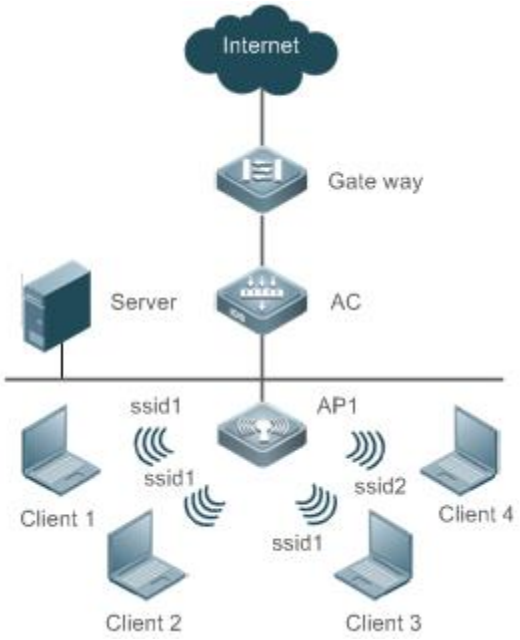
Scenario

Frame filtering provides the STA access control service on the WLAN, including allowing specified STAs to access WLANs or specified WLANs, preventing STAs from accessing WLANs or specified WLANs, preventing low-rate STAs from accessing WLANs, as well as dynamically controlling STA access.

The following figure shows an example. Assume that the WLANs have the following deployment requirements:

- 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 out low-rate STAs and disconnect them.
- Dynamically control STA access.

Figure 2-1 Networking Topology of Wireless Access Control



Deployment

The key configuration points for the devices are as follows:

- Add Client 1 to a WIDS allowlist. As a result, Client 1 can access the WLAN service provided by all APs connected to the AC. Other STAs not in the list cannot.
- Add Client 2 to the SSID 1-based allowlist. As a result, Client 2 can access SSID 1 provided by all APs connected to the AC. Other STAs not in the list cannot.
- Add Client 3 to a static blocklist. As a result, Client 3 cannot access the WLAN service provided by all APs connected to the AC.
- Add Client 4 to the SSID 1-based blocklist. As a result, Client 4 cannot access SSID 1 provided by all APs connected to the AC.
- Configure the threshold Rt for filtering out low-rate STAs. As a result, STAs with rates lower than the threshold will be disconnected.
- Enable the dynamic blocklist function, which can be used with the IDS function. After the dynamic blocklist and IDS functions are enabled, detected attacks are added to a dynamic blocklist. Before the blocklist ages out, the STAs that meet the conditions of the blocklist are prevented from communication and access through the AP.

1.2.2 User Isolation

Scenario

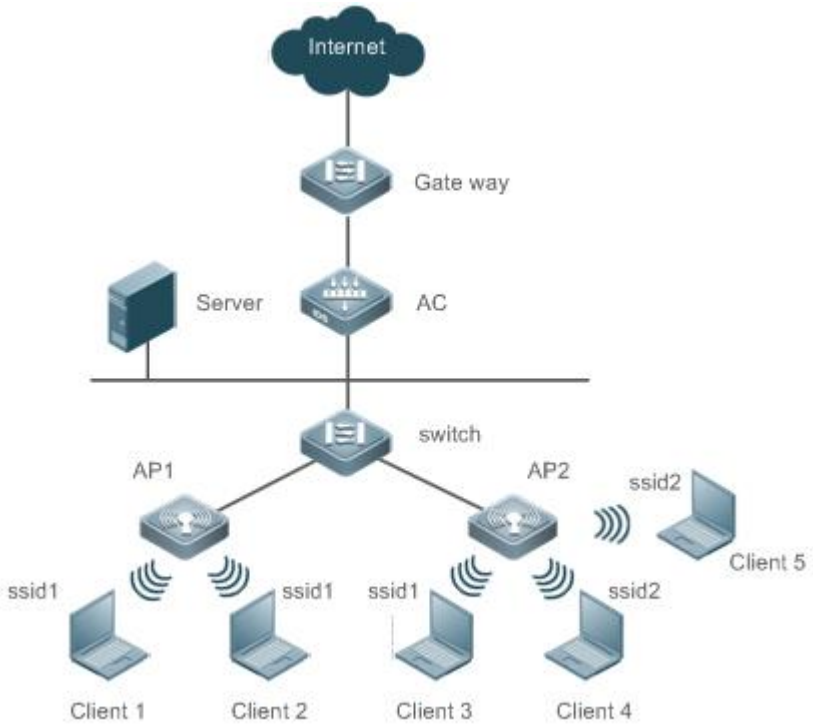
Layer 2 user isolation is provided on a WLAN, including AP-based, AP-SSID-based, and SSID-based user isolation. Assume that the WLANs have the following deployment requirements.

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.

- Direct communication cannot be conducted between Client 1 and Client 2, and between Client 3 to Client 5, but can be conducted among other users.

- Direct communication cannot be conducted between Client 1 and Client 2, and between Client 4 and Client 5, but can be conducted among other users.
- 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 conducted among other users.
- Direct communication cannot be conducted between Client 3 and Client 1 or Client 2, but can be conducted among other users.
- Direct communication cannot be conducted between Client 3 and Client 4 or Client 5, but can be conducted between Client 4 and Client 5.
- Direct communication cannot be conducted between Client 1 to Client 3, but can be conducted among other users.

Figure 2-2 Networking Topology of Wireless User Isolation



Deployment

The key configuration points for the devices are as follows:

- Configure AP-based user isolation. As a result, direct communication cannot be conducted between Client 1 and Client 2, and between Client 3 to Client 5.
- Configure AP-SSID based user isolation. As a result, direct communication cannot 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 or Client 2 and Client 3 to Client 5.
- Configure AC-SSID-based user isolation. As a result, direct communication cannot be conducted between Client 3 and Client 1 or Client 2.

- Configuring AP-SSID based user isolation can isolate direct communication between Client 3 and Client 4, and between Client 3 and Client 5.
- Configure SSID 1-based user isolation. As a result, direct communication cannot be conducted between Client 1, Client 2, and Client 3.

1.2.3 IDS

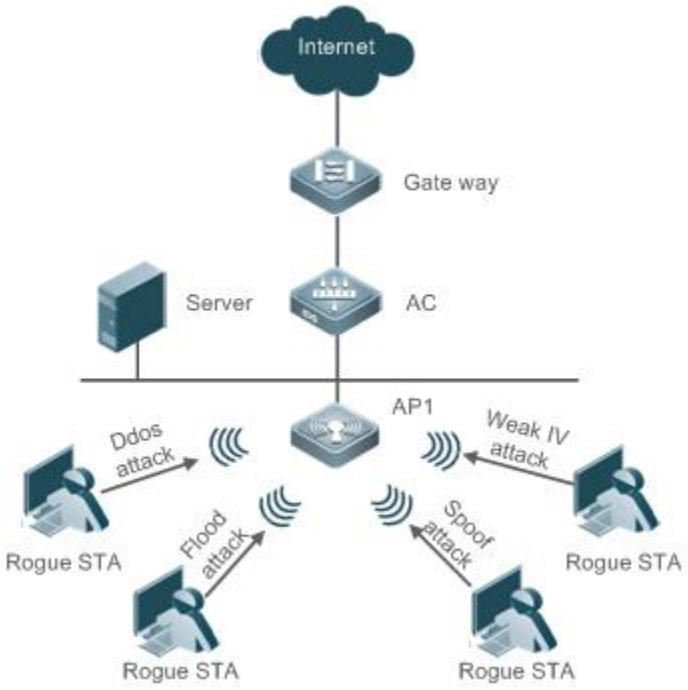
Scenario

Wireless invasion attacks exist on networks, including Distributed Denial of Service (DDoS), spoofing, flooding, and Weak initialization vector (IV) attacks. APs need to detect these attacks and implement countermeasures.

Assume that an AP needs to detect and defend against the following attacks:

- DDoS attacks
- Spoofing attacks
- Flooding attacks
- Weak IV attacks

Figure 2-3 Networking Topology of IDS



Deployment

The key configuration points for the devices are as follows:

- Enable DDoS attack detection and configure thresholds for collecting statistics on ARP, SYN, and ICMP attack packets from STAs. If any threshold is exceeded and the dynamic blocklist is enabled, the detection result is logged, and the STAs are added to the dynamic blocklist.

- Enable spoofing attack detection and configure thresholds for detecting deauthentication and disassociation packets. If any threshold is exceeded and the dynamic blocklist is enabled, the detection result is logged, and the STAs are added to the dynamic blocklist.
- Enable flood attack detection and configure thresholds for detecting Authentication, Association, Reassociation, Deauthentication, Disassociation, Probe, Null, and Action packets. If any threshold is exceeded and the dynamic blocklist is enabled, the detection result is logged, and the STAs are added to the dynamic blocklist.
- Enable weak IV attack detection and configure thresholds for detecting the IV values of web packets. If the number of consecutive attacks exceeds the threshold and the dynamic blocklist is enabled, the detection result is logged, and the STAs are added to the dynamic blocklist.

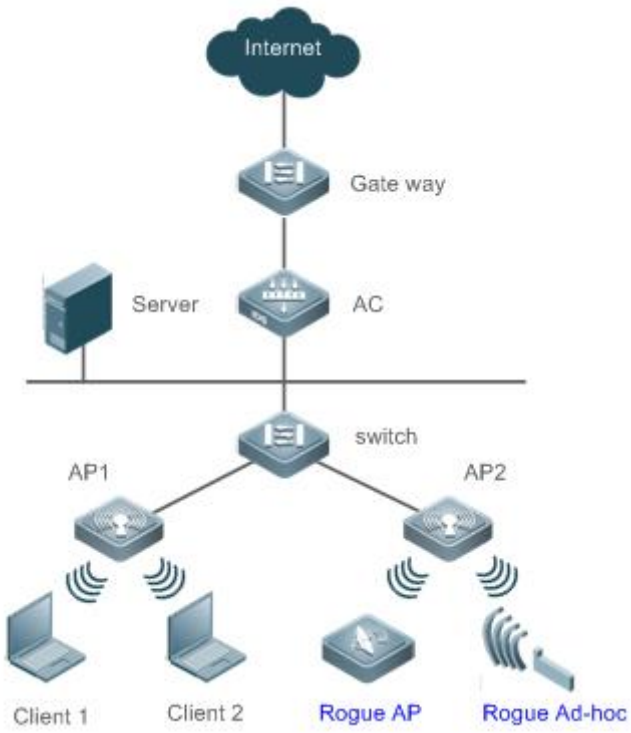
1.2.4 Rogue Detection and Containment

Scenario

Assume that there is the following deployment requirement on the network:

- Rogue AP and Ad-hoc devices exist on a network, and detection and containment are required.

Figure 2-4 Networking Topology of Rogue Detection and Containment



Deployment

The key configuration points for devices are as follows:

- Enable the monitor or hybrid mode for a specified AP. Then the AP starts the scanning timer and obtains scanning data at the end of each scanning period.
- Enable device containment and configure a containment mode.

- Regularly contain rogue APs and ad hoc devices based on the device containment mode and scanning data to prevent STAs from associating with counterfeit services.
- Before enabling AP containment to take effect, verify that the WLAN service is available on the AP; otherwise, the containment function is unavailable.

1.3 Features

Basic Concepts

Working Modes

WIDS has the following working modes:

- Normal mode: Provides only the access service.
- Monitor mode: Provides only the monitoring service.
- Hybrid mode: Provides both monitoring and access services.

IDS Detection Types

IDS provides detection of the following attacks:

- DDoS attacks, including ARP, ICMP, and SYN packets
- Flood attacks, including single-user and multi-user management packets
- Spoofing attacks, including broadcast disassociation and deauthentication attacks
- Weak IV attacks
- Interworking DoS attacks

User Isolation Modes

User isolation has the following modes:

- AC-based mode for isolating Layer 2 STAs connected to different APs associated with an AC.
- AP-based mode for isolating Layer 2 STAs connected to the same AP
- AC-SSID mode for isolating Layer 2 STAs connected to different APs associated with an AC on the same WLAN.
- AP-SSID-based mode for isolating Layer 2 STAs connected to the same AP on the same WLAN
- SSID-based mode for isolating Layer 2 STAs on a specified WLAN

Rogue Device Containment Modes

Rogue device containment has the following modes:

- Ad-hoc mode for containing the rogue Ad-hoc devices
- Rogue mode for containing the rogue devices with RSSIs exceeding the threshold
- SSID mode for containing unauthorized devices connected to the same SSID
- Config mode for containing unauthorized devices in the static attack list or SSID-based blocklist

Fuzzy Containment on Rogue APs

- Fuzzy match is performed based on the SSID of rogue APs. For example, if the fuzzy containment function is enabled and the SSID of the local AP is RUIJIE-WEB, rogue APs with the SSID of RU1JIE-WEB are contained.
- Fuzzy containment can be performed by keyword. For example, if the fuzzy containment function is enabled and the fuzzy containment keyword **ruijie** is configured, rogue APs with SSIDs that include **ruijie** such as **ruijie-free** are contained. The keyword is case-insensitive. For example, the keyword **ruijie** has 2^6 uppercase and lowercase combinations, and any of the combinations (such as **RUIjie** and **RuiJie**) can be matched for fuzzy containment.

Detected Devices

Rogue devices that can be detected are as follows:

- APs
- Ad-hoc devices
- Unknown STAs

Overview

Feature	Description
Frame Filtering	Uses frame filtering rules to filter the packets from STAs for STA access control.
IDS	Discovers and defends against malicious or unintentional attacks on WLANs in a timely manner.
User Isolation	Prevents insecure access between STAs on WLANs to avoid private information interception.
Rogue Device Detection and Containment	Monitors abnormal devices on the entire WLAN, helping network administrators discover potential risks on a network. Rogue device containment refers to containing rogue devices by sending fake deauthentication frames to addresses of the rogue devices in an attack list.

1.3.1 Frame Filtering

STA access control includes filtering based on low-rate STAs, allowlists, static blocklists, dynamic blocklists, SSID-based allowlists, and SSID-based blocklists.

Working Principle

Filtering Based on Low-Rate STAs

Filtering based on low-rate STAs is performed based on a filtering threshold. When the threshold is larger than 0, this function is enabled. If the STA rate is lower than this threshold, the STA's packets are discarded and this STA is disconnected.

Allowlist

The allowlist includes MAC addresses of allowed STAs. If the allowlist function is enabled, only allowlisted STAs can access the WLAN. Other STAs are forced to go offline and cannot access the WLAN, thereby reducing the impact of invalid packets on the WLAN.

Static Blocklist

The static blocklist includes the MAC address of denied STAs. If the static blocklist function is enabled, STAs in the static blocklist are forced to go offline and cannot access the WLAN.

Dynamic Blocklist

The dynamic blocklist includes the MAC addresses of denied STAs, which can be dynamically added by WIDS if IDS attacks are detected or manually configured. For example, if IDS attacks from a STA are detected on the WLAN, the MAC address of the STA can be dynamically added to the blocklist to prevent packet receiving from the STA, thereby ensuring WLAN security.

SSID-based Allowlist

The SSID-based allowlist includes the MAC addresses of the STAs that are allowed to access a WLAN with a specified SSID. You can configure the SSID-based allowlist on the CLI. If the SSID-based allowlist function is enabled, only the STAs in the allowlist of the specified WLAN are allowed to access. Other STAs cannot access the specified WLAN and online STAs that are not in the allowlist are forced to go offline, thereby reducing the impact of invalid packets on the WLAN.

SSID-based Blocklist

The SSID-based blocklist includes the MAC addresses of the STAs that are prevented from accessing a WLAN with a specified SSID. You can configure the SSID-based blocklist on the CLI. If the SSID-based blocklist function is enabled, STAs in the blocklist are forced to go offline and cannot access this WLAN.

1.3.2 IDS Attack Detection

To discover and defend against malicious or unintentional attacks on WLANs in a timely manner, WIDS can detect various types of attacks. When an attack is detected, an alarm or a log is generated to remind the network administrator to handle it. According to detection results, the network administrator can promptly adjust network configurations to eliminate insecure factors on the WLANs.

The following IDS attack detection types are supported:

- DDoS attack detection
- Flood attack detection
- Spoofing attack detection
- Weak IV attack detection
- Interworking DoS attack detection

Working Principle

DDoS Attack Detection

In DDoS attacks, an attacker sends a large number of attack packets to target devices in a short period to prevent authorized STAs from associating with the attacked devices. ARP packets, ICMP packets, and SYN packets can be identified.

The DDoS attack detection function of WIDS collects statistics on attacker's packets, determines whether the number of packets per second exceeds the configured threshold, and records the detection result in a log if the threshold is exceeded. If the dynamic blocklist function is enabled, the attacker address is added to the dynamic blocklist.

Flood Attack Detection

In flood attacks, an attacker sends a large number of packets of the same type in a short period. As a result, WLAN devices fail to process authorized STA requests.

Flood attack detection prevents flood attacks by continuously monitoring the traffic of each device. If the traffic within the specified period exceeds the upper limit set by the network administrator, the device is deemed as a flood attacker and is therefore blocked. Flood attack detection can be used with the dynamic blocklist function. In this case, if WIDS detects flood attacks, the STA initiating the attacks is added to the dynamic blocklist to protect the WLAN system against intrusions of this STA and ensure network security.

Spoofing Attack Detection

In spoofing attacks, an attacker sends spoofed packets by disguising as another STA. For example, a spoofed deauthentication packet can cause legal STAs to go offline.

WIDS performs detection on broadcast deauthentication and broadcast disassociation packets. When such packets are received, they are immediately defined as a spoofing attack and logged.

Weak IV Attack Detection

In weak IV attacks, an attacker intercepts packets with weak IVs on WLANs that use WEP encryption, cracks the shared key, and finally obtains encrypted information.

If a WLAN uses WEP encryption, an IV is generated for each packet. The IV and shared key are used as input to generate a key string. The key string and plaintext are encrypted to generate a ciphertext. When a WEP packet is sent, the IV used for packet encryption is also sent as a part of the packet header. If the IV is generated using an insecure method (for example, the same IV is frequently or always used), 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.

WIDS prevents weak IV attacks by identifying the IV of each WEP packet. When a packet with a weak IV is detected, WIDS immediately determines that a vulnerability exists and logs the detection result.

Interworking DoS Attack Detection

In interworking DoS attacks, every STA which is connected or tries to access, if the number of Action, Association, Authentication, Deauthentication, Disassociation, Reassociation, Probe Request, or Null data packets of each STA that is connected or tries to access is larger than the configured threshold, an attack occurs.

1.3.3 User Isolation

Because of mobility of STAs, STA information privacy is important in some scenarios (especially in public areas). Therefore, direct STA communication should be restricted. The user isolation technology can avoid insecure access (for example, through My Network Places) between STAs in WLAN coverage areas to prevent private information interception.

User isolation isolates STAs and prevents them from accessing each other without affecting normal network access, guaranteeing service security. User isolation has the following types:

- AP-SSID-based Layer 2 user isolation
- Inter-AP-SSID based Layer 2 user isolation
- AC-based user isolation

- AC-SSID-based user isolation
- Interworking 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.

Inter-AP-SSID-based Layer 2 User Isolation

Direct communication cannot be conducted between STAs who are associated with the same AP but with different SSIDs.

AC-based User Isolation

Direct communication cannot be conducted between Layer 2 STAs who are associated with the same AC but with different APs. This is effective only in centralized forwarding mode.

AC-SSID-based User Isolation

Direct communication cannot be conducted between STAs in the same WLAN who are associated with the same AC but with different APs. This is effective only in centralized forwarding mode.

Interworking User Isolation

Interworking user isolation depends on SSID-based isolation functions. It takes effect on APs in local forwarding mode and on ACs in centralized forwarding mode.

1.3.4 Rogue Device Detection and Containment

Network devices are typically classified into two types: unauthorized (rogue) and authorized. Rogue devices may have security vulnerabilities or may be manipulated by attackers, which poses a major threat or hazard to network security. The rogue device detection function of WIDS can monitor abnormal devices on the entire WLAN, helping a network administrator discover potential risks on networks.

Rogue detection is applicable to different rogue devices on WLANs, including APs, clients, wireless bridges, and ad hoc devices. Only detection of rogue APs, ad hoc devices, and unknown STAs is supported.

Rogue device containment refers to containing rogue devices by sending fake deauthentication frames to addresses of the rogue devices, in order to prevent STAs from accessing unauthorized services or access devices.

Working Principle

Rogue Device Detection

Rogue device detection is conducted by an AP in monitor or hybrid mode. WIDS obtains wireless packets by deploying some APs on WLANs and configuring them to operate in monitor or hybrid mode. By conducting analysis and statistics of monitored wireless packets, the APs can obtain information on rogue devices. Additionally, a network administrator can also configure unauthorized device detection rules to monitor abnormal devices on the entire WLAN.

Unknown STA Detection

The unknown STA detection function monitors the probe request packets from non-connected STAs on a network. Additionally, a network administrator can specify information on unknown STAs.

Rogue Device Containment

The rogue device containment function contains rogue devices that meet containment rules by simulating fake broadcast deauthentication packets, thereby preventing normal STAs from accessing rogue devices.

Unknown STA Containment

The unknown STA containment function denies access of unknown STAs by directly constructing deauthentication packets.

Interworking Rogue AP Detection

The function of interworking rogue AP detection is aimed at preventing unauthorized APs from interfering with authorized APs in signal transmission, and even preventing authorized STAs from being intercepted out of registration information. Based on rogue device detection, interworking rogue AP detection is used to terminate the network connection of unauthorized APs in collaboration with the background system if permitted.

1.4 Configuration

Configuration	Description and Command	
Configuring Frame Filtering	(Optional) It is used to configure frame filtering.	
	kickout threshold	Configures the threshold for disconnecting low-rate STAs.
	whitelist mac-address [**name** *another-name*]	Adds an entry to the allowlist.
	whitelist max	Configures the length of the allowlist.
	static-blacklist mac-address [**name** *another-name*]	Adds an entry to the static blocklist.
	static-blacklist max	Configures the length of the static blocklist.
	dynamic-blacklist enable	Enables the dynamic blocklist function.
	dynamic-blacklist lifetime	Configures the lifetime of the dynamic blocklist.
	dynamic-blacklist ac-max	Configures the length of the dynamic blocklist on ACs.
	dynamic-blacklist ap-max	Configures the length of the dynamic blocklist on APs.
	dynamic-blacklist mac-address	Configures dynamic blocklist entries.
	dynamic-blacklist mac-address [**name** *another-name*]	Adds an entry to the dynamic blocklist.
	ssid-filter max	Configures the SSID-based blocklist and allowlist and their length.

Configuration	Description and Command	
	ssid-filter blacklist mac-address [**name** *another-name*]	Adds an entry to the SSID-based blocklist.
	ssid-filter blacklist max	Configures the length of the SSID-based blocklist. The default value is 256.
	ssid-filter whitelist mac-address	Adds an entry to the SSID-based allowlist.
	ssid-filter whitelist max	Configures the length of the SSID-based allowlist. The default value is 256.
Configuring IDS	(Mandatory) It is used to configure IDS.	
	attack-detection enable	Specifies the IDS type.
	attack-detection ddos	Configures the packet rate threshold and interval of DDoS attack detection.
	attack-detection flood multi-mac	Configures the packet rate threshold and interval of multi-STA flood attack detection.
	attack-detection flood single-mac	Configures the packet rate threshold and interval of single-user flood attack detection.
	attack-detection spoof	Configures the packet rate threshold and interval of the spoofing attack detection.
	attack-detection weak-iv	Configures the packet rate threshold and interval of the weak IV attack detection.
	attack-detection statistics ac-max	Configures the length of IDS statistics on ACs.
	attack-detection statistics ap-max	Configures the length of IDS statistics on APs.
	dos-detection	Configures interworking DoS attack detection.
Configuring User Isolation	(Optional) It is used to configure user isolation.	
	user-isolation enable	Enables AC-based, AP-based, AC-SSID-based, AP-SSID-based and interworking Layer 2 user isolation.
	user-isolation permit-mac	Adds an entry to the allowed MAC address list for user isolation.
	user-isolation permit-mac max	Configures the length of the allowed MAC address list for user isolation.
Configuring Rogue Detection and Containment	(Optional) It is used to set device detection and containment.	
	countermeasures enable	Enables rogue device containment.
	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.

Configuration	Description and Command	
	countermeasures fuzzy-enable	Enables fuzzy containment.
	countermeasures fuzzy-keyword	Configures a keyword for fuzzy containment.
	device aging duration	Configures the aging duration of 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 blocklist.
	device max-black-ssid	Configures the length of the SSID-based blocklist.
	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 scan-para	Configures the interworking unauthorized AP detection.
	device detected-ap-max	Configures the maximum number of detected APs.
	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 channel scanning between different frequency bands.
	rogue-ap countermeasures enable	Enables interworking rogue AP containment.
Configuring the 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 frame filtering rules to enable packet filtering.

Notes

- A STA cannot be configured in both the static blocklist and the allowlist.
- A STA cannot be configured in both the blocklist and allowlist of the same SSID.

Configuration Steps

Configuring Low-Rate STA Filtering

- Optional.
- The **kickout threshold** command is used in WIDS configuration mode to configure the low-rate STA filtering threshold. The threshold must be larger than 0 to make the filtering function take effect.

Command	**kickout threshold** *rate*
Parameter Description	*rate*: Indicates the low-rate STA filtering threshold. The value range is from 0 to 130, in Mbps.
Defaults	By default, low-rate STAs are not filtered out, and the low-rate STA filtering threshold is 0.
Command Mode	WIDS configuration mode
Usage Guide	Set a low-rate STA filtering threshold as required.

Configuring STA Disconnection

- (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 to be disconnected.
Defaults	N/A
Command Mode	WIDS configuration mode
Usage Guide	This command can be used to disconnect a specified online STA.

Configuring an Allowlist

- Optional.
- Configure an allowlist entry on the AC that needs to be enabled with the allowlist function.
- Configure an allowlist length on the AC that needs to be enabled with the allowlist function.
- Run the **whitelist mac-address** command to add an entry to the allowlist in WIDS configuration mode. The allowlist function takes effect only after an effective allowlist entry is configured.
- Run the **whitelist max** command to configure the maximum number of entries in the allowlist in WIDS configuration mode.
- If an allowlist is configured, all online STAs whose addresses are not in the allowlist will be forced to go offline 1 minute after the last configuration command is executed.
- One *another-name* may map to multiple MAC addresses, but one MAC address can map to only one *another-name*.
- *another-name* is empty 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 an allowlist entry. **name** *another-name*: Indicates the alias of the MAC address in the allowlist. **max** *num*: Indicates the length of the allowlist. The value range is from 1 to 2048.
Defaults	By default, the allowlist is empty and the allowlist length is 1,024.
Command Mode	WIDS configuration mode
Usage Guide	The allowlist function takes effect only when the allowlist contains one or more entries.

Configuring a Static Blocklist

- Optional.
- Configure the static blocklist entry on the AC that needs to be enabled with the static blocklist function.
- Configure the static blocklist length on the AC that needs to be enabled with the static blocklist function.
- Run the **static-blacklist mac-address** command to add an entry to the static blocklist in WIDS configuration mode. The static blocklist-based filtering function takes effect only after an effective static blocklist entry is configured.
- Run the **static-blacklist max** command to configure the maximum number of entries in the static blocklist in WIDS configuration mode.
- After the MAC address of a STA is added to the static blocklist, 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*.
- *another-name* is empty 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 blocklist entry. **name** *another-name*: Indicates the alias of the MAC address in the static blocklist. **max** *num*: Indicates the length of the static blocklist. The value range is from 1 to 2048.
Defaults	By default, the static blocklist is empty and the static blocklist length is 1024.
Command Mode	WIDS configuration mode
Usage Guide	The static blocklist function takes effect only when the static blocklist contains one or more entries.

Configuring a Dynamic Blocklist

Whether this configuration is supported depends on the product version.

- Optional.
- Run the **dynamic-blacklist enable** command to enable the dynamic blocklist function in WIDS configuration mode. A dynamic blocklist entry is generated dynamically based on IDS attack detection and works only after the dynamic blocklist function is enabled.
- Run the **dynamic-blacklist lifetime** command to configure the lifetime of the dynamic blocklist in WIDS configuration mode, indicating how long the dynamic blocklist exists in the device.

- Run the **dynamic-blacklist** { **ac-max** | **ap-max** } command to configure the maximum number of dynamic blocklist entries on both ACs and 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* |**ac-max** *num* |**ap-max** *num* | **mac-address** *H.H.H* }
Parameter Description	**enable**: Enables the dynamic blocklist function **lifetime** *time*: Indicates the lifetime of the dynamic blocklist. The value range is from 60 to 86400, in seconds. **ac-max** *num*: Indicates the length of the dynamic blocklist on ACs. **ap-max** *num*: Indicates the length of the dynamic blocklist on APs. **mac-address** *H.H.H*: Indicates the MAC address of a dynamic blocklist entry.
Defaults	By default, the dynamic blocklist function is disabled, the length of a dynamic blocklist on an AC or AP is 2048, and its lifetime is 300 seconds.
Command Mode	WIDS configuration mode
Usage Guide	A dynamic blocklist entry is generated based on IDS attack detection.

Configuring the SSID-Based Blocklist

- Optional.
-
- Configure the SSID-based blocklist entry on the AC that needs to be enabled with the SSID-based blocklist function.
- Configure the SSID-based blocklist length on the AC that needs to be enabled with the SSID-based blocklist function.
- Configure the SSID list length on the AC that needs to be enabled with the SSID-based blocklist function.
- Run the **ssid-blacklist mac-address** command to add an entry to the SSID-based static blocklist in WIDS configuration mode. The static blocklist function takes effect only after an effective static blocklist entry is configured.
- Run the **ssid-filter blacklist max** command to configure the maximum number of entries in the SSID-based static blocklist in WIDS configuration mode.
- After the MAC address of a STA is added to the blocklist, 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*.
- *another-name* is empty 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 blocklist. The value range is from 1 to 128. The default value is 64. **blacklist mac-address** *H.H.H* **in-ssid** *string*: Adds an entry to the specified SSID-based blocklist. **name** *another-name*: Indicates the alias of the MAC address in the specified SSID-based blocklist.

	blacklist max *num*: Configures the length of the SSID-based blocklist. The value range is from 1 to 2048.
Defaults	The SSID-based blocklist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based blocklist contains one or more entries.

Configuring the SSID-Based Allowlist

- Optional.
- Configure the SSID-based allowlist entry only on the AC that needs to be enabled with the SSID-based allowlist function.
- Configure the SSID-based allowlist length only on the AC that needs to be enabled with the SSID-based allowlist function.
- Run the **ssid-filter whitelist mac-address** command to add an entry to the SSID-based allowlist in WIDS configuration mode. The allowlist function takes effect only after an effective allowlist entry is configured.
- Run the **ssid-filter whitelist max** command to configure the maximum number of entries in the SSID-based allowlist in WIDS configuration mode.
- After the SSID-based allowlist is configured, STAs that are not in the allowlist 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*.
- *another-name* is empty 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 allowlist entry for a specified SSID. **name** *another-name*: Indicates the alias of the MAC address in the specified SSID allowlist. **whitelist max** *num*: Configures the length of the SSID-based allowlist. The value range is from 1 to 2048.
Defaults	The SSID-based allowlist is empty.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the SSID-based allowlist contains one or more entries.

Verification

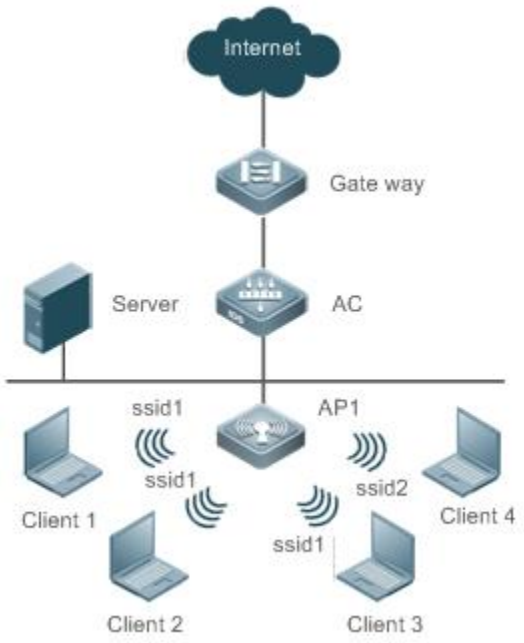
Verify functions based on corresponding frame filtering rules:

- Check the low-rate STA filtering function. The packets from the low-rate STAs are discarded and the low-rate STAs are successfully removed.
- Check the allowlist function. When the allowlist has an entry, the STAs not included in the allowlist cannot join the AP.
- Check the static blocklist function. When the static blocklist has an entry, the STAs in the static blocklist cannot join the AP.

- Check the dynamic blocklist function. When the dynamic blocklist function is enabled, entries are dynamically added to the dynamic blocklist based on IDS attack detection, and STAs in the dynamic blocklist cannot join the AP again.
- Check the SSID-based blocklist function. When the SSID-based blocklist has an entry, STAs in the SSID-based blocklist cannot access this SSID.
- Check the SSID-based allowlist function. When the SSID-based allowlist has an entry, STAs not included in the SSID-based allowlist cannot access this SSID.

Configuration Example

Configuring the Allowlist Entry

Scenario **Figure 2-5**	
Configuration Steps	● Add an entry to the allowlist on the AC.

	`Hostname# configure terminal`
	`Hostname(config)# wids`
	`Hostname(config-wids)# whitelist mac-address 0000.0000.0001`

Verification	After configuring the allowlist entry, you can use the following methods to check the configuration. ● Run the **show wids whitelist** command to display configured parameters. ● Associate the STA with this MAC address with the AC to verify whether the function has taken effect.

	`Hostname#show wids whitelist`
	`----------  Whitelist Information  ----------`
	`num  Mac-address`
	`1  0000.0000.0001`

Common Errors

N/A

1.4.2 Configuring IDS Attack Detection

Configuration Effect

- IDS attack detection can be used to discover and defend against malicious or unintentional attacks on WLANs in a timely manner.

Notes

- IDS attack detection needs to be used with the dynamic blocklist function to prevent attacks on WLANs more effectively.

Configuration Steps

Specifying the IDS Attack Detection Type

- Optional. IDS attack detection is disabled by default.
- Configure the IDS attack detection type.

Command	**attack-detection enable** { **all** | **ddos** | **flood** | **spoof** | **weak-iv** }
Parameter Description	**ddos**: Enables DDoS attack detection. **flood**: Enables flood attack detection. **spoof**: Enables spoofing attack detection. **weak-iv**: Enables weak IV attack detection. **all**: Enables all types of IDS attack detection.
Defaults	All types of IDS attack detection are disabled by default.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring DDoS Attack Detection

- Optional.
- Configure the packet rate thresholds and intervals for DDoS attack detection on different types of packets.

Command	**attack-detection ddos** { **arp-threshold** *num*| **icmp-threshold** *num*| **syn-threshold** *num* | **interval** *time* }
Parameter Description	**arp-threshold** *num*: Indicates the ARP packet rate threshold. The value range is from 1 to 10000, in pps. **icmp-threshold** *num*: Indicates the ICMP packet rate threshold. The value range is from 1 to 10000, in pps. **syn-threshold** *num*: Indicates the SYN packet rate threshold. The value range is from 1 to 10000, in pps. **interval** *time*: Indicates the interval of DDoS attack detection. The value range is from 10 to 60, in seconds.

Defaults	By default, the interval of DDoS attack detection is 30 seconds, and the DDoS attack detection thresholds for ARP packets, ICMP packets, and SYN packets are 50 pps, 100 pps, and 50 pps, respectively.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Flood Attack Detection

Whether this configuration is supported depends on the product version.

- Optional. Flooding attack detection is disabled by default.
- Configure the packet rate thresholds and intervals for flood attack detection on different types of packets.
- Run the **attack-detection flood single-mac** { **total** | **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold***num***interval***time* command to configure the packet rate threshold and interval of a specified type of packets for single-STA flood attack detection in WIDS configuration mode.
- Run the **attack-detection flood multi-mac** { **assoc** | **reassoc** | **disassoc** | **probe** | **action** | **auth** | **deauth** | **null-data** } **threshold** *num* **interval** *time* command to configure the packet rate threshold and interval of a specified type of packets for multi-STA flood attack detection in WIDS configuration mode.

Command	**attack-detection flood single-mac** { **total**	**assoc**	**reassoc**	**disassoc**	**probe**	**action**	**auth**	**deauth	null-data** } **threshold** *num* **interval** *time*
Parameter Description	**single-mac**: Configures single-STA attack detection. **total**: Configures all packets. **assoc**: Configures Association packets. **reassoc**: Configures Reassociation packets. **disassoc**: Configures Disassociation packets. **probe**: Configures Probe packets. **action**: Configures Action packets. **auth**: Configures Authentication packets. **deauth**: Configures Deauthentication packets. **null-data**: Configures Null packets. *num*: Indicates the packet rate threshold of flood attack detection. The value range is from 1 to 10000. *time*: Indicates the interval of flood attack detection. The value range is from 10 to 60, in seconds.
Defaults	By default, the packet rate thresholds for all types of single-STA and multi-STA flood attack detection are 300 and 4800, respectively, and the statistical interval is 10 seconds.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Command	**attack-detection flood multi-mac** { **assoc**	**reassoc**	**disassoc**	**probe**	**action**	**auth**	**deauth	null-data** } **threshold** *num* **interval** *time*
Parameter Description	**multi-mac**: Configures multi-STA detection. **assoc**: Configures Association packets. **reassoc**: Configures Reassociation packets.

	disassoc: Configures Disassociation packets. **probe**: Configures Probe packets. **action**: Configures Action packets. **auth**: Configures Authentication packets. **deauth**: Configures Deauthentication packets. **null-data**: Configures Null packets. *num*: Indicates the packet rate threshold of flood attack detection. The value range is from 1 to 10000. *time*: Indicates the interval of flood attack detection. The value range is from 10 to 60, in seconds.
Defaults	By default, the packet rate thresholds for all types of single-STA and multi-STA flood attack detection are 300 and 4800, respectively, and the statistical interval is 10 seconds.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring Spoofing Attack Detection

- Optional. Spoofing attack detection is disabled by default.
- Configure the packet rate thresholds and intervals for spoofing attack detection on different types of packets.

Command	**attack-detection spoof** { **threshold** *num* |**interval** *time* }
Parameter Description	**threshold** *num*: Indicates the packet rate threshold of spoofing attack detection. The value range is from 1 to 1000. **interval** *time*: Indicates the interval of spoofing attack detection. The value range is from 10 to 60, in 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.
- Configure the packet rate thresholds and intervals for weak IV attack detection on different types of packets.

Command	**attack-detection weak-iv** { **threshold** *num*| **interval** *time* }
Parameter Description	**threshold** *num*: Indicates the packet rate threshold of weak IV attack detection. The value range is from 1 to 10000. **interval** *time*: Indicates the interval of weak IV attack detection. The value range is from 1 to 60, in seconds.
Defaults	By default, the interval of weak IV detection is 15 seconds and the detection threshold is 10.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Length of the IDS Attack Detection List on the AC

- Optional.

Command	**attack-detection statistics ac-max** *num*
Parameter Description	*num*: Indicates the maximum number of IDS attack detection entries on the AC. The value range is from 1 to 4096.
Defaults	It is 2048 by default.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Length of IDS Attack Detection Statistics on APs

- Optional.

Command	**attack-detection statistics ap-max** *num*
Parameter Description	*num*: Indicates the length of IDS attack detection statistics on APs. The value range is from 1 to 1024.
Defaults	The default value is 512.
Command Mode	WIDS configuration mode
Usage Guide	N/A

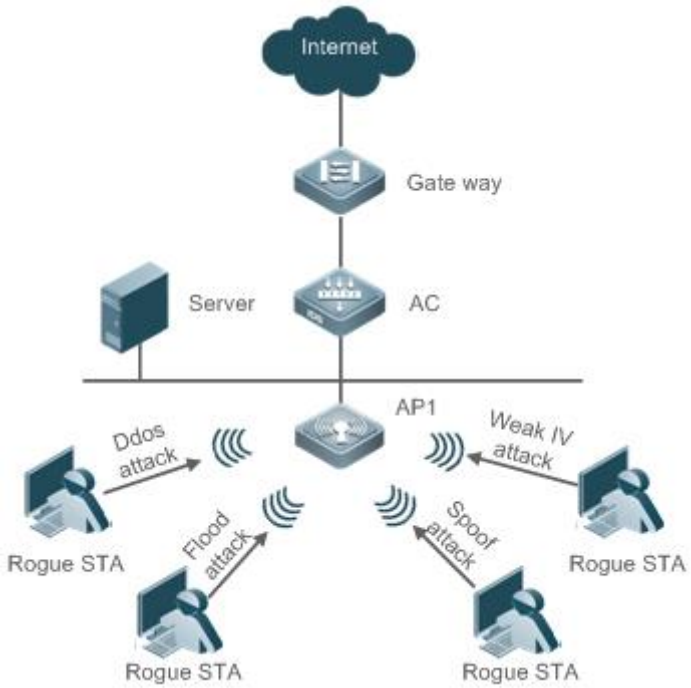
Verification

Verify detection functions based on the IDS attack detection type:

- DDoS attack detection: Check whether ARP packet attacks, ICMP packet attacks, and SYN packet attacks are detected.
- Flood attack detection: Check whether multi-STA flood attacks and single-STA flood attacks are detected.
- Spoofing attack detection: Check whether broadcast disassociation and deauthentication packet attacks are detected.
- Weak IV attack detection: Check whether weak IV packet attacks are detected.
- Interworking DoS attack detection: Check whether DoS attacks are detected.

Configuration Example

Configuring DDoS Attack Detection

Scenario **Figure 2-6**	
Configuration Steps	● Specify DDoS attack detection and configure the threshold and interval on the AC.

	`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 displayed on the AC.

	`*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 user isolation rules.

Notes

- User isolation is only valid for Layer 2 STAs.

Configuration Steps

Configuring a User Isolation Mode

- Optional.
- Unless otherwise noted, configure this function on ACs.

Command	**user-isolation** { **ac** | **ap** | **ssid-ac** | **ssid-ap** | **wlan-id** *num* } **enable**
Parameter Description	**ac**: Configures AC-based Layer 2 user isolation. **ap**: Configures AP-based Layer 2 user isolation. **ssid-ac**: Configures AC-SSID-based Layer 2 user isolation. **ssid-ap**: Configures AP-SSID-based Layer 2 user isolation **wlan-id** *num*: Configures SSID-based Layer 2 user isolation.
Defaults	User isolation is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The AC-based and AC-SSID-based Layer 2 user isolation modes take effect only in centralized forwarding mode.
	Whether this configuration is supported depends on the product version.

Configuring the Allowed MAC Address List for User Isolation

- Optional.
- Unless otherwise specified, configure this function on the AC.
- To cConfigure the length of the allowed MAC address list for user isolation.

Command	**user-isolation permit-mac** { *H.H.H* | **max** *num* }
Parameter Description	*H.H.H*: Indicates the allowed MAC address list entry for user isolation. **max** *num*: Indicates the length of the allowed MAC address list for user isolation. The value range is from 1 to 1024.
Defaults	By default, the allowed MAC address list for user isolation is empty, and the list length is 1024.
Command Mode	WIDS configuration mode
Usage Guide	N/A

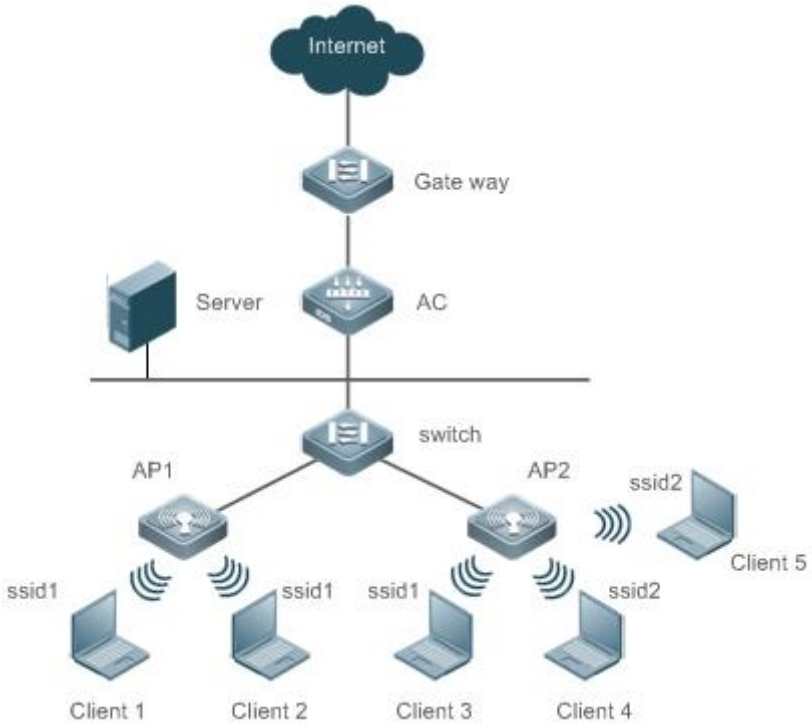
Verification

- Verify functions based on the isolation mode.

Configuration Example

Configuring User Isolation

Scenario	

Figure 2-7	
Configuration Steps	● Configure AP-based Layer 2 user isolation on the AC.

	`Hostname# configure terminal`
	`Hostname(config)# wids`
	`Hostname(config-wids)# user-isolation ap enable`

Verification	● Run the **show running-config** command to display configured parameters.

	`Hostname#show running-config`
	`…`
	`!`
	`wids`
	` user-isolation ap enable`
	`!`

Common Errors

N/A

1.4.4 Configuring Rogue Detection and Containment

Configuration Effect

Rogue device detection and containment can contain unauthorized devices and maintain WLAN security.

Notes

The rogue device detection and containment function takes effect only when the AP works in hybrid or monitor mode.

Configuration Steps

Enabling Rogue Device Containment

- Optional.
- Run the **countermeasures enable** command to enable rogue device containment in WIDS configuration mode.

Command	**countermeasures enable**
Parameter Description	N/A
Defaults	By default, rogue device containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Configuring the Rogue Device Containment Interval

- Optional. Run the **countermeasures interval** *time* command to configure the interval of rogue device containment in WIDS configuration mode.

Command	**countermeasures interval** *time*
Parameter Description	time: Indicates the rogue device containment interval. The value range is from 100 to 10000, in milliseconds.
Defaults	The default containment interval is 1000 ms.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Configuring the Rogue Device Detection and Containment Mode

- Optional.
- Run the **countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** } command to configure the rogue device detection and containment mode in WIDS configuration mode.

Command	**countermeasures mode** { **all** | **adhoc** | **config** | **rogue** | **ssid** }
Parameter Description	**adhoc**: Configures ad hoc containment mode to contain ad hoc devices. **config**: Configures config containment mode to contain devices that meet entries in the SSID-based blocklist and static attack list. **rogue**: Configures rogue containment mode to contain devices with RSSIs exceeding the threshold. **ssid**: Configures SSID containment mode to contain devices connected to the same SSID but different ACs. **all**: Configures all the preceding containment modes.
Defaults	By default, no rogue device containment mode is specified.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works 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 entry of a static attack list. **max** *num*: Indicates the length of the static attack list. The value range is from 1 to 1024.
Defaults	By default, the static attack list is empty, and the length of the static attack list is 512.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Configuring the SSID-based Blocklist

- Optional.
- Run the **device black-ssid** *ssid* command to configure the SSID-based blocklist information in WIDS configuration mode.

Command	**device { black-ssid** *ssid* |**max-black-ssid** *num* }
Parameter Description	**black-ssid** ssid: Indicates the SSID-based blocklist entry. **max-black-ssid** *num*: Indicates the length of the SSID-based blocklist. The value range is from 1 to 1024.
Defaults	By default, the SSID-based blocklist is empty and the length of the SSID-based blocklist is 512.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Configuring the Lists of Allowed MAC Addresses, SSIDs, and Vendors

- Optional.
- Run the **device permit mac-address** *H.H.H* command to configure the allowed MAC address list entry in WIDS configuration mode.
- Run the **device permit ssid** *ssid* command to configure the allowed SSID list entry in WIDS configuration mode.
- Run the **device permit vendor bssid** *H.H.H* command to configure the allowed 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 allowed MAC address list entry. It is empty by default. **mac-address max** *num*: Indicates the length of the allowed MAC address list. The value range is from 1 to 2048. The default value is 1024. **ssid** *ssid*: Indicates the allowed SSID list entry. It is empty by default. **max-ssid** *num*: Indicates the length of the allowed SSID list. The value range is from 1 to 1024. The default value is 512. **vendor bssid** *H.H.H*: Indicates the allowed vendor list entry. It is empty by default. **vendor bssid max** *num*: Indicates the length of the allowed vendor list. The value range is from 1 to 1024. The default value is 512.

Defaults	See **Parameter Description**.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Configuring the Maximum Number of Contained Devices in One Containment

- Optional.
- Run the **countermeasures ap-max** *ap-num* command to configure the maximum number of contained devices in one rogue device containment in WIDS configuration mode.

Command	**countermeasures ap-max** *ap-num*
Parameter Description	*ap-num*: Indicates the maximum number of devices contained in each containment interval. The value range is from 1 to 256.
Defaults	By default, the maximum number of contained devices in one containment is 30.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Configuring the Aging Duration of Detected Devices

- Optional.
- Run the **device aging duration** *time* command to configure the aging duration of detected devices in WIDS configuration mode.

Command	**device aging duration** *time*
Parameter Description	*time*: Indicates the aging duration of detected devices. The value range is from 500 to 5000, in seconds.
Defaults	The default aging duration is 1200 seconds.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works 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 AP can identify devices on the same AC.

Command	**device friendly-flags***value*
Parameter Description	*value*: Indicates the device friendly flag. The value range is from 1 to 4294967295.
Defaults	The default value is 0.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Configuring the Minimum RSSI for Containment

- Optional.
- Run the **countermeasures rssi-min** *num* command to configure the minimum RSSI for rogue device containment in WIDS configuration mode. A rogue device with an RSSI exceeding this threshold will be contained.
- Unless otherwise specified, configure this function on the AC where logs need to be written into the memory buffer.

Command	**countermeasures rssi-min** *num*
Parameter Description	*num*: Indicates the minimum RSSI for rogue device containment. The value range is from 0 to 75 (–95 to –20 dBm).
Defaults	The default minimum RSSI for containment is 25 (–70 dBm).
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Enabling Channel-Based Containment

- Optional. Run the **countermeasures channel-match** command to enable the channel-based containment function in WIDS configuration mode. This function enables containment based on the channel on which a detected rogue device operates.
-

Command	**countermeasures channel-match**
Parameter Description	**channel-match**: Enables channel-based containment.
Defaults	By default, channel-based containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Configuring Fuzzy Containment

- Optional.
- Run the **countermeasures fuzzy-enable** command to configure the fuzzy containment function in WIDS configuration mode. This function enables fuzzy match for the SSIDs of rogue APs. For example, if the SSID of the local AP is TEST-WEB, the rogue AP whose SSID is TE1ST-WEB can be contained after the fuzzy containment function is enabled.

Command	**countermeasures fuzzy-enable**
Parameter Description	N/A
Defaults	By default, the fuzzy containment function is disabled.
Command Mode	WIDS configuration mode
Usage Guide	If containment modes include the config containment mode, rogue APs whose SSIDs are similar to those in the SSID-based blocklist are contained. If containment modes include the SSID containment mode, rogue APs whose SSIDs are similar to the SSID of the local AP are contained. Fuzzy containment takes effect only in config 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**.

Command	**countermeasures fuzzy-keyword** *string*
Parameter Description	*strin*g: Indicates the fuzzy containment keyword, which is case-insensitive and saved in lowercase.
Defaults	By default, no fuzzy containment keyword is configured.
Command Mode	WIDS configuration mode
Usage Guide	The configuration takes effect only after the **countermeasures fuzzy-enable** command is executed. When the containment modes include the SSID containment mode, rogue APs whose SSIDs contain the configured keyword will be contained. The fuzzy containment keyword takes effect only in SSID containment 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. The list is empty by default. **mac-address max** *num*: Configures the length of the unknown STA list. The value range is from 1 to 256.
Defaults	By default, unknown STA detection and containment is disabled.
Command Mode	WIDS configuration mode
Usage Guide	The containment function does not take effect when the AP works in normal mode.

Enabling Unknown STA Detection Information Reporting

- Optional.
- This command is used to report detected unknown STAs to the AC.
- Run the **device unknown-sta report enable** command to enable unknown STA detection information reporting in WIDS configuration mode.

Command	**device unknown-sta report enable**
Parameter Description	N/A
Defaults	By default, the unknown STA detection information reporting function is disabled.
Command Mode	WIDS configuration mode
Usage Guide	This function takes effect only when the AP does not operate in normal mode. The scanning result can be reported to the AC.
	Whether this configuration is supported depends on the product version.

Configuring Interworking Rogue Device Detection

- Optional.
- Run the **device channel-bind radio** *radio-id* { **channel** *num*| **max-cycles** *value* } command to configure the scanning channel of a specified radio for interworking rogue device detection in AP configuration mode.
- Run the **device scan-para** { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } | **ap-mode** { **normal** | **monitor** } } command to configure scanning parameters for detection of interoperability with rogue APs in AP configuration mode.
- Run the **rogue-ap countermeasures enable** command to configure the function of containing interoperability with rogue APs in WIDS configuration mode.
- Configure scanning channel information on interoperability with rogue APs.

Command	**device channel-bind radio** *radio-id*{ **channel** *num* | **max-cycles** *value* }
Parameter Description	*radio-id*: Indicates the radio ID of a specified AP. **channel** *num*: Indicates the channel number. The Chinese channel is used by default. **max-cycles** *value*: Indicates the scanning count. The value is 10 by default and the value range is from 0 to 255.
Defaults	For details, see **Parameter Description**.
Command Mode	AP configuration mode
Usage Guide	N/A
	Whether this configuration is supported depends on the product version.

Command	**device scan-para** { **radio** *radio-id* **scan-type** { **active** | **passive** } **device-detect** { **enable** | **disable** } **|** **ap-mode** { **normal** | **monitor** } }
Parameter Description	**radio** *radio-id*: Indicates the radio ID. **scan-type active**: Indicates active scanning. Passive scanning is used by default. **scan-type passive**: Indicates passive scanning. **device-detect enable**: Enables detection. Detection is disabled by default. **device-detect disable**: Disables detection. **ap-mode normal**: Indicates that the AP works in normal mode. **ap-mode monitor**: Indicates that the AP works in monitor mode.
Defaults	For defaults, see **Parameter Description**.
Command	AP configuration mode

Mode	
Usage Guide	N/A

Command	**rogue-ap countermeasures enable**
Parameter Description	N/A
Defaults	By default, this function is disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring the Maximum Number of Detected APs in the List

- Optional.
- Run the **device detected-ap-max** *num* command to configure the maximum number of detected APs in WIDS configuration mode. A smaller value indicates that a smaller amount of data will be detected on the AP, which affects the device containment function. A larger value requires a larger memory space.

Command	**device detected-ap-max** *num*
Parameter Description	*num*: Indicates the maximum number of detected APs in the list. The value range is from 1 to 4096.
Defaults	The default maximum number of detected APs in the list is 2048.
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 the scanning status of a radio is disabled, the AP works in non-normal mode, and no device detection data can be obtained.

Command	**hybrid-scan radio** *num* **{ enable	disable }**
Parameter Description	*num*: Indicates a radio ID.
Defaults	By default, scanning on all radios is enabled.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring the Scanning Channel of a Specified AP

- Optional.
- Run the **scan-channels** { **802.11a** | **802.11b** | **6GHz** } **channels** *channels* command to configure the scanning channel in AP configuration mode. If no scanning channel is configured, the AP works in non-normal mode, and no device detection data can be obtained.

Command	**scan-channels { 802.11a | 802.11b** | **6GHz } channels** *channels*
Parameter Description	*num*: Indicates the number of the scanning channel. Multiple parameters can be input, separated by spaces.
Defaults	By default, the scanning channel is empty.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring Automatic Radio Switchover and Scanning

- Optional.
- Run the **scan-channels** { **dual-band** | **all-band** } **radio** *radio-id* command to configure automatic dual-radio switchover and scanning. The scanning results of two radios can be obtained for containment.

Command	**scan-channels** { **dual-band** | **all-band** } **radio** *radio-id*
Parameter Description	*radio-id*: Indicates the radio ID for multi-radio switchover.
Defaults	By default, automatic multi-radio switchover and scanning is disabled.
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.

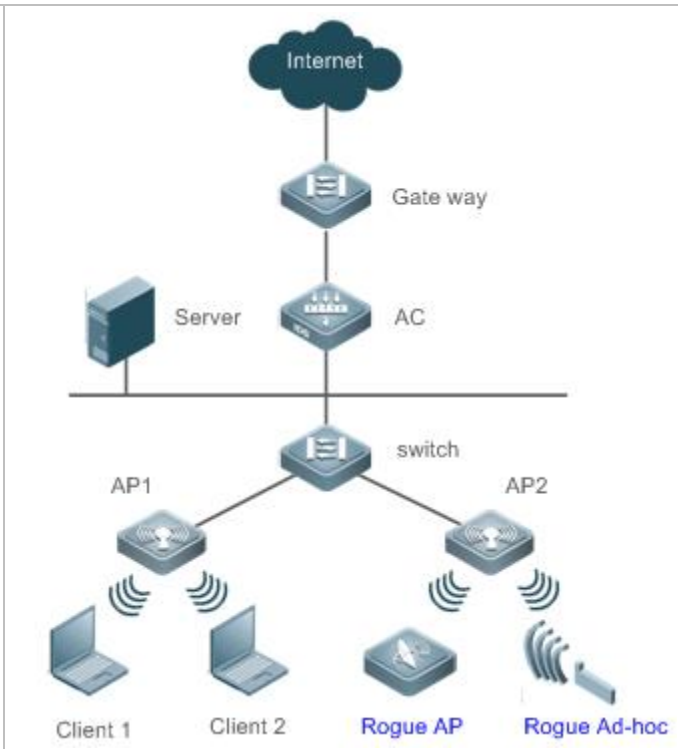
Verification

- Run the **show wids detected** command to display detected results.

Configuration Example

Configuring Rogue Device Containment

Scenario	

Figure 2-8	
Configuration Steps	● Configure rogue device containment information on the AC. Before configuring containment, confirm that the WLAN service has been deployed on the contained AP; otherwise, 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 configured parameters and the log information generated by the system.

	`Hostname#show running-config`
	`Hostname#show running-config`
	`...`
	`!`
	`wids`
	` countermeasures enable`
	` countermeasures mode SSID`
	`!`
	`...`

Common Errors

N/A

1.4.5 Configuring the AP Working Mode

Whether this function is supported depends on the product version.

Configuration Effect

- APs in different working modes can provide different services.

Notes

N/A

Configuration Steps

Configuring an AP Working Mode

- Optional.
- Unless otherwise specified, configure this function on each AP.

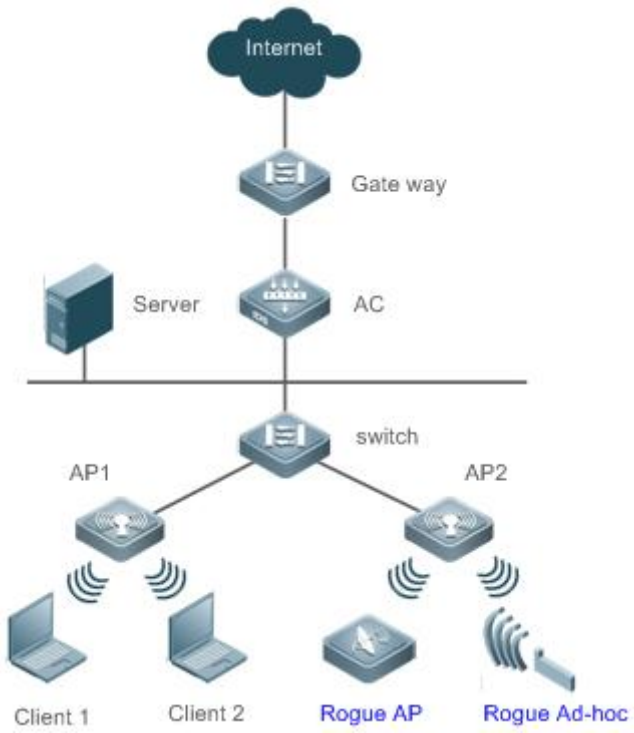
Command	**device mode** { **hybrid** | **monitor** [**radio** *radio-id*] | **normal** }
Parameter Description	**hybrid**: Configures the hybrid mode, in which the device provides both monitoring and access services. **monitor:** Configures the monitor mode, in which the device provides only the monitoring service. *radio-id*: Specifies a radio ID. The value range is from 1 to 96. **normal**: Configures the normal mode, in which the device provides only the access service.
Defaults	By default, an AP works in normal mode.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

- Run the **show ap-config running** *ap-name* command to display the working mode of the AP.

Configuration Example

Configuring the AP Working Mode

Scenario **Figure 2-9**	
Configuration Steps	● Configure the working mode of a specified AP on the AC.

	`Hostname# configure terminal`
	`Hostname(config)# ap-config ap220`
	`Ruijie (config-ap)#device mode hybrid`

Verification	● Run the **show ap-config running** *ap-name* command to display configured parameters.

	`Hostname#show ap-config running ap220`
	`!`
	`ap-config ap220`
	` device mode hybrid`
	` 11acsupport enable radio 1`
	` 11acsupport enable radio 2`
	` 802.11n mcs support 23 radio 1`
	` 802.11n mcs support 23 radio 2`
	` 802.11ac mcs support 29 radio 1`
	` 802.11ac mcs support 29 radio 2`
	` antenna receive 7 radio 1`
	` antenna receive 7 radio 2`
	` antenna transmit 7 radio 1`
	` antenna transmit 7 radio 2`
	`!`

Common Errors

N/A

1.5 Monitoring

Clearing

Command	Description
reset attack-list all	Clears entries in the static attack list.
reset black-ssid all	Clears entries in the SSID-based blocklist.
reset detected { all | adhoc | rogue { ap | client } | mac-address *H.H.H* **}**	Clears information about a specified device that is detected.
reset dos-detected	Clears interworking DoS attack detection information.
reset dynamic-blacklist { all | mac-address *H.H.H* **}**	Clears entries in the dynamic blocklist.
reset fuzzy-keyword all	Clears the configuration of fuzzy containment keywords.
reset permit-mac all	Clears entries in the allowed MAC address list.
reset permit-ssid all	Clears entries in the allowed SSID list.
reset permit-vendor all	Clears entries in the allowed vendor list.
reset rogue-ap detected	Clears information about interworking rogue AP device detection.
reset ssid-filter { ssid all | in-ssid *ssid* **}**	Clears all or specified entries in the SSID-based blocklist and allowlist.
reset ssid-filter { blacklist all | in-ssid *ssid* **}**	Clears all or specified entries in the SSID-based blocklist.
reset ssid-filter { whitelist all | in-ssid *ssid* **}**	Clears all or specified entries in the SSID-based allowlist.
reset static-blacklist all	Clears entries in the static blocklist.
reset statistic all	Clears information about the static attack statistic list.
reset unknown-sta all	Clears entries in the unknown STA list.
reset user-isolation-permit-list all	Clears allowed entries for user isolation.
reset whitelist all	Clears allowlist entries.

Displaying

Command	Description
show wids attack-list	Displays the attack list configuration.
show wids blacklist { **dynamic** | **static** }	Displays the dynamic or static blocklist configuration.
show wids black-ssid	Displays the SSID-based blocklist configuration.
show wids detected { **adhoc** | **all** | **friendly ap** |**interfering ap** | **rogue** { **adhoc-ap** | **ap** | **client** | **config-ap** | **ssid-ap** } | **mac-address** *H.H.H* }	Displays information about detected devices of a specified type.
show wids ssid-filter { **blacklist all** [**in-ssid** *string*] | **ssid all** | **whitelist all** [**in-ssid string**] }	Displays the SSID-based blocklist and allowlist configuration.
show wids permitted { **mac-address** | **ssid** | **vendor** }	Displays the configuration of allowed MAC, SSID, and vendor lists.
show wids statistics	Displays IDS attack detection information.

show wids unknown-sta	Displays the unknown STA list configuration.
show wids user-isolation permit-mac	Displays allowed MAC entries for user isolation.
show wids whitelist	Displays allowlist entries.
show running-config	Displays other WIDS configuration.
show wids dos-detected	Displays interworking DoS detection information.
show wids rogue-ap detected	Displays interworking rogue device detection information.
show wids fuzzy-keyword	Displays the configuration of fuzzy containment keywords.

Configuring WLAN Authentication

1. Configuring AAA
2. Configuring RADIUS
3. Configuring TACACS
4. Configuring IEEE 802.1X
5. Configuring Local EAP
6. Configuring Web-based Authentication
7. Configuring ROLE-MGMT
8. Configuring SCC
9. Configuring GSN

1 Configuring AAA

1.1 Overview

Authentication, authorization, and accounting (AAA) provides a unified framework for configuring authentication, authorization, and accounting services.

AAA provides the following services in a modular way:

- Authentication: Authenticates user identities for network access and network services. Authentication is classified into local authentication and authentication through Remote Authentication Dial In User Service (RADIUS) and Terminal Access Controller Access Control System+ (TACACS+).
- Authorization: Grants specific network services to users according to a series of defined attribute-value (AV) pairs. The pairs describe the operations which users are authorized to perform. AV pairs are stored on network access servers (NASs) or remote authentication servers.
- Accounting: Tracks resource usage 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 accounting, statistics, and tracking of network resource usage.

AAA is the main access control method. The device also provides other simple access control functions, such as local username authentication and online password authentication. Compared to them, AAA offers higher 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.

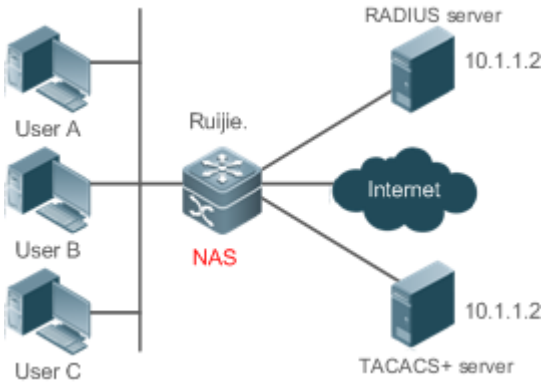
1.2.1 Configuring AAA in a Single-Domain Environment

Scenario

In the network scenario shown in Figure 2-1, the following application requirements must be satisfied to improve security management on the NAS:

1. To facilitate account management and avoid information disclosure, each administrator has an individual account the unique username and password.
2. To access the NAS, users are required to pass identity authentication. This authentication process can be in local or centralized mode. You are advised to combine the two modes, with centralized mode as the primary option and local mode as the backup. In centralized authentication mode, users must undergo authentication by the RADIUS server first. If the RADIUS server does not respond, local authentication is used.
3. During authentication, users can be restricted from accessing specific network devices.
4. Rights-based management: Network management users are classified into the super user and common user. Super users have the rights to view and configure the NAS, and common users are only allowed to view the NAS configuration.
5. AAA records of users are stored on servers and can be viewed and referenced for auditing (TACACS+ is used for accounting in this example).

Figure 2-1



Remarks	User A, User B, and User C are connected to the NAS in wired or wireless mode. The RADIUS server can be the Windows 2000/2003 Server (IAS), UNIX system component, and dedicated server software provided by a vendor. The TACACS+ server can be the dedicated server software provided by a vendor.

Deployment

- Enable AAA on the NAS.
- Configure an authentication server on the NAS.
- Configure local users on the NAS.
- Configure authentication on the NAS.
- Configure authorization on the NAS.
- Configure accounting on the NAS.

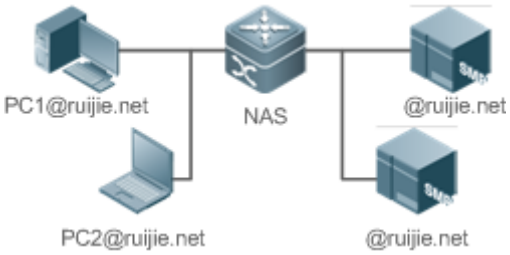
1.2.2 Configuring AAA in a Multi-Domain Environment

Scenario

Configure the domain-based AAA service on the NAS.

- A user can log in by entering the username **PC1@ruijie.net** or **PC2@ruijie.com.cn** and correct password on an 802.1X client.
- Rights-based management: Network management users are classified into the super user and common user. Super users have the rights to view and configure the NAS, and common users are only allowed to view the NAS configuration.
- AAA records of users are stored on servers and can be viewed and referenced for auditing.

Figure 2-2



Remarks	The clients with the usernames **PC1@ruijie.net** and **PC2@ruijie.com.cn** are connected to the NAS in wired or wireless mode. The NAS is an access device. 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 input passwords are verified by the user database on the NAS.

Remote server authentication is the process where input passwords are verified by the database on a remote server. It is mainly implemented by the RADIUS server and TACACA+ server.

↘ Method List

AAA is implemented using different security methods. A method list defines a method implementation sequence, and can contain one or more security protocols so that a standby method can be available when the first method becomes unavailable. The device uses the first method in the list in the beginning and then the next if there is no response for the first method. 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 defines one or more security protocols used for authentication, so that the standby authentication method is used when the active security method becomes unavailable. The device uses the first method in the list in the beginning and then the next if there is no response for the first method. 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.

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 2-3

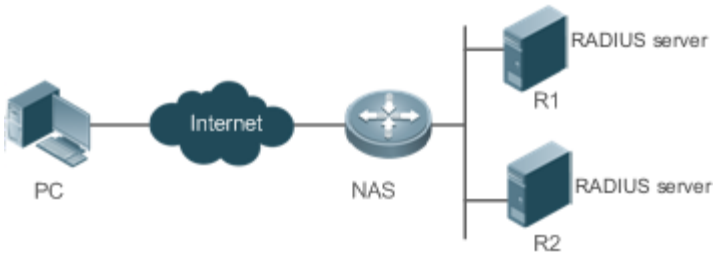


Figure 2-3 shows a typical AAA network topology, where two RADIUS servers (R1 and R2) and one NAS are deployed. The NAS can be the client for the RADIUS servers.

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 user passes authentication on R1, 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 and the connection is terminated. If R1 does not respond, the NAS considers that the R1 method times out and continues to query the user's identity on R2. This process continues as the NAS keeps trying the remaining authentication methods, until the user request is authenticated, rejected, or terminated. If all the authentication methods are responded with Timeout, authentication fails and the connection will be terminated.

The Reject response is different from the Timeout response. The Reject response indicates that the user does not meet the criteria of the available authentication database and therefore fails in authentication, and the Internet access request is denied. The Timeout response indicates that the authentication server fails to respond to the identity query. When detecting a timeout event, AAA proceeds to the next method in the list to continue the authentication process.

This document describes how to configure AAA on the RADIUS server. For details about TACACS+, see *Configuring TACACS+*.

AAA Server Group

You can define an AAA server group to include one or more servers of the same type. If the server group is referenced by a method list, the NAS preferentially sends requests to the servers in the referenced server group when the method list is used to implement AAA.

Overview

Feature	Description
AAA Authentication	Authenticates user identities for accessing the Internet.
AAA Authorization	Determines services or permissions users can enjoy.
AAA Accounting	Records the network resource usage of users.

Multi-Domain AAA	Creates domain-specific AAA schemes for users in different domains.

1.3.1 AAA Authentication

Authentication, authorization, and accounting are three independent services. Authentication user identities for accessing the Internet. During authentication, the username, password, and other user information are exchanged between devices to complete users' access or service requests. You can choose to 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. The defined authentication methods must be implemented by specified applications except 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. This method is not used in most situations.

- 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 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 centralized and unified authentication of multiple devices with high reliability. You can configure local authentication as the backup to avoid authentication failures when all the servers in the server group fail.

AAA Authentication Types

The device supports 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, or File Transfer Protocol (FTP).

- Enable authentication

After users log in to the CLI of the NAS, they must be authenticated before CLI permission update. This process is called Enable authentication in privileged EXEC mode.

- PPP authentication

PPP authentication is performed for the users that initiate dial-up access through Point-to-Point Protocol (PPP).

- 802.1X authentication

802.1X authentication is performed for users that initiate dial-up access through 802.1X.

- iPortal (built-in portal) authentication

iPortal authentication is performed by the first-generation portal server.

- Web-based (second-generation portal) authentication

Web-based 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 remote server authentication is used, first configure a RADIUS or TACACS+ server. If local authentication is selected, configure 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, and then configure authentication methods according to the access mode.

1.3.2 AAA Authorization

AAA authorization allows administrators to control services or permissions of users. After AAA authorization is enabled, the NAS configures user sessions 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 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 by the NAS and a remote server group. You can configure local or direct authorization as the backup 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, they are assigned permission levels (0 to 15).

- Config-commands authorization

Users are assigned permissions to run specific commands in configuration modes (including the global configuration mode and sub-modes).

- Console authorization

After users log in through consoles, they are authorized to run commands.

- Command authorization

After users log in to the CLI of the NAS, they are authorized to run specific commands.

- Network authorization

After users access the Internet, they are authorized to use specific session services. For example, after users access the Internet through PPP and Serial Line Internet Protocol (SLIP), they 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, first configure a RADIUS server. If local authorization needs to be implemented, configure 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, and then configure authorization methods according to the access mode.

1.3.3 AAA Accounting

In AAA, accounting is an independent process similar to authentication and authorization. During accounting, start-accounting, update-accounting, and end-accounting requests are sent to the configured accounting server. The accounting server records the network resource usage of users and performs accounting, audit, and tracking of users' activities.

The accounting scheme is optional.

AAA Accounting Schemes

- No accounting (**none**)

Accounting is not performed on users.

- Local accounting (**local**)

Accounting is completed on the NAS, and the NAS collects statistics on and limits the number of local user connections. Billing is not performed.

- Remote server-group accounting (**group**)

Accounting is performed by the NAS and a remote server group. You can configure local accounting as the backup 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

The device records commands that users run on the CLI of the NAS.

- Network accounting

The device records sessions that users set up after users pass 802.1X or web-based 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, first configure a RADIUS server. If local accounting needs to be implemented, configure 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, and then configure accounting methods according to the access mode.

1.3.4 Multi-Domain AAA

In a multi-domain environment, the NAS can provide AAA services for 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 user AVs in different domains and configure an AV set (including an AAA service method list, for example, RADIUS) for each domain.

The device supports the following username formats:

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

The userid format does not contain a domain name, and the **default** domain name is used.

The NAS provides the domain-based AAA service based on the following principles:

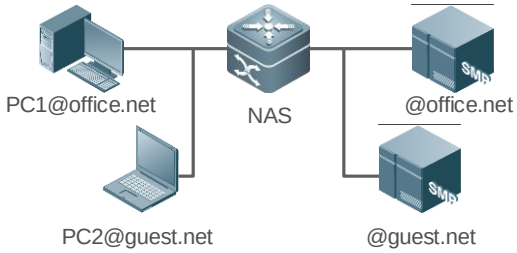
- Resolves the domain name carried by a user.
- Searches for the user domain according to the domain name.

- Searches for the corresponding AAA method list name according to the domain configuration on the NAS.
- Searches for the corresponding method list according to the method list name.
- Provides AAA services based on the method list.

If any of the preceding procedures fails, AAA services cannot be provided.

Figure 2-4 shows the typical multi-domain topology.

Figure 2-4



Related Configuration

Enabling AAA

By default, AAA is disabled.

To enable AAA, run the **aaa new-model** command.

Configuring an AAA Method List

By default, no AAA method list is configured.

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 AV set is configured for a domain.

An AV set for a domain contains the AAA method list, 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 the 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-based authentication.
	aaa authentication iportal	Defines a method list of built-in portal authentication.
	aaa authentication general	Defines a method list of general authentication.
	aaa local authentication attempts	Sets the maximum number of login attempts.
	aaa local authentication lockout-time	Sets the maximum lockout time upon a login failure.
Configuring AAA Authorization	⚠ Mandatory if different permissions and services need to be assigned to users.	
	aaa new-model	Enables AAA.
	aaa authorization exec	Defines a method list of EXEC authorization.
	aaa authorization commands	Defines a method list of command authorization.
	aaa authorization network	Configures a method list of network authorization.
	authorization exec	Applies EXEC authorization methods to a specified VTY line.
	authorization commands	Applies command authorization methods to a specified VTY line.
Configuring AAA Accounting	⚠ Mandatory if accounting, statistics, and tracking need to be performed on the network resource usage of users.	
	aaa new-model	Enables AAA.

Configuration	Description and Command	
	aaa accounting exec	Defines a method list of EXEC accounting.
	aaa accounting commands	Defines a method list of command accounting.
	aaa accounting network	Defines a method list of network accounting.
	accounting exec	Applies EXEC accounting methods to a specified VTY line.
	accounting commands	Applies command accounting methods to a specified VTY line.
	aaa accounting update	Enables accounting update.
	aaa accounting update periodic	Configures the accounting update interval.
Configuring an AAA Server Group	⚠ Recommended if a server group needs to be configured to handle AAA through different servers in the group.	
	aaa group server	Creates a user-defined AAA server group.
	server	Adds an AAA server group member.
Configuring the Domain-Based AAA Service	⚠ Mandatory if AAA management of 802.1X access STAs needs to be performed according to domains.	
	aaa new-model	Enables AAA.
	aaa domain enable	Enables the domain-based AAA service.
	aaa domain	Creates a domain and enters domain configuration mode.
	authentication dot1x	Associates the domain with an 802.1X authentication method list.
	authentication ppp	Associates the domain with a PPP authentication method list.
	authentication web-auth	Associates the domain with a web-based authentication method list.
	accounting network	Associates the domain with a network accounting method list.
	authorization network	Associates the domain with a network authorization method list.
	state	Configures the domain status.
	username-format	Configures whether to contain the domain name in usernames.
	access-limit	Configures the maximum number of domain users.

Configuration	Description and Command	
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.
	aaa user-diag log-num	Adjusts the number of tracks that can be recorded for each AAA user.
	aaa user-diag user-num	Adjusts the total number of all AAA user tracks.

1.4.1 Configuring AAA Authentication

Configuration Effect

Authenticate user identities for accessing the Internet.

Notes

- If an authentication scheme contains multiple authentication methods, these methods are executed according to the sequence in which they were configured.
- 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 obtain access even when no authentication method receives the response. Therefore, the **none** method is used only as the backup.

The **none** method is typically not used. 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 for 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 asked to enter the username again. This is because the input username 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-based Authentication

- Run the **aaa authentication web-auth** command to configure a method list of web-based authentication.
- This configuration is mandatory if you need to configure a web-based authentication method list including the configuration of the default method list.
- By default, no method list of web-based authentication is configured.

Defining a Method List of iPortal Web-based Authentication

- Run the **aaa authentication iportal** command to configure a method list of iPortal web-based authentication.
- This configuration is mandatory if you need to configure an iPortal web-based authentication method list including the configuration of the default method list.
- By default, no method list of iPortal web-based authentication is configured.

Defining a General Method List of 802.1X Authentication, Web-based Authentication, and iPortal Authentication

- Run the **aaa authentication general** command to configure a method list for 802.1X authentication, web-based authentication, and iPortal authentication.
- If the **aaa authentication dot1x**, **aaa authentication web-auth**, or **aaa authentication iportal** command is configured, it takes precedence 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 incorrect 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 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 security service, run this command. If AAA is not enabled, AAA commands cannot be configured.

Defining a Method List of Login Authentication

Command	**aaa authentication login** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default:** Indicates that the configured method list is the default one for login authentication. *list-name*: Indicates the name of a login authentication method list. It can be any character string.

	method: Indicates keyword **local**, **none**, **group**, or **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. The RADIUS and TACACS+ server groups are supported. **subs**: Indicates that the subs database is used for authentication.
Command Mode	Global configuration mode
Usage Guide	If the AAA login authentication service is enabled on the NAS, users must perform login authentication negotiation through AAA. Run the **aaa authentication login** command to configure the default or optional method list for login authentication. In a method list, the next method is executed only when the current method does not receive the 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**: Indicates that the configured method list is the default one for Enable authentication. *list-name*: Indicates the name of an Enable authentication method list. It can be any character string. *method*: Indicates keyword **enable**, **local**, **none**, or **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. The RADIUS and TACACS+ server groups are supported.
Command Mode	Global configuration mode
Usage Guide	● If the AAA login authentication service is enabled on the NAS, users must perform Enable authentication negotiation through AAA. Run the **aaa authentication enable** command to configure the default or optional method lists for Enable authentication. ● In a method list, the next method is executed only when the current method does not receive the response. ● The Enable authentication function automatically takes effect after configuring the Enable authentication method list. ● When the **local** method of Enable authentication is enabled for AAA authentication, the authentication permission level cannot exceed the permission level of the account.

Defining a Method List of 802.1X Authentication

Command	**aaa authentication dot1x** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: Indicates that the configured method list is the default one for 802.1X authentication. *list-name*: Indicates the name of an 802.1X authentication method list. It can be any character string. *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. The RADIUS server group is supported.
Command Mode	Global configuration mode
Usage Guide	If 802.1X authentication 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 the response.

Defining a Method List of PPP, Web-based, 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-based authentication. **iportal**: Configures a method list of iPortal authentication. **sslvpn**: Configures a method list of SSL VPN authentication. **default**: Indicates that the configured method list is the default one for PPP authentication. *list-name*: Indicates the name of a PPP authentication method list. It can be any character string. *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. The RADIUS server group is supported. **subs**: Specifies the SUBS authentication method using the SUBS database.
Command Mode	Global configuration mode
Usage Guide	If PPP authentication 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 the response.

Defining a General Method List of 802.1X, Web-based, and iPortal 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. It can be any character string. *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. 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, web-based authentication, and iPortal 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 login attempts.

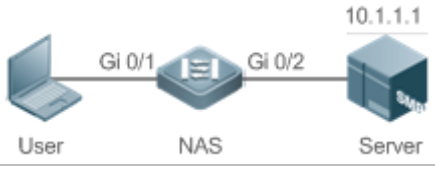
Setting the Maximum Lockout Time After a Login Failure

Command	**aaa local authentication lockout-time** *lockout-time*
Parameter Description	*lockout-time*: Indicates the time during which a user is locked after entering incorrect passwords up to the specified number of times. The value ranges from 1 to 43,200, in minutes.
Command Mode	Global configuration mode
Usage Guide	Use this command to set the maximum time during which a user is locked after entering incorrect passwords up to the specified number of times.

Configuration Example

Configuring AAA Login Authentication

On the NAS, configure a login authentication method list containing **group** *radius* and **local** methods in order.

Scenario Figure 2-5	
Configuration Steps	Step 1: Enable AAA. Step 2: First configure a RADIUS or TACACS+ server if remote group server authentication needs to be implemented. Configure 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 ruijie 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 asked 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

On the NAS, configure an Enable authentication method list containing **group** *radius*, **local**, and then **enable** methods in order.

Scenario **Figure 2-6**	
Configuration Steps	Step 1: Enable AAA. Step 2: First configure a RADIUS server if remote server-group authentication needs to be implemented. Configure 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. You can configure only the default method list that 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

On the NAS, configure an 802.1X authentication method list containing **group** *radius*, and then **local** methods in order.

Scenario **Figure 2-7**	
Configuration Steps	Step 1: Enable AAA. Step 2: First configure a RADIUS server if remote server-group authentication needs to be implemented. Configure 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

- The RADIUS or TACACS+ server is not configured.
- Usernames and passwords are not configured in the local database.

1.4.2 Configuring AAA Authorization

Configuration Effect

- Determine services or permissions that 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, authorization and authentication 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.
- Authorization methods in an authorization scheme are executed according to the sequence in which they were configured. The next authorization method is executed only when the current method does not receive the response. If authorization fails using a method, the next method will be not tried.
- Command authorization is supported only by TACACS+.
- Console authorization: The device can differentiate the users who log in through the console and 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 Console Users to Run Commands

- Run the **aaa authorization console** command to enable authorization for console users to run commands.
- By default, authorization is disabled for console users 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 security service, run this command. If AAA is not enabled, AAA commands cannot be configured.

Defining a Method List of EXEC Authorization

Command	**aaa authorization exec** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	**default**: Indicates that the configured method list is the default one for EXEC authorization. *list-name*: Indicates the name of an EXEC authorization method list. It can be any character string. *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 EXEC authorization. **none**: Indicates that EXEC authorization is not performed. **group**: Indicates that a server group is used for EXEC authorization. The RADIUS and TACACS+ 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. The NAS assigns the users CLI operation permissions (0 to 15). 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**: Indicates that the configured method list is the default one for command authorization. *list-name*: Indicates the name of a command authorization method list. It can be any character string. *method*: Indicates keyword **none** or **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 that can be executed by users. When a user enters a command, the AAA module sends the command to the authentication server. If the authentication server permits command execution, the command is executed. If the authentication server rejects command execution, the command is not executed and a message is displayed indicating that command 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**: Indicates that the configured method list is the default one for network authorization. *list-name*: Indicates the name of a network authorization method list. It can be any character string. *method*: Indicates keyword **none** or **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 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 the 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. That is, 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	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 you can run commands in configuration mode and sub-modes without authorization.

Enabling Authorization for Console Users to Run Commands

Command	**aaa authorization console**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The device can differentiate the users who log in through the console and 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, local authorization is used.

Scenario Figure 2-8	
Configuration Steps	Step 1: Enable AAA. Step 2: First configure a RADIUS server if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure 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 Command Authorization

Provide command authorization for login users according to the following default authorization method: Authorize level-15 commands first by using a TACACS+ server. If the TACACS+ server does not respond, local authorization is performed. Authorization is applied to the users who log in through the Console and the users who log in through other types of clients.

Scenario **Figure 2-9**	
Configuration Steps	Step 1: Enable AAA. Step 2: First configure a RADIUS or TACACS+ server if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure local user database information on the NAS. Step 3: Configure an AAA authorization method list according to different access modes and service types.

	Step 4: Apply the configured method list to an interface or line. Skip this step if the default authorization method is used.
NAS	Hostname#configure terminal Hostname(config)#username user1 password pass1 Hostname(config)#username user1 privilege 15 Hostname(config)#aaa new-model Hostname(config)#tacacs-server host 192.168.217.10 Hostname(config)#tacacs-server key aaa Hostname(config)#aaa authentication login default local Hostname(config)#aaa authorization commands 15 default group tacacs+ local Hostname(config)#aaa authorization console
Verification	Run the **show run** and **show aaa method-list** commands on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login default local Accounting method-list: Authorization method-list: aaa authorization commands 15 default group tacacs+ local
	Hostname#show run ! aaa new-model ! aaa authorization console aaa authorization commands 15 default group tacacs+ local aaa authentication login default local ! ! nfpp ! vlan 1 ! username user1 password 0 pass1 username user1 privilege 15 no service password-encryption ! tacacs-server host 192.168.217.10 tacacs-server key aaa ! line con 0 line vty 0 4 !

	! end

Configuring AAA Network Authorization

Scenario **Figure 2-10**	
Configuration Steps	Step 1: Enable AAA. Step 2: First configure a RADIUS or TACACS+ server if remote server-group authorization needs to be implemented. If local authorization needs to be implemented, configure 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

Accounting methods:

- If an accounting scheme contains multiple accounting methods, these methods are executed according to the sequence in which they were configured. The next accounting method is executed only when the current method does not receive the 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 a non-defined method list to a line, the system will display a message indicating that accounting on this line is ineffective. Accounting will take effect only when a defined method list is applied.

EXEC accounting:

- EXEC accounting is performed only when login authentication on the NAS is completed. EXEC accounting is not performed if login authentication is not configured or the **none** method is used for authentication. If Start-accounting is not performed for a user upon login, Stop-accounting will not be performed when the user logs out.

Command accounting:

- Only the TACACS+ protocol supports command accounting.

Configuration Steps

Enabling AAA

- Mandatory.
- Run the **aaa new-model** command to enable AAA.
- By default, AAA is disabled.

Defining a Method List of EXEC Accounting

- Run the **aaa accounting exec** command to configure a method list of EXEC accounting.
- This configuration is mandatory if you need to configure an EXEC accounting method list including the configuration of the default method list.
- The default access permission level of EXEC users is the lowest. Console users can connect to the NAS through the console port or Telnet. Each connection is counted as an EXEC user, for example, a Telnet user or an 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 be not 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 security service, run this command. If AAA is not enabled, AAA commands cannot be configured.

Defining a Method List of EXEC Accounting

Command	**aaa accounting exec** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	**default**: Indicates that the configured method list is the default one for EXEC accounting. *list-name*: Indicates the name of an EXEC accounting method list. It can be any character string. *method*: Indicates keyword **none** or **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. The RADIUS and TACACS+ server groups are 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. When a user logs in to the CLI of the NAS enabled with accounting, 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 upon user login, 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**: Indicates that the configured method list is the default one for command accounting. *list-name*: Indicates the name of a command accounting method list. It can be any character string. *method*: Indicates keyword **none** or **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. The TACACS+ server group is supported.
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. The NAS enabled with accounting 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**: Indicates that the configured method list is the default one for network accounting. *list-name*: Indicates the name of a network accounting method list. It can be any character string. **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 enabled. *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 a server group is used for network accounting. The RADIUS and TACACS+ server groups is supported.
Command Mode	Global configuration mode
Usage Guide	The device sends recorded 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 are unavailable if AAA is not enabled. After AAA is 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 are unavailable if AAA is not enabled. After AAA is 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 2-11**	

Configuration Steps	Step 1: Enable AAA. Step 2: If remote server-group accounting needs to be implemented, first configure the RADIUS or TACACS+ server. Step 3: Configure an AAA accounting 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 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 Command Accounting

Configure command authentication for login users and apply the default accounting method. Login authentication is performed in local mode, and the TACACS+ server is used for accounting.

Scenario **Figure 2-12**	
Configuration Steps	Step 1: Enable AAA. If remote server-group accounting needs to be implemented, configure a RADIUS or TACACS+ server in advance. Step 2: Configure an AAA accounting method list according to different access modes and service types. Step 3: Apply the configured method list to an interface or line. Skip this step if the default accounting method is used.
NAS	Hostname#configure terminal Hostname(config)#username user1 password pass1 Hostname(config)#username user1 privilege 15 Hostname(config)#aaa new-model Hostname(config)#tacacs-server host 192.168.217.10 Hostname(config)#tacacs-server key aaa Hostname(config)#aaa authentication login default local Hostname(config)#aaa accounting commands 15 default start-stop group tacacs+
Verification	Run the **show aaa method-list** command on the NAS to display the configuration.
NAS	Hostname#show aaa method-list Authentication method-list: aaa authentication login default local Accounting method-list: aaa accounting commands 15 default start-stop group tacacs+ Authorization method-list:
	Hostname#show run ! aaa new-model !

	aaa authorization config-commands aaa accounting commands 15 default start-stop group tacacs+ aaa authentication login default local ! ! nfpp ! vlan 1 ! username user1 password 0 pass1 username user1 privilege 15 no service password-encryption ! tacacs-server host 192.168.217.10 tacacs-server key aaa ! line con 0 line vty 0 4 ! ! end

Configuring AAA Network Accounting

Configure a network accounting method list for 802.1X users, and configure a remote RADIUS server for authentication and accounting.

Scenario **Figure 2-13**	
Configuration Steps	Step 1: Enable AAA. Step 2: If remote server-group accounting needs to be implemented, first configure a RADIUS server. 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 proper name to the user-defined server group. Do not use the pre-defined **radius** and **tacacs+** keywords in naming.

↘ Adding an AAA Server Group Member

- Mandatory.
- Run the **server** command to add AAA server group members.
- By default, a user-defined server group does not have servers.

Verification

Run the **show aaa group** command to verify the configuration.

Related Commands

Creating a User-Defined AAA Server Group

Command	**aaa group server** { **radius** | **tacacs+** } *name*
Parameter Description	*name*: Indicates the name of the server group to be created. The name cannot contain the **radius** or **tacacs+** keyword because they are the names of the default RADIUS and TACACS+ server groups.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure an AAA server group. The RADIUS and TACACS+ server groups are supported.

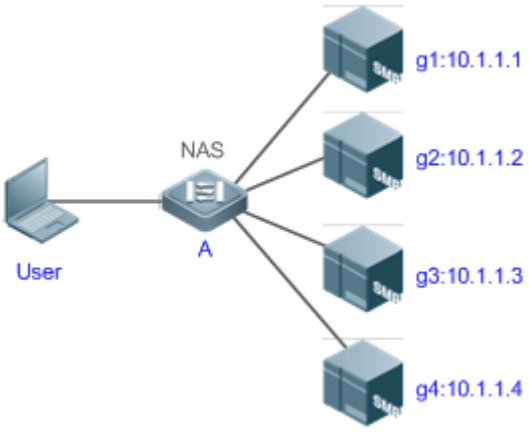
Adding an AAA Server Group Member

Command	**server** *ip-addr* [**auth-port** *port1*] [**acct-port** *port2*]
Parameter Description	*ip-addr*: Indicates the IP address of a server. *port1*: Indicates the authentication port of a server, which is supported only by the RADIUS server group. *port2*: Indicates the accounting port of a server, which 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 2-14**	
Prerequisites	1. The required interfaces, IP addresses, and VLANs have been configured on the network, network connections have been set up, and the routes from the NAS to servers are reachable.

	2. AAA has been enabled.
Configuration Steps	Step 1: Configure a server that belongs to the default server group. Step 2: Create user-defined AAA server groups. Step 3: Add servers to the AAA server groups.

NAS	`Hostname#configure terminal`
	`Hostname(config)#radius-server host 10.1.1.1`
	`Hostname(config)#radius-server host 10.1.1.2`
	`Hostname(config)#radius-server host 10.1.1.3`
	`Hostname(config)#radius-server host 10.1.1.4`
	`Hostname(config)#radius-server key secret`
	`Hostname(config)#aaa group server radius g1`
	`Hostname(config-gs-radius)#server 10.1.1.1`
	`Hostname(config-gs-radius)#server 10.1.1.2`
	`Hostname(config-gs-radius)#exit`
	`Hostname(config)#aaa group server radius g2`
	`Hostname(config-gs-radius)#server 10.1.1.3`
	`Hostname(config-gs-radius)#server 10.1.1.4`
	`Hostname(config-gs-radius)#exit`

Verification	Run the **show aaa group** and **show run** commands on the NAS to display the configuration.

NAS	`Hostname#show aaa group`
	`Type Reference Name`
	`---------- ---------- ----------`
	`radius 1 radius`
	`tacacs+ 1 tacacs+`
	`radius 1 g1`
	`radius 1 g2`

	`Hostname#show run`
	`!`
	`radius-server host 10.1.1.1`
	`radius-server host 10.1.1.2`
	`radius-server host 10.1.1.3`
	`radius-server host 10.1.1.4`
	`radius-server key secret`
	`!`
	`aaa group server radius g1`
	` server 10.1.1.1`
	` server 10.1.1.2`
	`!`
	`aaa group server radius g2`
	` server 10.1.1.3`
	` server 10.1.1.4`
	`!`

	!

Common Errors

- For RADIUS servers that use non-default authentication and accounting ports, when you run the **server** command to add servers, specify the authentication or accounting port.

1.4.5 Configuring the Domain-Based AAA Service

Configuration Effect

Create AAA schemes for 802.1X users in different domains.

Notes

Referencing method lists in domains:

- The AAA method lists that you select in domain configuration mode should be pre-defined. When you select the method lists are not pre-defined in domain configuration mode, the system prompts that the configuration does 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 for users in the domain.

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 for 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 for 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 for 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.

Domain names:

- The domain names carried by usernames and those configured on the NAS are matched based on the longest matching principle. For example, if two domains of **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** but not **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 for 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.
- The domain-based AAA service is applicable only to 802.1X access.

Associating the Domain with PPP and Web-based 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-based authentication method list.
- This configuration is mandatory if you need to apply a specified PPP or web-based 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, the global default method list is used for accounting by default.

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, the global default method list is used for authorization by default.

Configuring the Domain Status

- Optional.
- When a domain is in **block** state, users in the domain cannot log in.
- By default, after a domain is created, its state is **active**, indicating that all the users in the domain are allowed to request network services.

Configuring Whether to Contain the Domain Name in Usernames

- Optional.
- By default, the usernames exchanged between the NAS and an authentication server carry domain information.

Configuring the Maximum Number of Domain Users

- Optional.
- By default, the maximum number of access users allowed in a domain is not limited.

Verification

Run the **show aaa domain** command to verify the configuration.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	To enable the AAA security service, run this command. If AAA is not enabled, AAA commands cannot be configured.

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 use either of the following methods to restore accounting: ● Run the **clear dot1x user all** command to trigger authentication for 802.1X authentication users automatically. ● Run the **clear web-auth user all** command to disconnect web-based authentication users. The users need to initiate authentication requests manually.

Creating a Domain and Entering the 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 for 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 for the user. The system supports a maximum of 32 domains.

Associating the Domain with an 802.1X Authentication Method List

Command	**authentication dot1x** { **default** | *list-name* }
Parameter Description	**default**: Indicates that the default method list is used. *list-name*: Indicates the name of the method list to be associated.
Command Mode	Domain configuration mode
Usage Guide	Use this command to associate the domain with a 802.1X authentication method list.

Associating the Domain with a PPP Authentication Method List

Command	**authentication ppp** { **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 PPP authentication method list.

Associating the Domain with a Web-based 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 unavailable. **active**: Indicates that the configured domain is available.
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 that domain information is removed from usernames. **with-domain**: Indicates that domain information is retained 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 an authentication server in a specified domain.

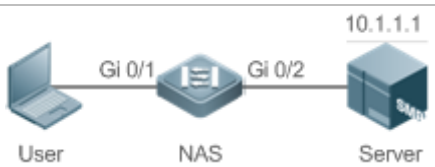
Configuring the Maximum Number of Domain Users

Command	**access-limit** *num*
Parameter Description	*num*: Indicates the maximum number of access users allowed in a domain, which applies only to 802.1X users.
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 for 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 2-15	

Configuration Steps	The following example shows how to configure RADIUS authentication and accounting. The RADIUS server must have been configured. 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**: Disconnects 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 the configuration about only the policy for accounting-start failures.

Configure a policy for accounting-start failures.

Scenario Figure 1-16	
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, including RADIUS and 802.1X modules.

Configuration Steps

Detecting AAA Heartbeats

- Optional.
- By default, heartbeat packet detection is enabled.

Verification

Run the **show run** command to verify the configuration.

Related Commands

Allowing Users to Get Online After Accounting Fails to Start

Command	[**no**] **aaa heartbeat enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Detecting AAA Heartbeats

Scenario Figure 1-17	
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 generated 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 many users go online, AAA logging may cause screen information to be refreshed or device performance to deteriorate. 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. By default, the device generates five logs per second. The value ranges from 0 to 65535. The value 0 indicates that the log generation rate is not limited.
Command Mode	Global configuration mode
Usage Guide	If many users go online, AAA logging may cause screen information to be refreshed or device performance to deteriorate. You can configure this command to configure a logging rate limit.

Adjusting the Number of Tracks That Can Be Recorded for Each AAA User

Command	**aaa user-diag log-num** *num*
Parameter Description	*num*: Indicates the number of tracks that can be recorded for each AAA user. The value range is from 1 to 100.
Command Mode	Global configuration mode
Usage Guide	When a large number of users go online or offline, the memory usage of the process for recording user tracks may increase quickly. This command is used to adjust the number of track records for each AAA user to reduce the memory usage of the process.

Adjusting the Total Number of AAA User Track Records

Command	**aaa user-diag user-num** *num*
Parameter Description	*num*: Indicates the total number of AAA user track records. The value range is from 1 to 10000.
Command Mode	Global configuration mode

Usage Guide	When a large number of users go online, the memory usage of the process for recording user tracks may increase quickly. This command is used to adjust the total number of AAA user track records to reduce the memory usage of the process.

Configuration Example

The following example involves only configuration about AAA logging.

Configure AAA logging.

Scenario **Figure 1-18**	
Configuration Steps	Configure the device to generate 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

Command	Description
clear aaa local user lockout { **all** | **user-name** *username* }	Clears locked users.
clear aaa user diag	Clears all AAA user tracks.

Displaying

Command	Description
show aaa accounting update	Displays accounting update information.
show aaa domain	Displays the current domain configuration.
show aaa lockout	Displays the current lockout configuration.
show aaa group	Displays AAA server groups.
show aaa method-list	Displays AAA method lists.

show aaa user	Displays AAA users.
show aaa user diag { **all** | **by-id** *session-id* | **by-mac** *mac-address* | **by-ip** *ip-address* }	Displays information about AAA user tracks.

1 Configuring RADIUS

1.1 Overview

The Remote Authentication Dial-In User Service (RADIUS) is a distributed client/server system.

RADIUS is used with Authentication, Authorization, and Accounting (AAA) to conduct identity authentication on users who attempt to access a network and prevent unauthorized access. A RADIUS client runs on a device or Network Access Server (NAS) and transmits identity authentication requests to the 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 typically applied to network environments that demand high security and allow access of remote users. RADIUS is an open protocol, and the RADIUS server is installed on many operating systems as a component, for example, UNIX, Windows 2000, and Windows 2008. Therefore, RADIUS is the most widely applied security server.

The Dynamic Authorization Extensions to Remote Authentication Dial In User Service is defined in RFC 3576, which 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 proactively initiates a user offline request to a device. The device locates a user according to the user session, 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

- RFC 2865: Remote Authentication Dial In User Service (RADIUS)
- RFC 2866: RADIUS Accounting
- RFC 2867: RADIUS Accounting Modifications for Tunnel Protocol Support
- RFC 2868: RADIUS Attributes for Tunnel Protocol Support
- RFC 2869: RADIUS Extensions
- RFC 3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

1.2 Applications

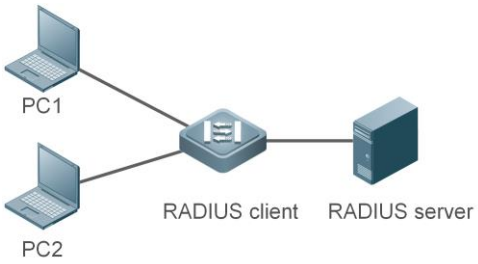
Application	Description
Providing Authentication, Authorization, and Accounting Services for Access Users	Authentication, authorization, and accounting are conducted on access users on a network, to prevent unauthorized access or operations.
Forcing Users to Go Offline	The server forces an authenticated user to go offline.

1.2.1 Providing Authentication, Authorization, and Accounting Services for Access Users

Scenario

RADIUS is typically applied for 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



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 device. 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 a vendor.

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 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 management.

0 shows the networking topology.

Deployment

- Perform the following operation according to 3.2.1 "Deployment".
- Enable the RADIUS dynamic authorization extension function on the RADIUS client.

1.3 Features

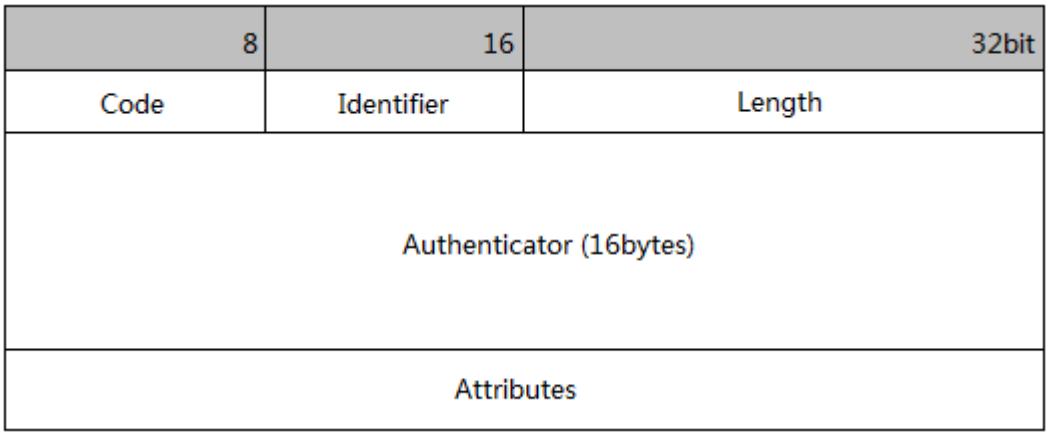
Basic Concepts

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 accepting or 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.

Format of RADIUS Packets

- The following figure shows the format of RADIUS packets.



- Code: Identifies the type of RADIUS packets, which occupies 1 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 1 byte. The identifier values of request packets and response packets of the same type are the same.
- Length: Identifies the length of a RADIUS packet, which includes **Code**, **Identifier**, **Length**, **Authenticator**, and **Attributes**. It occupies 2 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 encrypting or decrypting user passwords.
- Attributes: Carries authentication, authorization, and accounting information, with the variable length. The **Attributes** field usually contains multiple attributes. Each attribute is represented in the Type, Length, Value (TLV) format. **Type**

occupies 1 byte and indicates the attribute type. The following table lists common attributes of RADIUS authentication, authorization, and accounting. **Length** occupies 1 byte and indicates the attribute length, which is expressed in 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

Attribute No.	Attribute Name	Attribute No.	Attribute Name
29	Termination-Action	74	ARAP-Security-Data
30	Called-Station-Id	75	Password-Retry
31	Calling-Station-Id	76	Prompt
32	NAS-Identifier	77	Connect-Info
33	Proxy-State	78	Configuration-Token
34	Login-LAT-Service	79	EAP-Message
35	Login-LAT-Node	80	Message-Authenticator
36	Login-LAT-Group	81	Tunnel-Private-Group-id
37	Framed-AppleTalk-Link	82	Tunnel-Assignment-id
38	Framed-AppleTalk-Network	83	Tunnel-Preference
39	Framed-AppleTalk-Zone	84	ARAP-Challenge-Response
40	Acct-Status-Type	85	Acct-Interim-Interval
41	Acct-Delay-Time	86	Acct-Tunnel-Packets-Lost
42	Acct-Input-Octets	87	NAS-Port-Id

Shared Key

A RADIUS client and a RADIUS server 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 to ensure 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 Configuring AAA. In a RADIUS server group to which multiple RADIUS servers are added, 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. 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 802.1X authentication is used, the Calling-Station-ID attribute is set to the MAC address of the device where the 802.1X client is installed. The following table describes the format of MAC addresses.

Format	Description
ietf	Indicates the standard format specified in RFC 3580, which is separated by the separator (-). Example: 00-D0-F8-33-22-AC
normal	Indicates the common format that represents a MAC address in dotted hexadecimal notation, 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. As defined by RFC 2865, 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

ID	Function	TYPE	Extended TYPE
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 IP Address of RADIUS Packets	Specifies the source IP address used by a RADIUS client to transmit packets to a RADIUS server.
RADIUS Retransmission Upon Timeout	Specifies packet retransmission parameters 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 proactively detect whether a RADIUS server is reachable and maintain accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve handling performance of RADIUS services.
Forcible Disconnection	Enables a RADIUS server to proactively force authenticated users to go offline.

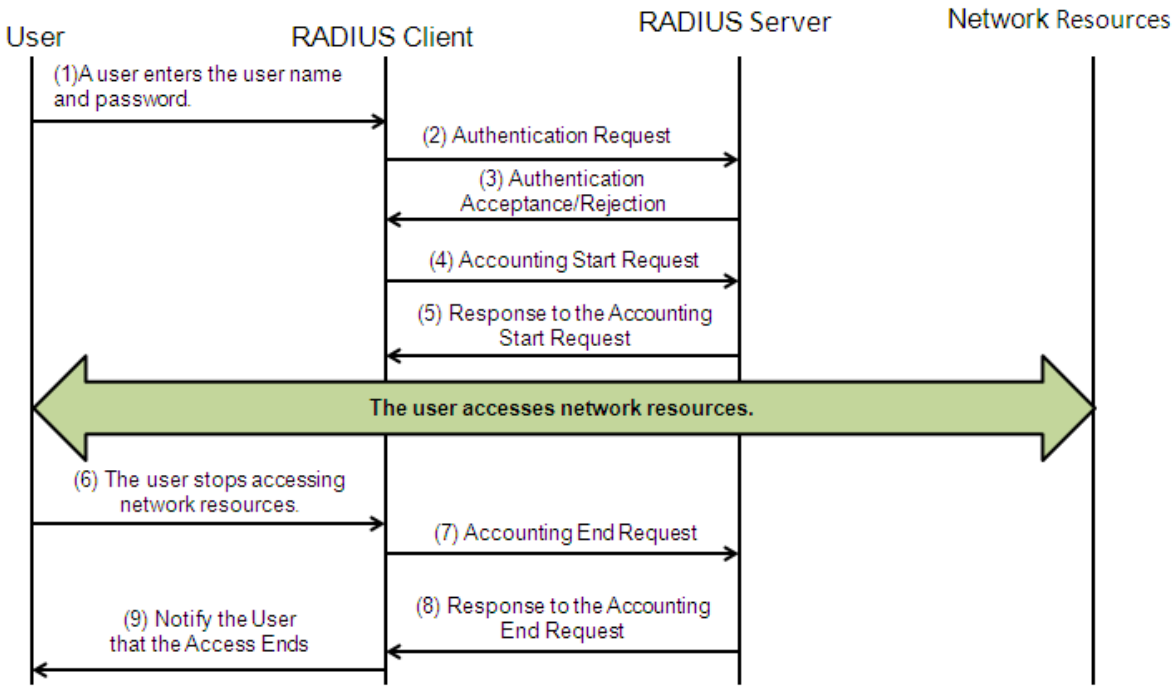
Configuring the DSCP Value of RADIUS Packets	The DSCP field is contained in the Type of Service (ToS) field of IP packets. The DSCP value marks the packet priority for transmission. The default DSCP value of RADIUS packets is 0. You can specify the DSCP value for RADIUS packets using commands. A larger DSCP value represents a higher priority of RADIUS packets.
Configuring the Units 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.
Configuring Load Balancing for the RADIUS Server Group	Enables load balancing of the RADIUS server group to reduce the resource consumption of a single server.
Configuring Hot Standby for the RADIUS Server	Enables the hot standby function to back up the server status and ensures that the active and standby servers in the same context maintain the same server status.
Configuring the Function of Copying Accounting Packets	Enables the RADIUS server to copy accounting packets and send them to servers (only the first three servers configured in a server group) in a specified server group.
RadSec Server	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 RADIUS Authentication and Authorization Process



The RADIUS authentication and authorization process is described as follows:

- A user enters the user name and password and transmits them to the RADIUS client.
- 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.
- 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 delivers authorization information apart from the authentication acceptance information. The authorization information varies with the type of access users.

The RADIUS accounting process is described as follows:

1. 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.
2. The RADIUS server returns the accounting start response packet, indicating accounting start.
3. The user stops accessing network resources and requests the RADIUS client to terminate the network connection.
4. The RADIUS client transmits the accounting end request packet to the RADIUS server.
5. The RADIUS server returns the accounting end response packet, indicating accounting end.
6. 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.

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.

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.

RADIUS accounting can be conducted only after the AAA accounting method list of relevant user types is configured.

1.3.2 Source IP 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, reducing the workload of maintaining a large amount of NAS information on the RADIUS server.

Related Configuration

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 Retransmission Upon Timeout

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 given period of time, the RADIUS client retransmits the packet.

Related Configuration

Configuring the Timeout Interval of the RADIUS Server

The default timeout interval is 5s.

You can run the radius-server timeout command to configure the timeout interval. The value ranges from 1 to 1,000, in seconds.

The response time of a RADIUS server is relevant to its performance and the network environment. Set an appropriate timeout interval as required.

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 0 to 100.

Configuring the Device 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 the device to retransmit accounting update packets for authenticated users.

1.3.4 RADIUS Server Accessibility Detection

Working Principle

A RADIUS client proactively detects whether a RADIUS server is reachable and maintains accessibility of each RADIUS server. A reachable RADIUS server is selected preferentially to improve handling performance of RADIUS services.

Related Configuration

Configuring the Criteria for the Device to Determine That a RADIUS Server Is Unreachable

A RADIUS server is unreachable when the two conditions are met:

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 10 consecutive times.

You can run the **radius-server dead-criteria** command to configure the criteria for the device to determine that the RADIUS security server is unreachable.

Configuring the Test User Name for Proactively Detecting the RADIUS Security Server

No test user name is specified for proactively detecting the RADIUS security server by default.

You can run the **radius-server host** *x.x.x.x* **testusername** *xxx* command to configure the test user name.

1.3.5 Forcible Disconnection

Working Principle

Figure 1-1 DM Message Exchange of the RADIUS Dynamic Authorization Extension Protocol

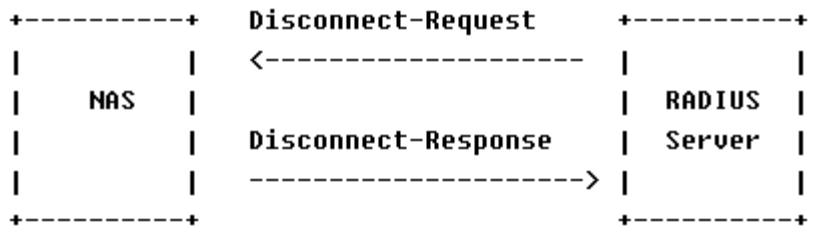


Figure 1-3 shows the exchange of DM messages between the RADIUS server and the device. The RADIUS server transmits the Disconnect-Request message to UDP port 3799 of the device. Then the device returns the Disconnect-Response message that carries the processing result to the RADIUS server.

Related Configuration

N/A

1.3.6 Configuring the 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 determines the packet priority 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 Units of Data Flows and Data Packets Sent to the RADIUS Server

Working Principle

By default, the units of data flows and data packets sent to the RADIUS server are bytes and packets, respectively. You can specify the units of data flows and data packets sent to the RADIUS server using commands.

Related Configuration

↘ Configuring the Units 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-packe**t | **giga-packet** } command to configure the unit of data flows and data packets sent to the RADIUS server.

1.3.8 Configuring Load Balancing for the RADIUS Server Group

Working Principle

The client is authenticated through the first server in the server group. The next server will be selected only when the first server is unreachable. After load balancing is enabled, polling is adopted. In this case, the authentication packet from the first client is sent to the first server, that from the second to the second server, and so on. After the last server receives the authentication packet from the client, the cycle restarts from the first server.

Related Configuration

Configuring Load Balancing for the RADIUS Server Group

Run the load-balance command to enable load balancing for the RADIUS server group.

1.3.9 Configuring Hot Standby for the RADIUS Server

Working Principle

When configuring the RADIUS server, you can enable the hot standby function to back up the server status and ensure that the active and standby servers in the same context maintain the same status.

Related Configuration

Configuring Hot Standby for the RADIUS Server

Run the **radius-server host** *ipv4-address* **context** *id hb_ipv4* **key** *text-string* command to enable hot standby for the RADIUS server.

1.3.10 Configuring the Function of Copying Accounting Packets

Working Principles

RADIUS accounting packets are sent to one server specified in the accounting method list by default. After this function is enabled, the server copies accounting packets and sends the packets to servers (only the first three servers configured in a server group) in a specified server group.

Related Configuration

Configuring the Function of Copying Accounting Packets

Run the **accounting-copy** *group_name* command in the accounting server group to copy accounting packets to servers in a specified server group.

1.3.11 RadSec Server

Working Principle

TLS RADIUS, also called RadSec, leverages the TLS protocol to ensure secure communication of RADIUS requests. RadSec redirects the normal RADIUS traffic to the remote server over TLS to ensure transmission security of RADIUS identity verification, authorization, and accounting data over insecure networks.

Combining TLS and TCP, RadSec provides higher security than the earlier RADIUS that uses UDP. UDP-based RADIUS uses the MD5 algorithm to encrypt the shared key, which is prone to attacks. RadSec exchanges valid loads in RADIUS data packets over TLS-encrypted tunnels to effectively reduce the risks of being attacked.

Related Configuration

Configuring the RadSec Service

The RadSec server is implemented by the RadSec target. To enable the RadSec service, you need to configure a RadSec server as a specific target and divert the RADIUS traffic to the target. Each RadSec target has a unique ID for easy

identification. In addition, the system supports multiple RadSec targets, which can be distinguished by different parameters, even if they point to the same RadSec server.

If you want to divert traffic from the traditional RADIUS server to the RadSec server, you only need to associate the RADIUS server with the specified RadSec target. For example, the IP address of the RADIUS server is 10.1.1.1. If you want to associate this server with RadSec target 10, run the following command: radius-server host 10.1.1.1 radsec-destination 10.

1.4 Configuration

Configuration	Description and Command	
Performing RADIUS Basic Configuration	(Mandatory) It is used to configure RADIUS authentication, authorization, and accounting.	
	radius-serverhost	Configures the IP address of the remote RADIUS security server.
	radius-serverkey	Configures the shared key for communication between the device and the RADIUS server.
	radius-serverretransmit	Configures the request transmission count, after which the device confirms that a RADIUS server is unreachable.
	radius-servertimeout	Configures the waiting time, after which the device retransmits a request.
	radius-server account update retransmit	Configures the device to retransmit 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-server attribute 30	Configures the format of RADIUS attribute No. 30 (Called-Station-ID).

Configuration	Description and Command	
	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 *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 vendor-specific attribute support	Configures whether the RADIUS server parses vendors' private attributes contained in packets.
	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 accessibility of the RADIUS server.	
	radius-server dead-criteria	Configures the global criteria for determining 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 proactive detection parameters.
Configuring the DSCP Value of RADIUS Packets	**radius dscp**	Configures the DSCP value of RADIUS packets.

Configuration	Description and Command	
Configuring the Units 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 Load Balancing for the RADIUS Server Group	**load-balance**	Enables load balancing for the RADIUS server group.
Configuring the Function of Copying Accounting Packets	⚠ (Optional) It is used to configure the function of copying accounting packets.	
	accounting-copy	Configures the function of copying accounting packets.
Configuring RadSec Target Attributes	⚠ (Optional) It is used to configure the port number, IP address, and keepalive parameters for the RadSec target server. This command is required after you configure RadSec traffic redirection.	
	radsec destination	Configures the port number, IP address, timeout period, and keepalive interval for the RadSec target server.

1.4.1 Performing 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 can use the source IP address to communicate 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 network environment.

In an 802.1X authentication environment where the RADIUS security protocol is used, 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 3s (the default value is 5s) and **radius-server retransmit** be set to 2 (the default value is 3) on the network device.

Configuring the Device to Retransmit Accounting Update Packets for Authenticated Users

- Optional.
- Determine whether to enable the device to retransmit accounting update packets of authenticated users as needed.

Configuring the Source Address of RADIUS Packets

- Optional.
- Configure the source address of RADIUS packets according to the network environment.

Verification

- Configure the AAA method list that specifies RADIUS for authentication, authorization, and accounting on users.
- Enable the device to interact with the RADIUS server. Obtain packets to confirm that the device communicates with the RADIUS server through RADIUS.

Related Commands

Configuring the Remote RADIUS Security Server

Command	**radius-server host** { *ipv4-address* | *ipv6-address* } [[**acct-port** *port-number* | **auth-port** *port-number*] * [**test username** *name* [**ignore-auth-port**] [**ignore-acct-port**] [**idle-time** *time*]] | **context** *id hb-ipv4* | **radsec-destination** *id-number*] * [**key** [**0** | **7**] *text-string*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the RADIUS security server. *Ipv6-address*: Indicates the IPv6 address of the RADIUS security server. **auth-port** *port-number*: Indicates the UDP port for RADIUS identity authentication. The value ranges from 0 to 65,535. If it is set to 0, the host does not conduct identity authentication. **acct-port** *port-number*: Indicates the UDP port for RADIUS accounting. The value ranges from 0 to 65,535. If it is set to 0, the host does not conduct accounting.

	context *id hb_ipv4*: Enables the hot standby function for the RADIUS server and specifies the hot standby context ID and peer IP address. The server status can be backed up so that the active and standby servers in the same context maintain the same status. **test username** *name*: Enables the device to proactively detect 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 device from detecting the authentication port of the RADIUS security server. It is enabled by default. **ignore-acct-port**: Disables the device from detecting the accounting port of the RADIUS security server. It is enabled by default. **Key** [**0** | **7**] *text-string* : Configures the shared key of the server. The global shared key is used if it is not configured. The configured key is displayed as "*" and you are required to enter the same key twice. If the entered keys are inconsistent, you need to re-enter the key. If inconsistency occurs for five consecutive times, the configuration will fail. **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	**0** | **7**: Indicates the encryption type of the key. The value 0 indicates no encryption and 7indicates simple encryption. The default value is 0. *text-string*: Indicates the text of the shared key.
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 determine that a security

	server does not respond as follows: The security server does not respond within the RADIUS packet retransmission duration of the specified retransmission count, and there is the timeout interval between two consecutive retransmissions.

Configuring the Waiting Time, After which the Device Retransmits a Request

Command	**radius-server timeout** *seconds*
Parameter Description	*seconds*: Indicates the timeout interval, in seconds. The value ranges from 1 to 1,000.
Command Mode	Global configuration mode
Usage Guide	Use this command to adjust the timeout interval for packet retransmission.

Configuring Retransmission of Accounting Update Packets for Authenticated Users

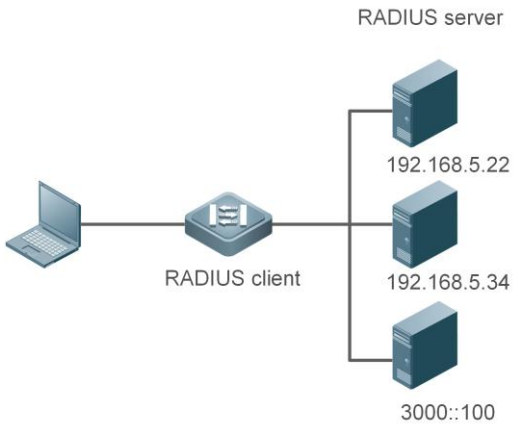
Command	**radius-server account update retransmit**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the device to retransmit accounting update packets for authenticated users. Accounting update packets are retransmitted by default. The configuration does not affect users of other types.

Configuring the Device to Send Accounting-On Packets After the NAS Device Restarts

Command	**radius-server accounting-on enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the device to send 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 3-2**	
Configuration Steps	1. Enable AAA. 2. Configure RADIUS server information. 3. Configure RADIUS authentication, authorization, and accounting methods. 4. Apply the configured authentication method on the interface.

RADIUS Client	`Hostname#configure terminal`
	`Hostname(config)#aaa new-model`
	`Hostname(config)# radius-server host 192.168.5.22`
	`Hostname(config)#radius-server host 3000::100`
	`Hostname(config)# radius-server key aaa`
	`Hostname(config)#aaa authentication login test group radius`
	`Hostname(config)#aaa authorizationexectest group radius`
	`Hostname(config)#aaa accountingexectest start-stop group radius`
	`Hostname(config)# line vty 0 4`
	`Hostname(config-line)#login authentication test`
	`Hostname(config-line)# authorization exec test`
	`Hostname(config-line)# accounting exec test`

Verification	Log in to a device from a PC in Telnet mode. The user is asked to enter the user name and password. Enter the correct user name and password to log in to the device. After obtaining an access level granted by the server, only commands under this access level can be executed. Check the authentication log of the user on the RADIUS server; perform management operations on the device and then log out; check 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 here 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.

Configuring the Format of RADIUS Attribute No. 30 (Called-Station-ID)

- Optional.
- Configure the address format of Called-Station-ID to a type supported by the server.

Configuring the RADIUS Private Attribute Type

- Optional.
- If the server is a Ruijie application server, the RADIUS private attribute type needs to be configured.

Setting the Private Attribute port-priority Issued by the Server to the CoS Value of an Interface

- Optional.
- Set the private attribute port-priority issued by the server to the CoS value of an interface as required.

Configuring the Device to Support the CUI Attribute

- Optional.
- Configure whether the device supports the RADIUS CUI attribute as required.

Configuring a Mode for the Device to Parse Private Attributes

- Optional.
- Configure the index of a Ruijie private attribute parsed by the device as required.

Configuring the Device to Encapsulate a Specified Attribute in RADIUS Authentication Request Packets

- Optional.
- Configure RADIUS authentication request packets to contain a specified attribute.

Configuring the Device to Encapsulate a Specified Attribute in RADIUS Accounting Request Packets

- Optional.
- Configure RADIUS accounting request packets to contain a specified attribute.

Configuring the Device to Encapsulate a VSA in RADIUS Authentication Request Packets

- Optional.
- Configure RADIUS authentication request packets to contain a VSA.

Configuring the Device to Encapsulate a VSA in RADIUS Accounting Request Packets

- Optional.
- Configure RADIUS accounting request packets to contain a VSA.

Configuring Whether the 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 for QinQ and non-QinQ scenarios. The default is the common encapsulation format.

Verification

- Configure the AAA method list that specifies RADIUS for authentication, authorization, and accounting on users.
- Enable the device to interact with the RADIUS server. Obtain packets to check the MAC address format of Calling-Station-Id.

- Enable the device to interact with the RADIUS server. Check debugging information of the device to determine that Ruijie private attributes are correctly parsed by the device.
- Enable the device to interact with the RADIUS server. Check debugging information of the device to determine 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 RFC 3580, which is separated by the separator (-), for example, 00-D0-F8-33-22-AC. **normal**: Indicates the common format that represents a MAC address (dotted hexadecimal notation), which is separated by the separator (.), for example, 00d0.f833.22ac. **unformatted**: Indicates the format without separators, for example, 00d0f83322ac. This format is used by default. **dot-split**: Indicates the format of MAC address, which is separated by the period (.).This parameter should be used with **mode1** or **mode2**. **colon-split**: Indicates the format of MAC address, which is separated by the semicolon (:). This parameter should be used with **mode1** or **mode2**. **hyphen-split**: Indicates the format of MAC address, which is separated by the hyphen (-). This parameter should be used 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 used 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 a Mode for the Device to Parse 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 from the class attribute. **format-16bytes**: Sets the format of the rate limit to 16 bytes in the **class** attribute. **format-32bytes**: Sets the format of the rate limit 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.

Configuring the Format of RADIUS Attribute No. 30 (Called-Station-ID)

Command	**radius-server attribute 30** { **ap-mac** | **ap-name** }
Parameter Description	**ap-mac**: Specifies the attribute format of Called-Station-ID as ap-mac:SSID, which is the default format. **ap-mac**: Specifies the attribute format of Called-Station-ID as ap-name:SSID.
Command Mode	Global configuration mode
Usage Guide	Configure the desired format based on the server. The default format is ap-mac:SSID.

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 a Mode for the Device to Parse 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 the Device to Encapsulate a Specified Attribute in RADIUS Authentication Request Packets

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 the device to encapsulate a specified attribute in RADIUS

	authentication request packets.

Configuring the Device to Encapsulate a Specified Attribute in RADIUS Accounting Request Packets

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 the device to encapsulate a specified attribute in RADIUS accounting request packets.

Configuring the Device to Encapsulate a VSA in RADIUS Authentication Request Packets

Command	**radius-server authentication vendor** *vendor_name* **package**
Parameter Description	*vendor_name*: Indicates a vendor name, which can be **cmcc**, **microsoft**, **cisco**, or **hw**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the device to encapsulate a VSA in RADIUS authentication request packets.

Configuring the Device to Encapsulate a VSA in RADIUS Accounting Request Packets

Command	**radius-server account vendor** ***vendor***_*name* **package**
Parameter Description	*vendor_name*: Indicates a vendor name, which can be **cmcc**, **microsoft**, **cisco**, or **hw**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the device to encapsulate a VSA in RADIUS accounting request packets.

Configuring Whether the 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, which can be **cisco**, **huawei**, or **ms**.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure whether the 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 that the device encapsulates the NAS-Port-ID attribute based on a predefined combination of the interface name, inner VLAN ID (VID) and outer VID. **port-vid**: Indicates that the device encapsulates the NAS-Port-ID attribute based on a predefined

	combination of the interface name and VID. **normal**: Indicates that the device encapsulates the NAS-Port-ID attribute based on the interface name. **mode1**: Indicates that the device encapsulates 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 unavailable.
Command Mode	Global configuration mode
Usage Guide	Configure the NAS-Port-ID encapsulation format of RADIUS packets for QinQ and non-QinQ scenarios.

Configuration Example

↘ Configuring the RADIUS Attribute Type

Scenario	One authentication device
Configuration Steps	1. Configure the MAC address format of RADIUS Calling-Station-Id. 2. Set the QoS value issued by the RADIUS server to the CoS value of the interface. 3. Configure the RADIUS function to support the CUI attribute. 4. Configure the device to support private attributes of other vendors. 5. Configure the device not to encapsulate the NAS-Port-ID attribute in RADIUS authentication request packets. 6. Configure the device to encapsulate CMCC VSA in RADIUS accounting request packets. 7. Configure the RADISU server not to parse Cisco VSA. 8. 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)#radiussupport cui`
	`Hostname(config)#radiusvendor-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	Obtain packets to check debugging information of the device. Check whether the RADIUS standard attributes and private attributes are encapsulated or 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, or accounting requests of access users to an unreachable RADIUS server unless all the other servers in the same RADIUS server group are all unreachable.

The device proactively detects a specified RADIUS server. The proactive detection function is disabled by default. If the proactive detection function is enabled for a specified RADIUS server, the device will periodically transmits detection authentication or accounting requests to the RADIUS server. The transmission interval is as follows:

- For a reachable RADIUS server, the interval is the proactive detection interval of the reachable RADIUS server (the default value is 60 minutes).
- For an unreachable RADIUS server, the interval has a fixed value of 1 minute.

Notes

- All the following conditions need to be met before the proactive 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 or accounting port) of the RADIUS server is configured on the device.
- If the following two conditions are met, the device considers 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, the device considers that an unreachable RADIUS server becomes reachable:
- The device receives correct responses from the RADIUS server.
- The duration that the RADIUS server is in unreachable state exceeds the time set in **radius-server deadtime** and the proactive detection function is disabled for the RADIUS server.
- The authentication or accounting port of the RADIUS server is updated on the device.

Configuration Steps

Configuring the Global Criteria for Determining That a RADIUS Security Server Is Unreachable

- Mandatory.
- Before enabling the proactive detection function, you must configure the global criteria for determining that a RADIUS security server is unreachable.

Configuring the IP Address of the Remote RADIUS Security Server, Authentication Port, Accounting Port, and Proactive Detection Parameters

- Mandatory.
- Configuring proactive detection parameters of the RADIUS server is the prerequisite for enabling the proactive 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 proactive detection function is disabled for the RADIUS server.

Verification

Run the **show radius server** command to check accessibility information of each RADIUS server.

Related Commands

Configuring the Global Criteria for Determining 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, the device considers that the RADIUS security server meets the inaccessibility duration condition. The value ranges from 1 to 120, in 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, the device considers 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 the condition of the duration condition and consecutive request timeout count, the device considers that the RADIUS security server is unreachable. You can use this command to adjust the duration condition and consecutive request timeout count.

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, in minutes. The value ranges from 1 to 1,440 (24 hours).
Command Mode	Global configuration mode
Usage Guide	If the proactive 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 proactive 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 unreachable state exceeds the time specified in **radius-server deadtime**.

Configuration Example

Configuring Accessibility Detection on the RADIUS Server

Scenario **Figure 3-3**	

Configuration Steps	1. Configure the global criteria for determining that a RADIUS security server is unreachable. 2. 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 device from the server at 192.168.5.22. Perform RADIUS authentication on 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 Units of Data Flows and Data Packets Sent to the RADIUS Server

Configuration Effect

Configure the units of data flows and data packets sent to the RADIUS server.

Notes

Specify the units of data flows and data packets as required.

Configuration Steps

↘ **Configuring the Units 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 Units 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 Load Balancing for the RADIUS Server Group

Configuration Effect

Client authentication packets are sent to different servers in the server group through polling. The authentication packets from one client are sent to the same server, while the authentication packets from the next client are sent to the next server.

Notes

- The servers in the same server group must have the same configurations, including the username, password, and authorization policy.

- Ensure that the accounts registered on one server are automatically synchronized to the other servers in the server group, or the authentication will be affected.

Configuration Steps Configuring Load Balancing for the RADIUS Server Group

Optional.

Command	**load-balance**
Parameter Description	N/A
Command Mode	Server group configuration mode
Usage Guide	When multiple servers form a server group and they share the same configurations, enable load balancing to reduce the resource consumption of a single server.

Verification

Run the **show running-config** command to verify the configuration result.

1.4.7 Configuring the Function of Copying Accounting Packets

Configuration Effect

- Accounting packets are copied and sent to servers in a specified server group based on the configuration. Currently, accounting packets are sent to only the first three servers configured in the specified server group.

Notes

- When you configure the target server group to which accounting packets are copied and sent, ensure that the servers in the target server group are different from the servers in the current server group. Otherwise, accounting may be inaccurate.

Configuration Steps

Configuring the Function of Copying Accounting Packets

- Optional.

Command	**accounting-copy** *group_name*
Parameter Description	*group_name*: Indicates the name of the target server group that receives accounting packets to be synchronized. The value is a string of 1 to 64 characters.
Command Mode	Server group configuration mode
Usage Guide	1. When you configure the target server group to which accounting packets are copied and sent, ensure that the servers in the target server group are different from the servers in the current server group. Otherwise, accounting may be inaccurate. 2. By default, accounting packets are copied and sent to only the first three servers configured in the target server group. If the first three servers contain a server that sends and receives accounting packets, this server is automatically ignored, and accounting packets are sent to the first three servers configured in the server group in sequence.

Verification

- Run the **show running-config** command to display the configured target server group for accounting packet synchronization.

- Run the **show radius group** command to display detailed information about the target server group for accounting packet synchronization.

1.4.8 Configuring RadSec Target Attributes

Configuration Effect

The TLS protocol guarantees secure communication of RADIUS requests.

Notes

To use the RadSec service, you must define a RadSec server as the target and divert the RADIUS traffic to the target.

Configuration Steps

Associating a RADIUS Server with a RadSec Target

- Mandatory.
- Configure a RadSec server as the target to receive traffic redirected from the standard RADIUS server.

Configuring RadSec Attributes

- Mandatory.
- Specify related parameters for the RadSec server. This step is required if you want to enable the RadSec function.

Verification

- Configure RADIUS traffic redirection and perform user authentication, authorization, and accounting.
- When the device exchanges data with a RadSec server, obtain TLS packets.
- When the device exchanges data with a RADIUS server, check whether exchange between the device and the RadSec server is normal based on the debugging information.

Related Commands

Configuring Attributes of the RadSec Server

Command	**radsec destination** *id-number* **host** *ipv4-address* [**port** *port-number*] [**tls-timeout** *seconds*] [**keep-alive** *times*]
Parameter Description	*id-number*: Indicates the unique ID of the RadSec server. *ipv4-address*: Indicates the IP address of the RadSec target server. *port-number*: Indicates the port number of the RadSec server. *seconds*: Indicates the TLS connection timeout period, in seconds. *times*: Indicates the keepalive packet sending interval, in seconds.
Command Mode	Global configuration mode
Usage Guide	This command can be used to configure the required information of the RadSec target server. The RadSec server and the RADIUS server can be the same server or different servers. Null RADIUS requests are used as keepalive packets. The minimum keepalive packet sending interval is 20s, and the maximum interval is 86400s. The keepalive packet sending interval must be smaller than the server keepalive interval.

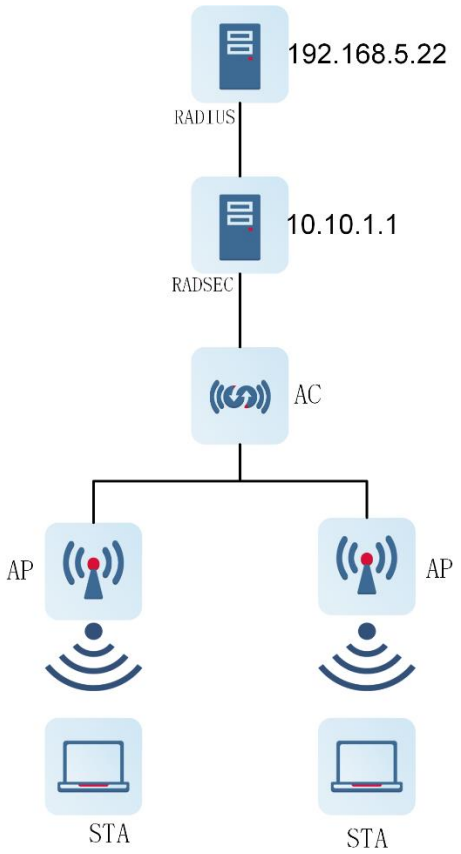
Configuration Example

The following configuration example describes RadSec-related configuration only.

Configuring RadSec Target Attributes

Scenario

Figure 1-1



Prerequisites

1. Interfaces, IP addresses, and VLANs are configured on the network, the network is connected, and the route from the NAS device to the server is reachable.
2. 802.1X authentication is enabled.

Configuration Steps

- Associate the RADIUS server with the RadSec target.
- Set the unique ID of the RadSec target server to 10, the IP address to 10.10.1.1, the port number to 2022, and the TLS keepalive interval to 300s.

```
Hostname(config)# radius-server host 192.168.5.22 radsec-destination 10

Hostname(config)# radsec destination 10 host 10.10.1.1 port 2022 keep-alive 300
```

Verification

- Obtain packets or view debugging information to check whether TLS packets are correctly encapsulated or parsed.
- 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 State: Active

Radsec server port : 2022

tls-timeout        : 5 Seconds

Keep alive time    : 300 Seconds
```

1.5 Monitoring

Clearing

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

Command	Description
clear radius user diag	Clears RADIUS user tracks.
clear radius event diag	Clears RADIUS message tracks.

Displaying

Command	Description
show radius parameter	Displays global parameters of the RADIUS server.
show radius server	Displays the configuration of the RADIUS server.
show radius vendor-specific	Displays the configuration of the RADIUS private attribute type.
show radius dynamic-authorization-extension statistics	Displays statistics on the RADIUS dynamic authorization extension function.
show radius auth statistics	Displays statistics on RADIUS authentication.
show radius acct statistics	Displays statistics on RADIUS accounting.
show radius group	Displays configuration of RADIUS server groups.
show radius attribute	Displays RADIUS standard attributes.
show radius user diag { **all** | **by-id** *session-id* | **by-mac** *mac-address* | **by-ip** *ip-address* }	Displays information about RADIUS user tracks.
show radius event diag coa { **all** | **by-id** *msg-id* }	Displays information about RADIUS Change of Authorization (CoA) message tracks.
show radius event diag dm { **all** | **by-id** *msg-id* }	Displays information about RADIUS DM message tracks.
show radsec statistics	Displays statistics on a RadSec target.
show radsec state	Displays the RadSec connection status.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debugradiusevent	Debugs the RADIUS event.

debugradiusdetail	Debugs RADIUS packet printing.
debug radiusextension event	Debugs the RADIUS dynamic authorization extension function.
debug radius extension detail	Debugs the RADIUS dynamic authorization extension packet printing.

Adjusting

Description	Command
radius event-diag msg-num *num*	Adjusts the total number of RADIUS message track records.
radius event-diag log-num *num*	Adjusts the number of tracks that can be recorded for each RADIUS message.
radius user-diag user-num *num*	Adjusts the total number of RADIUS user track records.

1 Configuring TACACS+

1.1 Overview

TACACS+ is an enhanced security protocol based on the Terminal Access Controller Access Control System (TACACS) protocol. It provides advanced functionality for implementing authentication, authorization, and accounting (AAA) for multiple users.

Protocols and Standards

- RFC 1492: Terminal Access Controller Access Control System

1.2 Applications

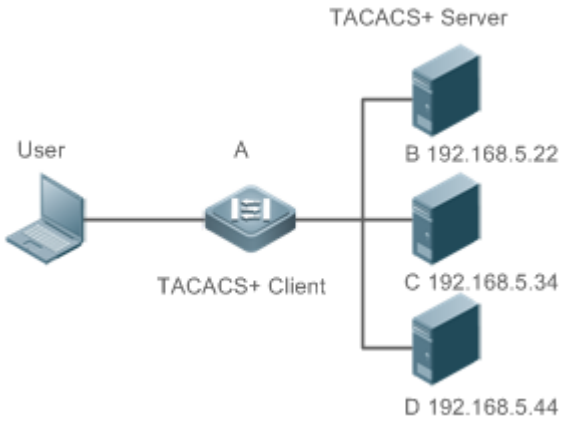
Application	Description
Managing and Controlling Login of End Users	Password authentication and authorization need to be performed on end users.

1.2.1 Managing and Controlling Login of End Users

Scenario

TACACS+ is typically applied for login management and control of end users. A network device serves as the TACACS+ client and sends the user name and password to the TACACS+ server for authentication. The user is allowed to log in to the network device and perform operations after passing authentication and obtaining authorization.

Figure 1-1



Remarks	
	● Device A is a client that initiates TACACS+ requests. ● Server B, Server C, and Server D process TACACS+ requests.

Deployment

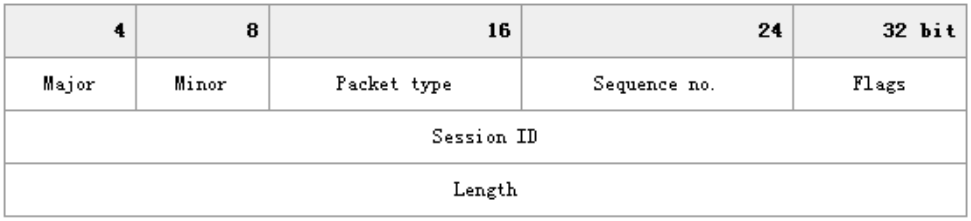
- Start the TACACS+ server on Server B, Server C, and Server D, and configure information on the access device (Device A) so that the servers provide AAA functions based on TACACS+ for the access device. Enable the AAA function on Device A to start authentication for user login.
- Enable the TACACS+ client function on Device A, configure IP addresses of TACACS+ servers (Server B, Server C, and Server D) and the shared key so that Device A communicates with the TACACS+ servers to implement AAA functions.

1.3 Features

Basic Concepts

↘ Format of TACACS+ Packets

Figure 1-2



- Major: Indicates the major TACACS+ version number.
- Minor: Indicates the minor TACACS+ version number.
- Packet Type: Indicates the type of packets:
  - TAC_PLUS_AUTHEN: = 0x01 (authentication)
  - TAC_PLUS_AUTHOR: = 0x02 (authorization)
  - TAC_PLUS_ACCT: = 0x03 (accounting)
- Sequence no.: Indicates the sequence number of a data packet in a session. The sequence number of the first TACACS+ data packet in a session must be 1 and that of each subsequent data packet increases by one. Therefore, the client sends data packets only with an odd sequence number and TACACS+ Daemon sends packets only with an even sequence number.
- Flags: Contains various bitmap format flags. The value specifies whether data packets need to be encrypted.
- Session ID: Indicates the ID of a TACACS+ session.
- Length: Indicates the body length of a TACACS+ data packet (excluding the header). Packets are encrypted for transmission on a network.

Overview

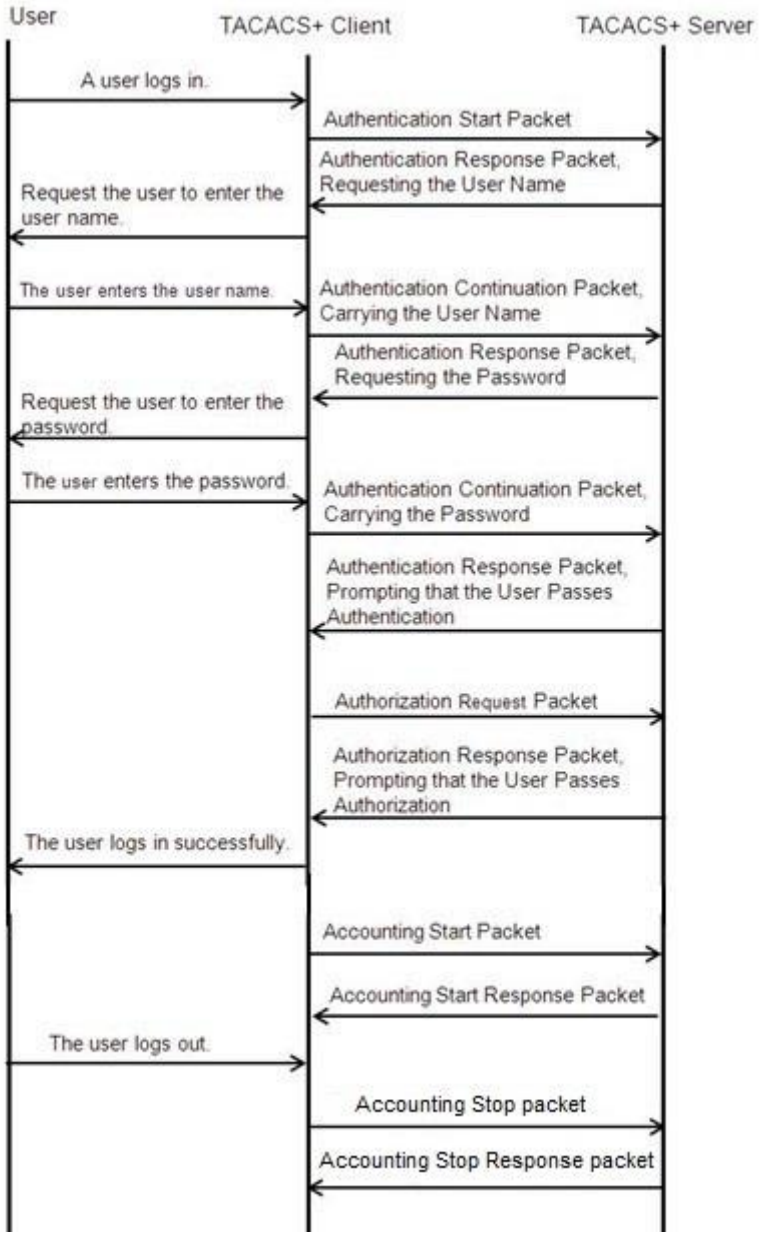
Feature	Description
TACACS+ Authentication, Authorization, and Accounting	Performs authentication, authorization, and accounting on end users.

1.3.1 TACACS+ Authentication, Authorization, and Accounting

Working Principle

Figure 1-3 uses basic authentication, authorization, and accounting of user login to describe exchange of TACACS+ data packets.

Figure 1-3



Packet exchange involves authentication, authorization, and accounting processes:

1. Authentication process:

   (1) A user requests to log in to a network device.

   (2) After receiving the request, the TACACS+ client sends an Authentication Start packet to the TACACS+ server.

   (3) The TACACS+ server returns an authentication response packet, requesting the user name.

(4) The TACACS+ client requests the user to enter the user name.

(5) The user enters the login user name.

(6) After receiving the user name, the TACACS+ client sends an Authentication Continue packet that carries the user name to the TACACS+ server.

(7) The TACACS+ server returns an authentication response packet, requesting the login password.

(8) The TACACS+ client requests the user to enter the login password.

(9) The user enters the login password.

(10) After receiving the login password, the TACACS+ client sends an Authentication Continue packet that carries the login password to the TACACS+ server.

(11) The TACACS+ server returns an authentication response packet, indicating that the user passes authentication.

2. User authorization starts after successful authentication:

(1) The TACACS+ client sends an authorization request packet to the TACACS+ server.

(2) The TACACS+ server returns an authorization response packet, indicating that the user passes authorization.

(3) After receiving the authorization success packet, the TACACS+ client displays the network device configuration interface for the user.

3. Accounting and audit need to be conducted on the login user after successful authorization:

(1) The TACACS+ client sends an Accounting Start packet to the TACACS+ server.

(2) The TACACS+ server returns an accounting response packet, indicating that the Accounting Start packet has been received.

(3) The user logs out.

(4) The TACACS+ client sends an Accounting Stop packet to the TACACS+ server.

(5) The TACACS+ server returns an accounting response packet, indicating that the Accounting Stop packet has been received.

1.4 Configuration

Configuration	Description and Command	
Configuring TACACS+ Basic Functions	(Mandatory) It is used to enable the TACACS+ security service.	
	tacacs-server host	Configures the TACACS+ server.
	tacacs-server key	Specifies the key shared by the server and network device.
	tacacs-server timeout	Configures the global waiting timeout time of the TACACS+ server for communication between a network device and the TACACS+ server.

	ip tacacs source-interface *interface-name*	Specifies the source address for TACACS+ packets.
Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+	⚠ (Optional) It is used to separately process authentication, authorization, and accounting requests.	
	aaa group server tacacs+	Configures TACACS+ server groups and assigns TACACS+ servers to different groups.
	server	Adds servers to TACACS+ server groups.

1.4.1 Configuring TACACS+ Basic Functions

Configuration Effect

- TACACS+ basic functions are available after the configuration is complete. When configuring the AAA method list, specify the TACACS+ method to implement TACACS+ authentication, authorization, and accounting.
- When authentication, authorization, and accounting operations are performed, TACACS+ initiates authentication, authorization, and accounting requests to configured TACACS+ servers according to the sequence in which they were configured. If response timeout occurs on a TACACS+ server, TACACS+ traverses the TACACS+ server list in sequence.

Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

Configuration Steps

↘ Enabling AAA

- Mandatory. The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

Command	**aaa new-model**
Parameter Description	N/A
Defaults	The AAA function is disabled.
Command Mode	Global configuration mode
Usage Guide	The AAA method list can be configured only after AAA is enabled. TACACS+ provides services according to the AAA method list.

↘ Configuring the IP Address of the TACACS+ Server

- Mandatory. Otherwise, a device cannot communicate with the TACACS+ server to implement the AAA function.

Command	**tacacs-server host** { *ipv4-address* | *ipv6-address* } [**port** *integer* | **timeout** *integer*] * [**key** [**0** | **7**] *text-string*]
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. *ipv6-address*: Indicates the IPv6 address of the TACACS+ server. **port** *integer*: Indicates the TCP port used for TACACS+ communication. The default TCP port is 49. **timeout** *integer*: Indicates the timeout interval for communication with the TACACS+ server. The global timeout interval is used by default. **key** [**0** | **7**] *text-string*: Indicates the shared key of the server. The global key is used if it is not configured. An encryption type can be specified for the configured key. The value **0** indicates no encryption and **7** indicates simple encryption. The default value is **0**.
Defaults	No TACACS+ server is configured.
Command Mode	Global configuration mode
Usage Guide	1. You can specify the shared key of the server when configuring the IP address of the server. If no shared key is specified, the global key configured using the **tacacs-server key** command is used as the shared key of the server. The shared key must be the same as that configured on the server. 2. You can specify the communication port of the server when configuring the IP address. 3. You can specify the communication timeout interval of the server when configuring the IP address. 4. You can specify the mode of a TCP connection with the server.

Configuring the Shared Key of the TACACS+ Server

- Optional.
- If no global communication protocol is configured using this command, set **key** to specify the shared key of the server when running the **tacacs-server host** command to add server information. Otherwise, a device cannot communicate with the TACACS+ server.
- If no shared key is specified by specifying **key** when you run the **tacacs-server host** command to add server information, the global key is used.

Command	**tacacs-server** [**key** [**0** | **7**] *text-string*]
Parameter Description	*text-string*: Indicates the text of the shared key. **0 | 7**: Indicates the encryption type of the key. The value **0** indicates no encryption and **7** indicates simple encryption.
Defaults	No shared key is configured for any TACACS+ server.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the global shared key for servers. To specify a different key for each server, set **key** when running the **tacacs-server host** command.

Configuring the Timeout Time of the TACACS+ Server

- Optional.
- You can set the timeout interval to a large value when the link between the device and the server is unstable.

Command	**tacacs-server timeout***seconds*

Parameter Description	*seconds*: Indicates the timeout interval, in seconds. The value range is from 1 to 1,000.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the global server response timeout interval. To set the different timeout interval for each server, set **timeout** when running the **tacacs-server host** command.

Configuring the Source Address for TACACS+ Packets

- Optional.
- To reduce the workload of maintaining a large number of NAS information on the TACACS+ server, you can use this command to set the source address for TACACS+ packets.

Command	**ip tacacs source-interface** *interface-name*
Parameter Description	*interface-name*: Indicates the name of the interface with the source address for TACACS+ packets.
Defaults	The source address for TACACS+ packets is specified by the network layer by default.
Command Mode	Global configuration mode
Usage Guide	To reduce the workload of maintaining a large number of NAS information on the TACACS+ server, you can use this command to set the source address for TACACS+ packets. Then the source address for TACACS+ packets will be set to the first IP address of the specified interface.

Verification

Configure the AAA method list that specifies TACACS+ for authentication, authorization, and accounting on users.

- Enable the device to interact with the TACACS+ server and obtain packets to check the TACACS+ exchange process between the device and the TACACS+ server.
- View server logs to check whether authentication, authorization, and accounting are normal.

Configuration Example

Using TACACS+ for Login Authentication

Scenario **Figure 1-4**	
Remarks	• Device A is a client that initiates TACACS+ requests. • Server B processes TACACS+ requests.
Configuration	• Enable AAA.

Steps	● Configure TACACS+ server information. ● Configure the TACACS+ method for authentication. ● Apply the configured authentication method to an interface.

Device A	`Hostname# configure terminal`
	`Hostname(config)# aaa new-model`
	`Hostname(config)# tacacs-server host 192.168.5.22`
	`Hostname(config)# tacacs-server key aaa`
	`Hostname(config)# aaa authentication login test group tacacs+`
	`Hostname(config)# line vty 0 4`
	`Hostname(config-line)# login authentication test`

Verification	Log in to a device from a PC through Telnet. The user is asked to enter the user name and password. Enter the correct user name and password to log in to the device. View the authentication log of the user on the TACACS+ server.

Common Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- No method list is configured.

1.4.2 Configuring Separate Processing of Authentication, Authorization, and Accounting of TACACS+

Configuration Effect

- Authentication, authorization, and accounting in the security service are processed by different TACACS+ servers, which improves security and achieves load balancing.

Notes

- The TACACS+ security service is a type of AAA service. You need to run the **aaa new-model** command to enable the security service.
- Only one security service is provided after TACACS+ basic functions are configured. To make the TACACS+ functions take effect, specify the TACACS+ service when configuring the AAA method list.

Configuration Steps

↘ Configuring TACACS+ Server Groups

- Mandatory. There is only one TACACS+ server group by default, which cannot implement separate processing of authentication, authorization, and accounting.
- Three TACACS+ server groups need to be configured for separately processing authentication, authorization, and accounting.

Command	**aaa group server tacacs+***group-name*
Parameter Description	*group-name*: Indicates the name of a group. A group name cannot be **radius** or **tacacs+**, which are the names of embedded groups.
Defaults	No TACACS+ server group is configured.
Command Mode	Global configuration mode
Usage Guide	Group TACACS+ servers so that authentication, authorization, and accounting are completed by different server groups.

Adding Servers to TACACS+ Server Groups

- Mandatory. If no server is added to a server group, a device cannot communicate with TACACS+ servers.
- In server group configuration mode, add the servers that are configured using the **tacacs-server host** command.

Command	**server {***ipv4-address* | *ipv6-address*}
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the TACACS+ server. *ipv6-address*: Indicates the IPv6 address of the TACACS+ server.
Defaults	No server is configured.
Command Mode	TACACS+ server group configuration mode
Usage Guide	Before configuring this command, you must run the **aaa group server tacacs+** command to enter the TACACS+ server group configuration mode. For the address of a server configured in a TACACS+ server group, the server must be configured using the **tacacs-server host** command in global configuration mode. If multiple servers are added to one server group, when one server does not respond, the device continues to send a TACACS+ request to another server in the server group.

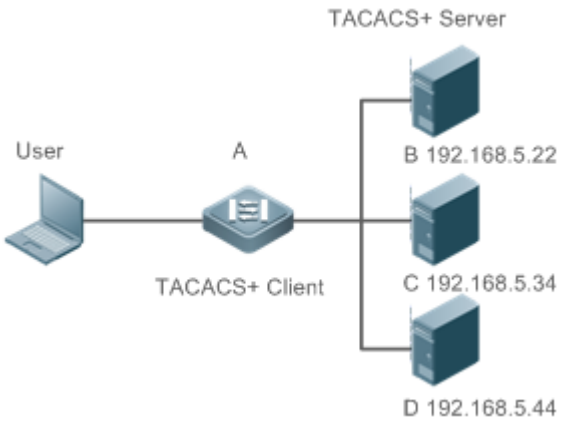
Verification

Configure the AAA method list that specifies TACACS+ for authentication, authorization, and accounting on users.

- Enable a device to interact with TACACS+ servers. Obtain packets to check that authentication, authorization, and accounting packets are exchanged with different servers, and check the source addresses in packets.

Configuration Example

Configuring Different TACACS+ Server Groups for Separately Processing Authentication, Authorization, and Accounting

Scenario **Figure 1-5**	
Remarks	● Device A is a client that initiates TACACS+ requests. ● Server B processes TACACS+ authentication requests. ● Server C processes TACACS+ authorization requests. ● Server D processes TACACS+ accounting requests.
Configuration Steps	● Enable AAA. ● Configure TACACS+ server information. ● Configure TACACS+ server groups. ● Add servers to TACACS+ server groups. ● Configure the method of using TACACS+ for authentication. ● Configure the method of using TACACS+ for authorization. ● Configure the method of using TACACS+ for accounting. ● Apply the configured authentication method to an interface. ● Apply the configured authorization method to an interface. ● Apply the configured accounting method to an interface.
	Hostname# configure terminal Hostname(Hostname(config)# aaa new-model Hostname(config)# tacacs-server host 192.168.5.22 Hostname(config)# tacacs-server host 192.168.5.34 Hostname(config)# tacacs-server host 192.168.5.44 Hostname(config)# tacacs-server key aaa Hostname(config)# aaa group server tacacs+ tacgrp1 Hostname(config-gs-tacacs)# server 192.168.5.22 Hostname(config-gs-tacacs)# exit Hostname(config)# aaa group server tacacs+ tacgrp2 Hostname(config-gs-tacacs)# server 192.168.5.34 Hostname(config-gs-tacacs)# exit Hostname(config)# aaa group server tacacs+ tacgrp3

	Hostname(config-gs-tacacs)# server 192.168.5.44 Hostname(config-gs-tacacs)# tacacs-server single-connect-timeout 5 Hostname(config-gs-tacacs)# exit Hostname(config)# aaa authentication login test1 group tacacs+ Hostname(config)# aaa authentication enable default group tacgrp1 Hostname(config)# aaa authorization exec test2 group tacgrp2 Hostname(config)# aaa accounting commands 15 test3 start-stop group tacgrp3 Hostname(config)# line vty 0 4 Hostname(config-line)# login authentication test1 Hostname(config-line)#authorization exec test2 Hostname(config-line)# accounting commands 15 test3
Verification	Log in to a device from a PC through Telnet. The user is asked to enter the user name and password. Enter the correct user name and password to log in to the device. Enter the **enable** command and enter the correct **enable** password to initiate Enable authentication. Enter the privilege EXEC mode after passing authentication. Perform operations on the device and then exit the device. View the authentication log of the user on the server at 192.168.5.22. View the **enable** authentication log of the user on the server at 192.168.5.22. View the **exec** authorization log of the user on the server at 192.168.5.34. View the command accounting log of the user on the server at 192.168.5.44.

Common Errors

- The AAA security service is disabled.
- The key configured on the device is inconsistent with the key configured on the server.
- Undefined servers are added to a server group.
- No method list is configured.

1.5 Monitoring

Displaying

Command	Description
show tacacs	Displays interaction with each TACACS+ server.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug tacacs+ detail	Debugs TACACS+.

1 Configuring 802.1X

1.1 Overview

IEEE 802.1X is a port-based network access control that provides secure access service for local area networks (LANs).

On an IEEE 802-compliant LAN, users connecting to the network access devices (NASs) can access network resources without authentication and authorization, bringing security risks to the LAN. The IEEE 802.1X standard is proposed to resolve security problems of such a LAN.

802.1X provides authentication, authorization, and accounting (AAA):

- Authentication: Controls network access and restricts unauthorized users.
- Authorization: Grants services to users and controls permissions of authorized users.
- Accounting: Records network resources consumed by users for subsequent billing.
- 802.1X can be deployed on a network to realize user authentication, authorization, and other functions.

Protocols and Standards

- IEEE 802.1X: Port-Based Network Access Control

1.2 Applications

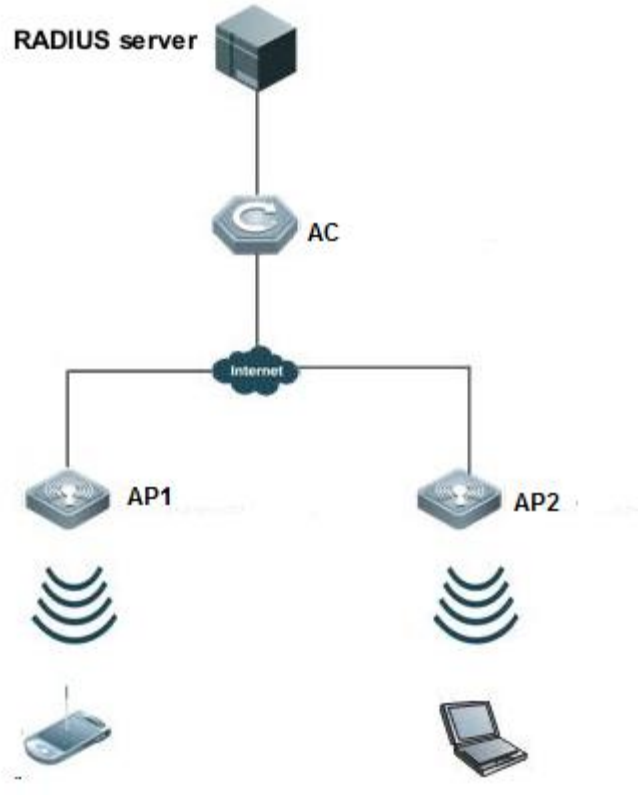
Application	Description
Wireless 802.1X Authentication	When an enterprise deploys a wireless LAN (WLAN), 802.1X authentication is enabled on the access controller (AC).
EAP Termination	When an enterprise deploys a WLAN, the Extensible Authentication Protocol (EAP) termination function of 802.1X authentication is enabled on the AC.

1.2.1 Wireless 802.1X Authentication

Scenario

- On the wireless authentication network where Fat APs and the authentication server are deployed, 802.1X is enabled on fat APs for secure access control. Wireless stations (STAs) must pass 802.1X authentication to access the enterprise network, as shown in Figure 1-1: STAs have the IEEE 802.1X-compliant software installed, which may come with the operating system or others such as Ruijie Supplicant.
- The AC supports 802.1X.
- One or more Remote Authentication Dial in User Service (RADIUS) servers are used for authentication.

Figure 1-1



Remarks	STAs support 802.1X authentication. After connecting to APs, they will be authenticated through 802.1X. 802.1X authentication is enabled on the AC. The RADIUS server runs the RADIUS server software to perform identity verification.

Deployment

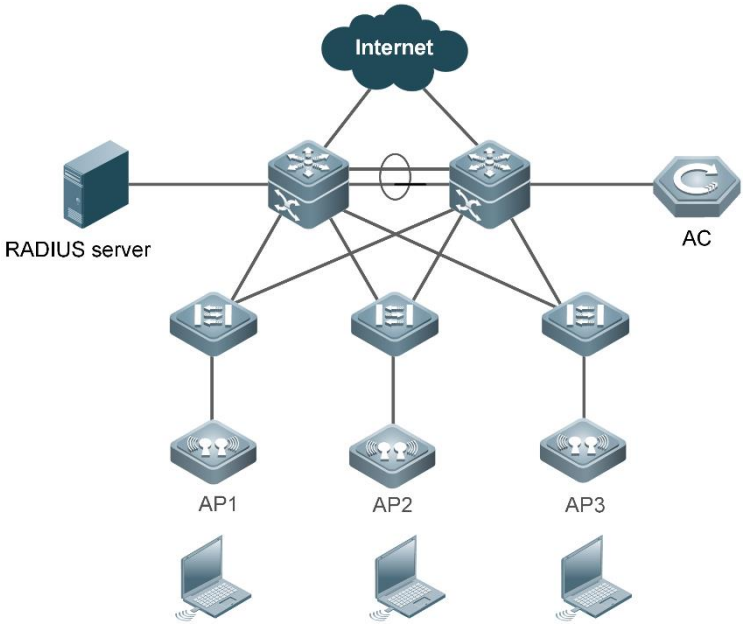
- Enable 802.1X authentication on the AC based on the WLANs broadcast by APs to control access of associated STAs. Only authenticated STAs can access the network.
- Configure an AAA authentication method list so that an appropriate method and the authentication server are adopted in 802.1X authentication.
- Configure RADIUS parameters to ensure communication between the AC and the RADIUS server. For details, see Configuring RDS.
- If a Ruijie RADIUS server is used, configure Simple Network Management Protocol (SNMP) parameters so that the RADIUS server can search and configure connected devices.
- Create accounts, register IP addresses of connected devices, and configure RADIUS parameters so that the RADIUS server can respond to requests of the AP or AC.

1.2.2 EAP Termination

Scenario

As shown in Figure1-2, an AC, APs, and a RADIUS authentication server are deployed on a wireless network. 802.1X authentication is configured on the AC for network access. The RADIUS authentication server does not support the EAP protocol. Therefore, EAP termination of 802.1X authentication needs to be enabled on the AC.

Figure 1-11



Deployment

- Configure a WLAN.
- Configure 802.1X authentication mode to ensure wireless network security.
- Configure the 802.1X authentication method list of AAA.
- Configure a RADIUS server.
- Enable EAP termination of 802.1X authentication.

1.3 Features

Basic Concepts

User

IEEE 802.1X, a LAN-based protocol, identifies users based on physical information but not accounts. Except for them, all other information such as the account ID and IP address may vary. On WLANs, one MAC address represents an STA.

RADIUS

RADIUS is a widely used remote authentication protocol defined in RFC 2865. With this protocol deployed, the authentication server can be remotely deployed to perform authentication. Authentication information between the NAS and the authentication server is transmitted through RADIUS packets.

Timeout

During authentication, an NAS needs to communicate with the authentication client and server. If the client or server does not respond and authentication times out, authentication fails. Ensure that the 802.1X authentication timer is longer than the RADIUS timer.

MAB

MAC address bypass (MAB) authentication uses the MAC address as the username and password for authentication. Because some dumb terminals such as printers cannot have Ruijie Supplicant installed, MAB authentication is adopted to perform security control.

EAP

802.1X uses the Extensible Authentication Protocol (EAP) to carry authentication information. Defined in RFC 3748, EAP provides a universal authentication framework with multiple authentication modes embedded, including Message Digest Algorithm 5 (MD5), Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), and Transport Layer Security (TLS). The NAS supports various authentication 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 QoS binding.

Accounting

Accounting performs network audit on online duration and traffic usage, which facilitates network O&M and management.

Some RADIUS servers such as RG-SAM+ and RG-SMP servers need to check the online and offline status based on accounting packets. Therefore, accounting must be enabled on these RADIUS servers.

RIPT

The Remote Intelligent Perceptive Technology (RIPT) ensures availability of Wireless Local Area Networks (WLANs) when the AC fails or the CAPWAP tunnel between an AP and an AC is terminated, allowing the AP to continue providing wireless services. 802.1X can be used with RIPT.

Overview

Feature	Description
Authentication	Provides secure access for users. Only authenticated users can access the network.
Authorization	Grants permissions to authenticated users, such as IP address binding and ACL binding.
Accounting	Audits online records, such as the online duration and traffic.
EAP Termination	Terminates EAP packets and forwards simple authentication information carried in the EAP protocol to the external server.

1.3.1 Authentication

Authentication aims to check clients' identities and prevent unauthorized access to a network. Clients must pass authentication to obtain the network access permission, and can access the network only after the authentication server verifies the account. Before authentication succeeds, only Extensible Authentication Protocol over LAN (EAPOL) packets) can be transmitted over the network for authentication.

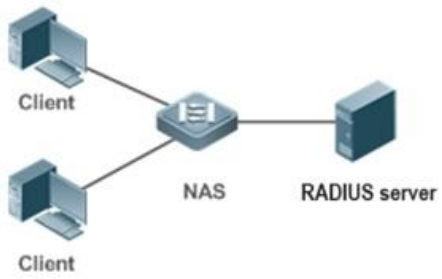
Working Principle

802.1X authentication is simple. After a client submits its account information, the NAS sends the account information to the remote RADIUS server for identity authentication. If the authentication succeeds, the client can access the network.

Roles in Authentication

802.1X authentication involves three roles: supplicant, authenticator, and server, which correspond to the client, NAS, and authentication server (RADIUS server typically) respectively.

Figure 4-3



- Supplicant

The supplicant is the role of clients, which is usually a PC. It requests to access network services and replies to the request packets of the authenticator. The supplicant must run software in compliance with the IEEE 802.1X standard. Except for the typical 802.1X-compliant software that comes with the operating system, Ruijie Supplicant also meets the requirement.

- Authenticator

The authenticator is typically an NAS such as a 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 authentication information from the server, and forwards it to the client. In addition to the 802.1X authenticator, the NAS also acts as a RADIUS client. It encapsulates the response packet of the client into the RADIUS packets and forwards the packets to the RADIUS server. After receiving 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. Clients connected to the controlled ports can access network resources only when being authenticated. Clients connected to the uncontrolled ports can directly access network resources without authentication. Clients can be connected to the controlled ports for security control. The uncontrolled ports are mainly used to connect the authentication server to ensure communication between the authentication server and the NAS.

- Authentication server

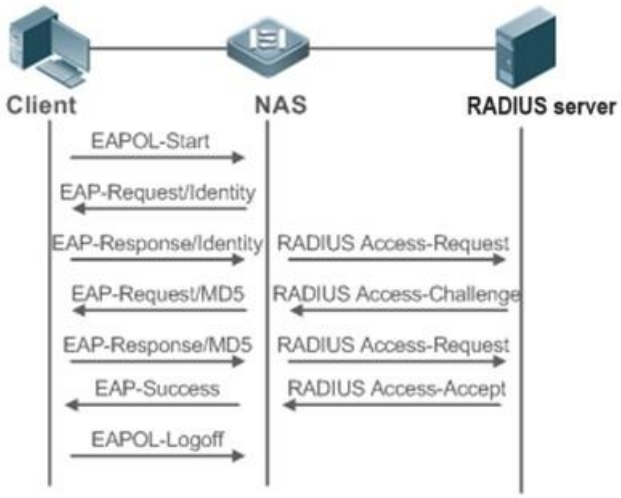
The authenticator server is usually an RADIUS server. It is used with the authenticator to provide the authentication service for clients. The authentication server saves usernames, passwords, and related authorization information. One server can provide the authentication service for multiple authenticators to achieve centralized client management. The authentication server also manages accounting data received from authenticators. The NAS enabled with IEEE 802.1Xis compatible with the standard RADIUS server, including Microsoft IAS/NPS, FreeRADIUS, and Cisco Access Control Server (ACS).

↘ Authentication Process and Packet Exchange

The supplicant exchanges information with the authenticator through EAPOL and exchanges information with the authentication server through RADIUS. The EAPOL packet is encapsulated over the MAC layer, with the Ethernet type of 0x888E. The multicast MAC address 01-80-C2-00-00-03 is assigned to EAPOL for packet transmission during initial authentication. Ruijie Supplicant may also use 01-D0-F8-00-00-03 for initial authentication packets.

Figure 4-4 shows the typical authentication process of a wired client.

Figure 4-4



This is a typical authentication process initiated by a user. In special cases, the NAS may take the place of the user to initiate an authentication request.

Authenticating the User Status

802.1X determines whether a user on a port can access the network based on the authentication status of the port. Based on 802.1X, the NAS realizes access control based on users (identify a wired user by the MAC address and VLAN ID and identify a STA by the MAC address) by default. 802.1X can also be enabled in interface configuration mode on the NAS.

All users on an uncontrolled port can access network resources, while users on a controlled port can access network resources only after being authorized. When a user initiates authentication, its status remains unauthorized and cannot access the network. 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 packet requesting the user name of the user by the NAS. In this case, the user remains unauthorized and cannot access network resources.

In the scenario where the user supports 802.1X but the NAS does not support 802.1X, if the user does not receive any response after sending a specified number of EAPOL-Start packets, the user considers that the connected port is the uncontrolled port and directly accesses network resources.

On the 802.1X-enabled device, all ports are uncontrolled by default. A port can be configured as controlled so that all users connected to this port need 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 free from authentication, you are advised to add a static MAC address or configure IP-MAC binding.

Deploying the Authentication Server

802.1X uses the RADIUS server as the authentication server. That is, when 802.1X is deployed, the RADIUS server also needs to be deployed. Common RADIUS servers include Microsoft IAS/NPS, Cisco ACS, and RG-SAM/SMP.

Configuring Authentication Parameters

To use 802.1X authentication, enable 802.1X authentication on the access port and configure an AAA authentication method list and RADIUS server parameters. To ensure accessibility between the NAS and RADIUS server, configure the 802.1X server timer to be longer than the RADIUS server timer.

Supplicant

A user should start Ruijie Supplicant to enter the user name and initiate authentication. If the authentication client of the operating system is used, 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 that Ruijie Supplicant be used as the authentication client. If other software is used, see related software description.

Logout

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, shutting down the connected port, and using the offline function provided by some supplicants.

1.3.2 Authorization

After a user passes authentication, the NAS restricts accessible network resources of the user in multiple approaches, such as accessible VLANs.

Working Principle

Authorization indicates binding permissions to 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 to a user to implement authorization.

ACL Authorization

After user authentication is complete, the authentication server delivers an ACL or ACE to users. The ACL must have been configured on the authentication server, while no extra configuration is required for the ACE. In this mode, an ACL is delivered based on RADIUS attributes such as standard attributes, Ruijie-proprietary attributes, and Cisco-proprietary attributes.

Logout

The 802.1X authentication server can be used with RG-SAM+ or RG-SMP to disconnect online users. The disconnected users are not allowed to access the network. This function can be used to control the online duration and monitor accounting in real time.

1.3.3 Accounting

Accounting allows a network operator to audit 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 accounting defined in RFC 2869. 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 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 NAS sends the RADIUS server an Accounting Start packet carrying user accounting attributes such as the 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, improving the real-time performance of accounting. 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.

1.3.4 EAP Termination

The device can terminate EAP packets and forward simple authentication information carried in the EAP protocol to the external server. In this case, the device can adapt to external authentication servers that cannot provide the required EAP method. For example, Protected Extensible Authentication Protocol version 1/Generic Token Card (PEAPv1/GTC) is required for client authentication, and the external authentication server can only provide the Password Authentication Protocol (PAP) for authentication.

Working Principle

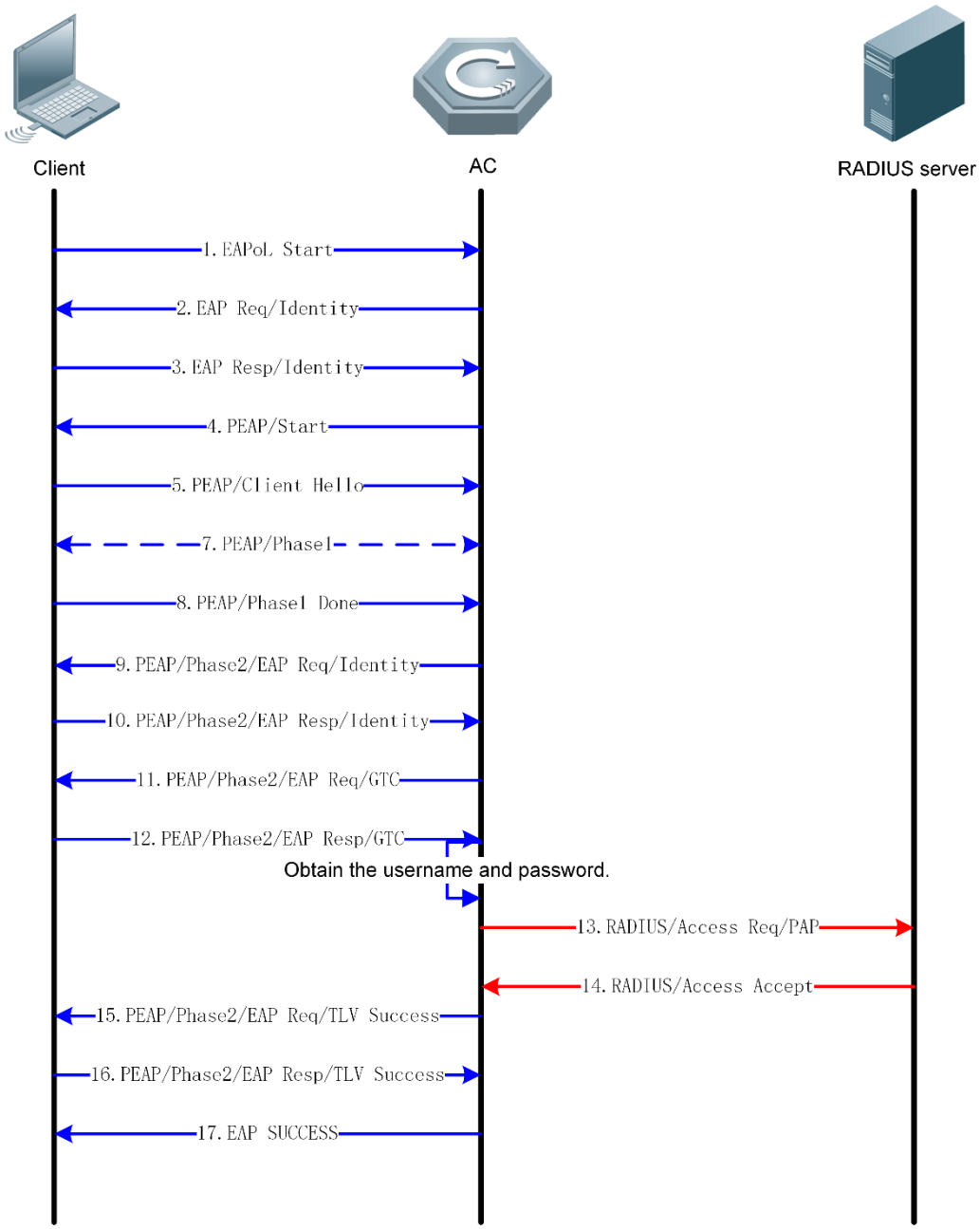
EAP-GTC termination is used as an example to describe the working principle of EAP termination. Figure 1-3 shows the flowchart of EAP-GTC termination. The RADIUS server supports the PAP authentication method only. However, the PEAPv1/GTC authentication method is used between the AC and a client.

- Steps 1 to 12: The AC exchanges packets with a client required by the PEAPv1/GTC authentication method. After step 12 is performed, the AC obtains the client's authentication credential (including the username and cleartext password).
- Steps 13 to 14: The 802.1X module uses the obtained authentication credential to initiate a PAP authentication to the RADIUS server and obtains the authentication success result.

- Steps 15 to 17: Based on the result returned by the RADIUS server, the 802.1X module continues to perform the PEAPv1/GTC authentication process.

In the following flowchart, when the AC performs EAP-GTC termination, the client does not perceive it and regards that a PEAPv1/GTC authentication is performed. However, the RADIUS server regards that the client is performing a PAP authentication. The flowcharts of PEAP termination and EAP-MSCHAPv2 termination are similar.

Figure 1-12



Related Configuration

Configuring EAP Termination

EAP termination is not configured by default.

Run the **dot1x eap-terminate peap inner-methods gtc** command to enable EAP-GTC termination. Run the **dot1x eap-terminate peap inner-methods mschapv2** command to enable EAP-MSCHAPV2 termination.

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 RADIUS server parameters.
	radius-server key	Configures the pre-shared key for communication between the NAS and the RADIUS server.
	dot1x port-control auto	Configures 802.1X authentication on a port.
Configuring 802.1X Parameters	(Optional) It is used to configure 802.1X parameters. Ensure that the 802.1X server timeout is longer than the RADIUS server timeout. Online 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 for retransmitting EAP-Request/Identity packets.
	dot1x reauth-max	Configures the maximum count of EAP-Request/Identity packet retransmission.
	dot1x timeout supp-timeout	Configures the interval for retransmitting EAP-Request/Challenge packets.
	dot1x max-req	Configures the maximum count 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 the connection status detection for Ruijie Supplicant.
	dot1x probe-timer interval	Configures a detection interval for Ruijie Supplicant.

Configuration	Description and Command	
	dot1x probe-timer alive	Configures a detection timer for Ruijie Supplicant.
Configuring Authorization	(Optional). It is used to configure 802.1X parameters. Supplicant authorization is based on Ruijie Supplicant.	
	dot1x private-supplicant-only	Configures the device to filter non-Ruijie supplicants.
	dot1x redirect	Configures the second-generation supplicant update for users to download the supplicant through redirection to the specified website.
	snmp	Configures SNMP parameters. RG-SAM+ or RG-SMP can log off 802.1X authentication users through the SNMP protocol. This function requires SNMP parameter configuration.
Configuring MAB	(Optional) It is used to configure MAC Authentication Bypass (MAB) authentication. 802.1X authentication takes precedence over MAB authentication. Single-MAB authentication and multi-MAB authentication cannot be configured simultaneously. MAB authentication uses PAP. Ensure that the server configuration is correct.	
	dot1x mac-auth-bypass	Configures single-MAB authentication.
	dot1x mac-auth-bypass multi-user	Configures multi-MAB authentication.
	dot1x multi-mab quiet-period	Configures the quiet period after a multi-MAB authentication failure.
	dot1x mac-auth-bypass timeout-activity	Configures the timeout interval of MAB authentication.
	dot1x mac-auth-bypass violation	Configures MAB violation.
	dot1x mac-auth-bypass vlan	Configures a VLAN for MAB authentication.
Configuring EAP Termination	(Optional) It is used to enable EAP termination.	
	dot1x eap-terminate peap inner-methods	Enables EAP termination.
Configuring PKI Information	(Optional) It is used to regenerate or import Public Key Infrastructure (PKI) information.	
	dot1x pki-manage generate self-signed	Regenerates the self-signed PKI information.

Configuration	Description and Command	
	dot1xpki-manage import pfx	Imports PKI information in PKCS#12 format.
Configuring Extended Functions	(Optional) It is used to configure active authentication requests on a port. (Optional) It is used to configure the authenticated client list. (Optional) It is used to configure the device to send 802.1X packets that carries the bogus source MAC address. (Optional) It is used to configure multiple accounts for the same MAC address.	
	dot1x auto-req	Configures the device to initiate 802.1X authentication.
	dot1x auto-req packet-num	Configures the number of automatic authentication request packets.
	dot1x auto-req user-detect	Configures automatic authentication user detection.
	dot1x auto-req req-interval	Configures the interval for the device to initiate authentication requests.
	dot1x auth-address-table address	Configures the trusted host list.
	dot1x pseudo source-mac	Configures the device to use the virtual MAC address as the source MAC address in outgoing 802.1X packets.
	dot1x multi-account enable	Enables multi-account authentication with one MAC address.
	dot1x valid-ip-acct enable	Enables IP address-triggered accounting.
	dot1x valid-ip-acct timeout	Configures the timeout interval for obtaining IP addresses after users are authenticated. If the timeout interval is reached, they will be disconnected.
	dot1x event server-invalid action bypass-wlan	Configures the bypass WLAN for the RADIUS server.
	dot1x encryption only	Configures 802.1X authentication for encryption only when 802.1X and web-based authentication are both enabled.
	dot1x logging rate-limit	Limits the rate of generating online and offline logs.
	dot1x offline-detect	Enables traffic detection on users on a WLAN.
	dot1x user-trap enable	Enables SNMP trap during user login and logout.
	dot1x mab-default-role	Configures the default role of clients after they pass the MAB authentication.

Configuration	Description and Command	
	dot1x dot1x-default-role	Configures the default role of clients after they pass the 802.1X authentication.
	dot1x domain-name	Configures a domain name for 802.1X authentication.
	dot1x dbg-filter	Enables the print information filter.
	dot1x no-ip-before-mab	Disables the clients to obtain the IP address before they pass the MAB authentication.
	dot1x mab-pass-to-web	Configures the web authentication after clients pass the MAB 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 or disable 802.1X authentication on a port.
- On a wireless network, set the WLAN security mode to WPA or WPA2 and enabled 802.1X authentication for the WLAN. The STAs connected to the WLAN can communicate only when they pass 802.1X authentication.
- 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. The parameters assigned by the authentication server takes precedence over the parameters configured on the NAS.

Notes

- Configure accurate RADIUS parameters to ensure correct RADIUS communication.
- The 802.1X authentication method list and accounting method list must be configured in AAA. Otherwise, errors may occur during authentication and accounting.
- If port-based 802.1X authentication is enabled and the number of users to be authenticated exceeds the maximum allowed by port security, port security cannot be enabled.
- If both port security and 802.1X authentication are enabled, and the secure address ages out, the users who are authenticated through 802.1X must be re-authenticated for communication.
- Users with static addresses or users who comply with IP+MAC binding can access the network without authentication.
- 802.1X uses the default method list by default. If the default method list is not configured for AAA, run the **dot1x authentication** and **dot1x accounting** commands to reconfigure it.

- When RG-SAM+ or RG-SMP is used, accounting must be enabled. Otherwise, the RADIUS server will fail to detect users going offline, causing offline users to remain 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 client access through 802.1X authentication.

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 deploying of 802.1X authentication.

Enabling an AAA Authentication Method List

- Mandatory.
- The AAA authentication method list must be consistent with the 802.1X authentication method list.
- Enable an AAA authentication method list after 802.1X authentication is enabled on the NAS.

Command	**aaa authentication dot1x** *list-name* **group radius**
Parameter Description	*list-name*: Indicates the 802.1X authentication method list of AAA.
Defaults	No AAA authentication method list is configured by default.
Command Mode	Global configuration mode
Usage Guide	• AAA authentication modes are disabled by default. • The AAA authentication mode must be consistent with the 802.1X authentication mode.

Configuring RADIUS Server Parameters

- (Mandatory) RADIUS server parameters must be configured to ensure 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 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.

Enabling 802.1X on a Wired Port

- This command is mandatory for a wired port.

Command	**dot1x port-control auto**
Parameter Description	N/A
Defaults	802.1X is disabled on a port by default.
Command Mode	Interface configuration mode and VXLAN mode
Usage Guide	• 802.1X is disabled on a port by default. This command is mandatory for deploying 802.1X authentication. • The default method list is used by default. If the 802.1X authentication method list in AAA is not the default one, the 802.1X authentication method list configured by **dot1x authentication list-name** is used.

Enabling 802.1X

- This function is mandatory on a wireless network.
- Enable 802.1X on an AC.
- If 802.1X is enabled on a WLAN, only 802.11 management frames and EAP packets are allowed to pass.
- For related commands, see *Configuring RSNA*.

Verification

Start Ruijie Supplicant, enter the correct account information, and initiate authentication. Then check whether the 802.1X and RADIUS configurations are correct.

Checking 802.1X Authentication Entries

Command	**show dot1x summary**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and 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 AAA User Entries

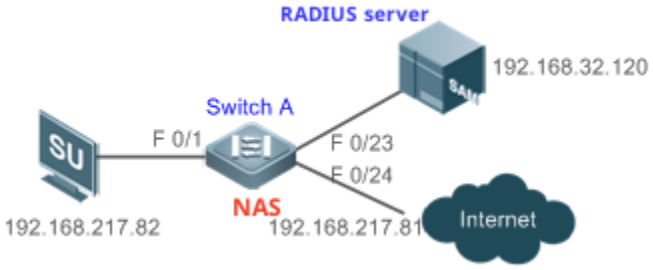
Command	**show aaa user all**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Display information of AAA users.

Command Display	`Hostname#show aaa user all`
	`----------------------------`
	`Id ----- Name`
	`2345687901 wwxy`
	`----------------------------`

- Check whether the RADIUS server responds to authentication based on the RADIUS packets between the NAS and the RADIUS server. If not, the network is disconnected or parameter configurations are incorrect. If the RADIUS server directly returns a rejection response, check the log file on the RADIUS server to identify the cause. For example, check whether the authentication mode of the authentication server is correctly configured.

Configuration Example

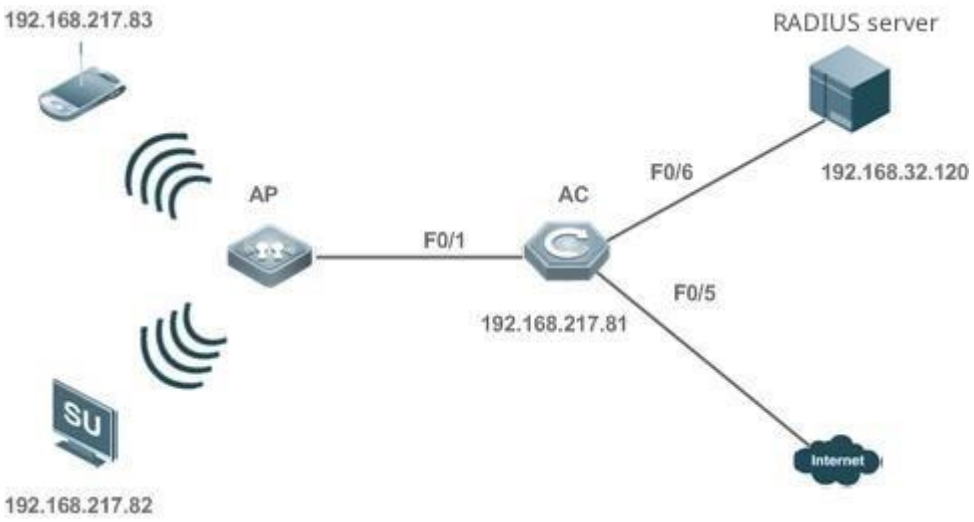
Configuring Wired 802.1X Authentication

Scenario **Figure 1-3**	
Configuration Steps	● Register the IP address of the device on the RADIUS server and configure the key for the device to communicate with the server. ● Create an account on the RADIUS server. ● Enable AAA on the device. ● Configure RADIUS parameters on the device. ● Enable 802.1X authentication on interfaces of the device. ● The following displays the device configuration. For details about the server configuration, see the server configuration guide.

	`Hostname# configure terminal`
	`Hostname(config)# aaa new-model`
	`Hostname(config)# radius-server host 192.168.32.120`
	`Hostname(config)# radius-server key Hostname`
	`Hostname(config)# interface FastEthernet 0/1`
	`Hostname(config-if)# dot1x port-control auto`

Verification	Check whether authentication can be performed normally and whether network access behavior changes after authentication.
	● Create an account on the server, for example, **username:tests-user** or **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 about the authenticated user is displayed.
	`Hostname# show dot1x summary`
	`ID Username MAC Interface VLAN Auth-State`
	`Backend-State Port-Status User-Type Time`
	`--------- ---------- -------------- --------- ---- --------------- -`
	`------------ ----------- --------- -------------------`
	`16778217 ts-user 0023.aeaa.4286 Fa0/1 2 Authenticated`
	`Idle Authed static 0days 0h 0m 7s`

Configuring 802.1X Authentication on a WLAN

Scenario **Figure 4-5**	
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. ● The NAS configuration is as follows. For details about the configuration of the RADIUS server, see *Configuring RADIUS*.

	`Hostname# configure terminal`
	`Hostname(config)# aaa new-model`
	`Hostname(config)# radius-server host 192.168.32.120`
	`Hostname(config)# radius-server key radius-key`
	`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`

Verification	Check whether authentication is normal and whether 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 failures.

1.4.2 Configuring 802.1X Parameters

Configuration Effect

- Adjust 802.1X parameter configurations based on the network situation. For example, if the authentication server has poor performance, you can increase the timeout interval of the authentication server.

Notes

- 802.1X and RADIUS have separate server timeout intervals. By default, the authentication server timeout interval of 802.1X is 5 seconds while that of RADIUS is 15 seconds. In practice, ensure that the former is greater than the latter. You can run the **dot1x timeout server-timeout** command to adjust the authentication server timeout interval of 802.1X. For details, see *Configuring RADIUS*
- Connection status detection for Ruijie supplicants is only supported in Ruijie supplicants.

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-auth period** *period*
Parameter Description	*period*: Indicates the re-authentication interval, in 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 for Retransmitting EAP-Request/Identity Packets

- (Optional) A larger value indicates a longer interval of packet retransmission.
- Configure the interval for retransmitting EAP-Request/Identity packets after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout tx-period** *period*
Parameter Description	*period*: Indicates the interval for retransmitting EAP-Request/Identity packets, in seconds.
Defaults	The default value is 4 seconds.
Command Mode	Global configuration mode
Usage Guide	The default value is recommended. Adjust the value based on the duration during which the authentication client responds to the NAS's requests.

Configuring the Maximum Count of EAP-Request/Identity Packet Retransmission

- (Optional) A larger value indicates more frequent retransmission.
- Configure the maximum count 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 count of EAP-Request/Identity packet retransmission.
Defaults	The default value is 6.
Command Mode	Global configuration mode
Usage Guide	The default value is recommended. In the case of high packet loss rate, increase this value so that the clients can easily receive packets from the NAS.

Configuring the Interval for Retransmitting EAP-Request/Challenge Packets

- (Optional) A larger value indicates a longer retransmission interval.
- Configure the interval for retransmitting EAP-Request/Challenge packets after 802.1X authentication is enabled on the NAS.

Command	**dot1x timeout supp-timeout** *time*
Parameter Description	*time*: Indicates the interval for retransmitting EAP-Request/Challenge packets, in seconds.
Defaults	The default value is 3 seconds.
Command Mode	Global configuration mode

Usage Guide	The default value is recommended. Increase this value in the case of high packet loss rate.

Configuring the Maximum Count of EAP-Request/Challenge Packet Retransmission

- (Optional) A larger value indicates more frequent retransmission.
- Configure the maximum count 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 count of EAP-Request/Challenge packet retransmission, in seconds.
Defaults	The default value is 3.
Command Mode	Global configuration mode
Usage Guide	• Optional. • The default value is recommended. Increase this value in the case of high packet loss rate.

Configuring the Timeout Interval of the Authentication Server

- (Optional) A larger value indicates a longer timeout interval of the authentication server.
- Configure the timeout interval of the authentication server after 802.1X authentication is enabled on the NAS.
- The timeout interval of RADIUS authentication must be greater than that of 802.1X authentication.

Command	**dot1x timeout server-timeout** *time*
Parameter Description	*time*: Indicates the timeout interval of the authentication server, in seconds.
Defaults	The default value is 5 seconds.
Command Mode	Global configuration mode
Usage Guide	The default value is recommended. 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, in seconds.
Defaults	The default value is 10 seconds.
Command Mode	Global configuration mode
Usage Guide	The default value is recommended. 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 the supplicant and the authentication server.

Configuring Connection Status Detection for Ruijie Supplicant

- (Optional) After this function is enabled, Ruijie Supplicant disconnection will be detected in a timely manner, avoiding inaccurate accounting.
- The supplicant must be a Ruijie Supplicant.
- Configure this function after 802.1X authentication is enabled.

Command	**dot1x client-probe enable**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	You are advised to enable this function when using Ruijie Supplicant.

Configuring a Detection Interval for Ruijie Supplicant

- (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 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 Supplicant

- (Optional) A greater value indicates a longer interval at which the device identifies disconnection of Ruijie Supplicant.
- Configure this function after 802.1X authentication is enabled.

Command	**dot1x probe-timer alive** *time*

Parameter Description	*time:* Indicates the interval at which the device identifies disconnection of Ruijie Supplicant, in seconds. The default value 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 Ruijie Supplicant within the period defined by the detection timer, the device identifies disconnection of Ruijie Supplicant. The default value is recommended.

Verification

Run the **show dot1x** command to check whether parameter configurations take effect.

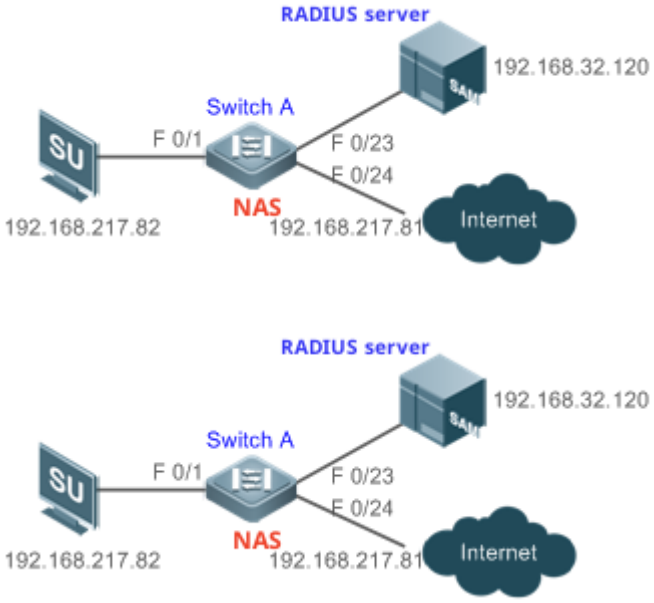
Configuration Example

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(config)#show dot1x`
	
	`802.1X basic information:`
	`  802.1X Status ..... enable`
	`  Authentication Mode ..... chap`
	`  Authorization mode ..... disable`
	`  Total User Number ..... 0 (exclude dynamic user)`
	`  Authenticated User Number ..... 0 (exclude dynamic user)`
	`  Dynamic User Number ..... 0`
	`  Re-authentication ..... disable`
	`  Re-authentication Period ..... 3600 seconds`
	`  Re-authentication max ..... 3 times`
	`  Quiet Period ..... 10 seconds`
	`  Tx Period ..... 30 seconds`
	`  Supplicant Timeout ..... 3 seconds`
	`  Server Timeout ..... 5 seconds`
	`  Maximum Request ..... 3 times`
	`  Client Online Probe ..... disable`
	`  Eapol Tag ..... disable`
	`  802.1x redirect ..... disable`
	`  Private supplicant only ..... disable`

Configuring Connection Status Detection for Ruijie Supplicant

Scenario **Figure 1-4**	
Configuration Steps	Enable connection status detection for Ruijie Supplicant.
	`Hostname(config)#dot1x client-probe enable`
Verification	● Ruijie Supplicant keeps 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 timeout interval of the authentication server is shorter than the timeout interval for RADIUS authentication.
- Connection status detection is configured for non-Ruijie supplicants.

1.4.3 Configuring Authorization

Configuration Effect

- Filtering non-Ruijie supplicants can require STAs to authenticate using Ruijie Supplicant, so the STAs can enjoy services provided by Ruijie Supplicant, such as anti-proxy or short message functions.
- The redirection function supports second-generation supplicant deployment. The second-generation supplicant deployment indicates that STAs download Ruijie Supplicant through a web page and are authenticated through Ruijie Supplicant. This facilitates rapid deployment of Ruijie Supplicant in environments with a large number of users.

Notes

- When using RG-SAM+ or RG-SMP for real-time user logout, correct SNMP parameters need to be configured. You can refer to the SNMP configuration guide for detailed instructions.
- If there are multiple types of authentication client software in the environment, do not enable the device to filter non-Ruijie supplicants.
- Second-generation supplicant deployment and web-based authentication cannot be used simultaneously.
- Configuring redirection parameters is required for second-generation supplicant deployment. For details, see *Configuring Web-based Authentication*.
- SNMP is used for user disconnection of RG-SAM+ or RG-SMP, so SNMP parameters need to be configured. For details, see *Configuring SNMP*.

Configuration Steps

↘ Configuring Second-Generation Supplicant Deployment

- (Optional) After second-generation supplicant deployment is configured, users without the 802.1X authentication client on controlled ports can download and install 802.1X authentication clients through a web page.
- It is configured after 802.1X authentication is enabled on the device.
- You must configure redirection parameters. For details, see *Configuring Web-based Authentication*.

Command	**dot1x redirect**
Parameter Description	N/A
Defaults	Disabled
Command Mode	Global configuration mode
Usage Guide	You need to configure redirection parameters properly. For details, see *Configuring Web-based Authentication*.

↘ Filtering Non-Ruijie Clients

- (Optional) When enabled, non-Ruijie clients will not be able to authenticate.

- It is configured after enabling 802.1X authentication on the device.

Command	dot1x private-supplicant-only
Parameter Description	N/A
Defaults	Disabled
Command Mode	Global configuration mode
Usage Guide	To configure this feature, the STA must use Ruijie Supplicant software for authentication.

Verification

- Enable second-generation su deployment and open a Web browser to access a specific URL. The client will be automatically redirected to the download page to download the authentication client. The client must pass authentication through the client before being able to access the network.
- If a user goes online after authentication, you can perform the kickoff function on the Ruijie SAM/SMP. The device will then disconnect the user, and the user will not be able to access the network.

Common Errors

- There are multiple authentication clients on the network, but the device is enabled to filter non-Ruijie supplicants, causing authentication failures of some STAs.
- RG-SAM+ or RG-SMP is used, but the device is not configured with SNMP parameters, resulting in disconnection failures.
- The second-generation supplicant upgrade function cannot be used due to incorrect configuration of redirection parameters.

1.4.4 Configuring MAB Authentication

Configuration Effect

- MAB authentication uses the MAC address of a STA as the authentication account, eliminating the need to install a supplicant on the STA. MAB authentication is applicable to dumb terminals, such as network printers.
- Single-MAB authentication is applicable when there is only one dumb STA connected to a port or when only one STA needs to be authenticated. Other STAs can also access the network after this STA is authenticated. For example, if a wireless router is connected to a port, real-time MAB authentication can be configured for the wireless router, and users connected to the wireless router can access the network after authentication.
- Multi-MAB authentication is applicable when there are multiple types of dumb STAs connected to a port. For example, multiple VoIP access devices are deployed in a network call center.
- Multi-MAB authentication can be used with 802.1X authentication, and is applicable to mixed access environments. For example, voice and data flows are transmitted in the voice VLAN and data VLAN respectively, and office personnel need to use PC for data communication and IP phones for voice communication.
- On a WLAN, WLAN-based MAB authentication is supported. If MAB authentication is enabled, the NAS automatically uses the MAC address of a STA on the WLAN as the user name and password to initiate authentication to the authentication server.

Notes

- A port configured with MAB authentication sends an authentication request packet an intervals specified by *tx-period*at intervals. If there is no response after the maximum re-authentication count, the port enters the MAB authentication mode. Ports in MAB authentication mode can learn MAC addresses and use these MAC addresses as accounts for authentication.
- When configuring the username and password of the MAC account on the server, ensure that the format cannot contain separators. For example, if the MAC address of a STA is 00-d0-f8-00-01-02, the account needs to be configured as 00d0f8000102 on the server.
- 802.1X authentication takes precedence over MAB authentication. Therefore, if a STA passes MAB authentication and then uses the client software to perform 802.1X authentication, the MAB authentication entry will be deleted.
- MAB authentication only supports PAP, so the server needs to be correctly configured.
- MAB authentication mainly proactively discovers whether a STA can perform 802.1X authentication, , so proactive authentication must be enabled during MAB authentication deployment.
- If MAB authentication is enabled on a WLAN, set the WLAN security mode to OPEN.

Configuration Steps

Configuring Single-MAB Authentication

- Optional.
- It applies to scenarios where only one STA needs to be authenticated on a port.
- It is configured on the 802.1X controlled port of the device.

Command	**dot1x mac-auth-bypass**
Parameter Description	N/A
Defaults	Disabled
Command Mode	Interface configuration mode
Usage Guide	To limit the number of STAs, configure MAB violation.

Configuring the Timeout Interval for MAB Authentication

- Optional.
- For the STA whose MAC address is authenticated goes online in MAB authentication mode, the device considers that the STA remains online unless there is a re-authentication failure, port Down event, or logout due to a management policy (for example, forcible disconnection by an administrator). You can configure the online time allowed for these authenticated addresses, with a default value of 0, which means no time limit.
- It is configured on the 802.1X controlled port of the device.

Command	**dot1x mac-auth-bypass timeout-activity** *value*
Parameter Description	*value*: Indicates the MAB authentication online time, in seconds. It is 0 by default, indicating that the online time is not limited.

Defaults	The value is 0 by default, indicating that the online time is not limited.
Command Mode	Interface configuration mode
Usage Guide	It is applicable to both single-MAB and multi-MAB authentication scenarios.

Configuring MAB Violation

- Optional.
- It is configured on the 802.1X controlled port of the device.
- By default, after one MAC address passes MAB authentication, data from all devices on the port is allowed to be forwarded. However, in some security applications, an administrator may require only one MAC address on a port enabled with MAB authentication. In this case, MAB violation can be configured on the port. When the port enters the MAB authentication mode, a violation will be triggered if more than one MAC address is detected on the port.

Command	**dot1x mac-auth-bypass violation**
Parameter Description	N/A
Defaults	Disabled
Command Mode	Interface configuration mode
Usage Guide	• This command can only be configured when it is required to limit the number of dumb STAs under a port to only one. • It applies to the single-MAB authentication scenario only.

Configuring Multi-MAB Authentication

- Optional.
- It is configured on the 802.1X controlled port of the device.

Command	**dot1x mac-auth-bypass multi-user**
Parameter Description	N/A
Defaults	Disabled
Command Mode	Interface configuration mode
Usage Guide	Use this command when multiple dumb STAs on a port need to be authenticated.

Configuring the Quiet Period After a Multi-MAB Authentication Failure

- Optional.
- It is configured after multi-MAB authentication is enabled on the device.
- When multi-MAB authentication is enabled, to prevent unauthorized users connected to the port from attacking the device, disable frequent authentication attempts by unauthorized users to reduce the load on the server. The quiet period for multi-MAB authentication users is configured globally, with the default value of 30s. That is, if a STA's MAC address fails to be authenticated, the STA needs to wait for 30s before initiating authentication again. The quiet period

can be configured according to the environment. If the value is configured as 0, the STA can immediately attempt authentication again after an authentication failure.

Command	**dot1x multi-mab quiet-period** *value*
Parameter Description	*value*: Indicates the quiet period after an authentication failure.
Defaults	It is 30s by default.
Command Mode	Global configuration mode
Usage Guide	You can configure this command to limit the authentication frequency when many dumb STAs connected to a port need to be authenticated.

Configuring a VLAN for MAB Authentication.

- Optional.
- It is configured after enabling multi-MAB authentication is enabled on the device.
- To allow only users within certain VLANs on the interface to perform MAB authentication, configure the VLANs as VLANs for MAB authentication. Then STAs not in the VLANs cannot perform MAB authentication.

Command	**dot1x mac-auth-bypass vlan** *vlan-list*
Parameter Description	*vlan-list*: Indicates the VLANs allowed for MAB authentication.
Defaults	Disabled
Command Mode	Interface configuration mode
Usage Guide	Use this command when only users within specific VLANs on the port are allowed to perform MAB authentication.

Enabling WLAN-based MAB Authentication

- Optional.
- Enable MAB authentication on the WLAN connected to STAs.

Command	**dot1x-mab**
Parameter Description	N/A
Defaults	WLAN-based MAB authentication 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.

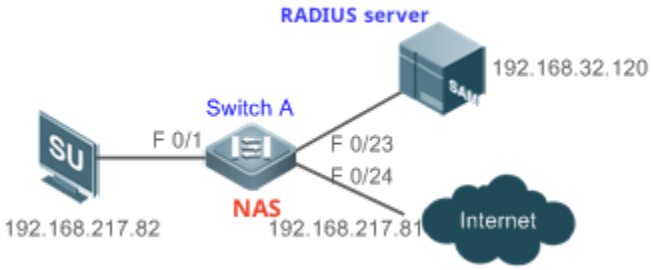
Verification

- Check whether a dumb STA can access the network. If so, MAB authentication takes effect. If not, MAB authentication does not take effect.
- Check whether MAB authentication is configured on the authentication server and NAS.

- Check whether dumb STAs with invalid MAC addresses cannot access the network.
- Check whether dumb STAs with invalid MAC addresses can access the network.

Configuration Example

Configuring Wired Multi-MAB Authentication

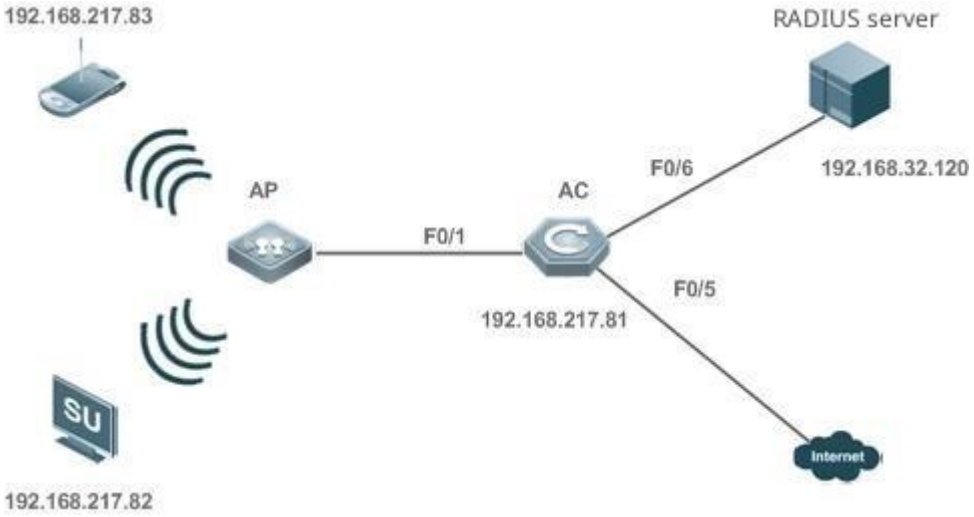
Scenario **Figure 1-5**	
Configuration Steps	● Register the IP address of the device on the RADIUS server and configure the key for the device to communicate with the server. ● Create an account on the RADIUS server. ● Enable AAA on the device. ● Configure RADIUS parameters on the device. ● Enable 802.1X authentication and multi-MAB authentication on device ports. ● The following shows the device configuration. For details about the server configuration, see the server configuration guide.

	`Hostname# configure terminal`
	`Hostname(config)# aaa new-model`
	`Hostname(config)# radius-server host 192.168.32.120`
	`Hostname(config)# radius-server key Hostname`
	`Hostname(config)# interface FastEthernet 0/1`
	`Hostname(config-if)# dot1x port-control auto`
	`Hostname(config-if)# dot1x mac-auth-bypass multi-user`

Verification	Check whether authentication can be performed normally and whether network access behavior changes after authentication.
	● Create an account on the server. For example, the value of username is 0023aeaa4286 and the value of password is **0023aeaa4286**.
	● A non-authenticated STA fails to ping 192.168.32.120.
	● The STA connects to the device, a page indicating the authentication succeeds is displayed, and the STA can successfully ping 192.168.32.120.
	● Check the information about authenticated users.
	`Hostname# show dot1x summary`
	`ID Username MAC Interface VLAN Auth-State`
	`Backend-State Port-Status User-Type Time`
	`--- --- --- --- --- --- -`
	`--- --- --- ---`

	16778217 0023aea... 0023.aeaa.4286 Fa0/1 2 Authenticated Idle Authed static 0days 0h 5m 8s

Enabling WLAN-based MAB Authentication

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 *Configuring RADIUS*.
	Hostname# configure terminal Hostname(config)# aaa new-model Hostname(config)# radius-server host 192.168.32.120 Hostname(config)# radius-server key radius-key Hostname(config)#wlansec 1 Hostname(config-wlansec)#dot1x-mab
Verification	Check whether authentication is normal and whether network access behaviors change after authentication. ● The account is successfully created. For example, the value of username is 0023aeaa4286 and the value of password is **0023aeaa4286**. ● The user fails to ping 192.168.32.120 before authentication. ● The user connects to the NAS, the authentication succeeds, and the user can successfully ping 192.168.32.120. ● Information about the authenticated user is displayed. Hostname# show dot1x summary ID Username MAC Interface VLAN Auth-State Backend-State Port-Status User-Type Time

```
--------- ---------- --------------  --------- ---- --------------- -
------------ ----------- --------- ------------------
16778217  0023aea...  0023.aeaa.4286  Fa0/1    2    Authenticated
Idle          Authed      static    0days 0h 5m 8s
```

Common Errors

The MAC account format is incorrect on the authentication server.

1.4.5 Configuring EAP Termination

Configuration Effect

Configure the device to terminate EAP packets and act a proxy to forward simple authentication information carried in the EAP protocol to the external server. In this case, the device can adapt to external authentication servers that cannot provide the required EAP method.

Configuration Steps

Enabling EAP Termination

- Mandatory.
- Only two types of termination are supported. You can configure either one or both of them.

Related Commands

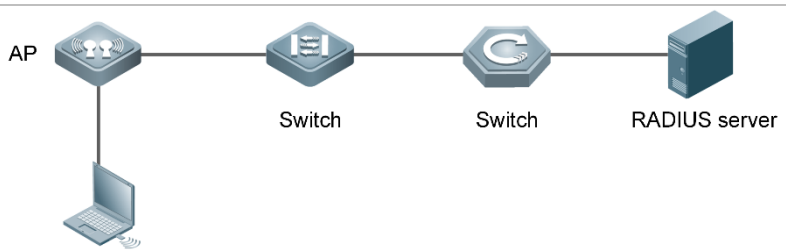
Enabling EAP Termination

Command	**dot1x eap-terminate peap inner-methods** { **gtc** | **mschapv2** }
Parameter Description	**gtc**: Sets the termination type to EAP-GTC termination. **mschapv2**: Sets the termination type to EAP-MSCHAPv2 termination.
Command Mode	WLAN security configuration mode
Usage Guide	• When GTC termination is enabled, the authentication mode of the device is changed from EAP-GTC to PAP authentication, and the device sends a PAP authentication request to the external authentication server. • When MSCHAPv2 termination is enabled, the device encapsulates the challenge and peer response obtained from the PEAP-MSCHAPv2 protocol into one MSCHAPv2 authentication packet and sends the packet to the external authentication server. • EAP termination of 802.1X authentication supports VAC scenarios. • When EAP termination of 802.1X authentication and local EAP termination are enabled simultaneously, traffic continues to be processed by local EAP termination after being terminated by EAP termination of 802.1X authentication, though it is determined that termination is not required. • You are advised to use EAP termination of 802.1X authentication when EAP termination needs to be configured.

Configuration Examples

The following configuration example only describes configuration related to EAP termination.

Enabling EAP-GTC Termination

Scenario **Figure 1-116**	
Configuration Steps	• Configure a WLAN. • Configure 802.1X authentication mode to ensure wireless network security. • Configure the 802.1X authentication method list. • Configure a RADIUS server. • Enable EAP termination of 802.1X authentication.

Switch	# Assign the downlink ports of the switch to VLAN 100 to which the AP belongs.
	`Hostname# configure terminal`
	`Hostname(config)# interface GigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# poe enable`
	`Hostname(config-if-GigabitEthernet 0/1)# switchport access vlan 100`
	# Configure the uplink ports of the switch as trunk ports.
	`Hostname(config)# exit`
	`Hostname(config)# interface GigabitEthernet 0/2`
	`Hostname(config-if-GigabitEthernet 0/2)# switchport mode trunk`

AC	# Configure GigabitEthernet 0/1 connected to the switch as a trunk port.
	`Hostname# configure terminal`
	`Hostname(config)# interface GigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk`
	# Configure the IP address of Loopback 0 for the AC to establish a CAPWAP tunnel with the AP.
	`Hostname(config-if-GigabitEthernet 0/1)# exit`
	`Hostname(config)# interface Loopback 0`
	`Hostname(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255`
	# Configure AP VLAN 100 and STA VLAN 10, and configure the AC as the DHCP server for VLAN 100 and VLAN 10.
	`Hostname(config)#vlan 100`
	`Hostname(config-vlan)#exit`
	`Hostname(config)#interface vlan 100`
	`Hostname(config-if-VLAN 100)# ip address 192.168.100.1 255.255.255.0`
	`Hostname(config)#vlan 10`
	`Hostname(config-vlan)#exit`
	`Hostname(config)#interface vlan 10`
	`Hostname(config-if-VLAN 100)# ip address 192.168.10.1 255.255.255.0`
	`Hostname(config-if-VLAN 100)# exit`

	Hostname(config)# service dhcp Hostname(config)# ip dhcp pool ap_vlan100 Hostname(dhcp-config)# option 138 ip 10.1.1.1 # here must be the IP address of loopback 0. Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.100.10 192.168.100.100 Hostname(dhcp-config)# default-router 192.168.100.1 Hostname(dhcp-config)# exit Hostname(config)# ip dhcp pool sta_vlan10 Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.10.10 192.168.10.100 Hostname(dhcp-config)# default-router 192.168.10.1 Hostname(dhcp-config)# exit # Configure a WLAN. Hostname(config)#wlan-config 1 miaosf_eap Hostname(config-wlan)#exit Hostname(config)#ap-group default Hostname(config-ap-group)#interface-mapping 1 10 Hostname(config-ap-group)# exit # Configure 802.1X authentication mode to ensure wireless network security. 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 Configure the 802.1X authentication method list and authentication termination for AAA. Hostname(config)#wlansec 1 Hostname(config-wlansec)# dot1x authentication default Hostname(config-wlansec)# dot1x eap-terminate peap inner-methods gtc Hostname(config-wlansec)#dot1x eap-terminate peap inner-methods mschapv2 Hostname(config)# aaa new-model Hostname(config)# aaa authentication login default none Hostname(config)# aaa authentication dot1x default group radius # Configure the RADIUS server. Hostname(config)# radius-server host 192.168.197.79 Hostname(config)# radius-server key ruijie
Verification	If both username and password configured on the RADIUS server are **admin**, enter the username and password on the STA (such as a mobile phone). The STA can access WLAN **miaosf_eap**.

Common Errors

The 802.1X authentication method list is incorrectly configured.

1.4.6 Configuring PKI Information

Configuration Effect

The device can generate self-signed PKI information, or users can import PKI information in PKCS#12 format through the CLI.

Configuration Steps

Regenerating the Self-signed PKI Information

- Optional.
- When no PKI information exists on the device, the device automatically generates the self-signed PKI information. Typically, users do not need to generate PKI information through the CLI. For security reasons, users can regenerate the self-signed PKI information by using this function.

Importing PKI Information in PKCS#12 Format

- Optional.
- When the self-signed PKI information generated by the device does not meet user requirements, users can import the required PKI information to the device using a file in PKCS#12 format (file name extension is pfx or p12).
- Note that importing a certificate will cause the client that is being authenticated to fail the authentication.

Verification

- Run the **show dot1x pki** [**self-signed | pfx** command to display PKI information.

Related Commands

Regenerating the Self-signed PKI Information

Command	**dot1x pki-manage generate self-signed**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	● When no PKI information exists on the device, the device automatically generates the self-signed PKI information. Typically, users do not need to generate PKI information through the CLI. For security reasons, users can regenerate the self-signed PKI information by using this function. ● The generated PKI information is stored in the flash memory and loaded from the flash memory during system startup. This command is not saved in the configuration file.

Importing PKI Information in PKCS#12 Format

Command	**dot1x pki-manage import pfx** *filepath* [**password** *password*]
Parameter Description	*filepath:* Indicates the path of the PKCS#12 file in the flash memory. *password:* Indicates the password for decrypting the imported file (optional). If the file is not encrypted, no password needs to be input.
Command Mode	Global configuration mode

Usage Guide	● When the self-signed PKI information generated by the device does not meet user requirements, users can import the required PKI information to the device using a file in PKCS#12 format (file name extension is pfx or p12). The imported information is stored in the flash memory, and loaded from the flash memory during system startup. This command is not saved in the configuration file. ● The PKI information imported by users takes precedence over the PKI information generated by the device. When both the self-signed PKI information generated by the device and the PKI information imported by a user exist, the device will use the PKI information imported by the user. When the device finds that the preceding two types of PKI information do not exist upon startup, the device will automatically generate and use the self-signed PKI information.

Configuration Examples

↘ Uploading the PKCS#12 File to the Device and Importing PKI Information in PKCS#12 Format

Configuration Steps	● Upload the PKCS#12 file to the device. ● Import PKI information in PKCS#12 format.

	# Upload the PKCS#12 file to the device.
	`Hostname# copy tftp://192.168.1.1/pki.pfx flash:pki.pfx`
	Import PKI information in PKCS#12 format.
	`Hostname# config terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#dot1x pki-manage import pfx pki.pfx password filepassword`
	`Import PKI from file [pki.pfx] successfully`

Verification	● Run the **show dot1x pki** [**self-signed | pfx** command to display PKI information.

1.4.7 Configuring Extended Functions

Configuration Effect

- Some STAs use built-in authentication clients in their operating systems, which may not initiate authentication immediately upon network access. Proactive authentication allows STAs to initiate authentication immediately after network access.
- Proactive authentication indicates that STAs proactively sends request/id packets, which can trigger Ruijie Supplicant to perform 802.1X authentication. This function can be used to detect whether STAs are using Ruijie Supplicant. For example, Ruijie Supplicant is required if MAB authentication is deployed.
- The authenticated host list can restrict authentication of STAs connected to an access port, thereby improving network security by controlling physical locations of STAs.
- The multi-account function allows a user to switch its account upon re-authentication. In special scenarios such as Windows domain authentication, authentication needs to be performed for multiple times to access the domain and the user account changes during authentication.
- By default, the device uses its own MAC address as the source MAC address for EAP packets during 802.1X authentication. In some versions of Ruijie Supplicant, the source MAC address of EAP packets is used to determine whether the access device is a Ruijie device and to implement proprietary features. If you need to use these

proprietary features during 802.1X authentication with Ruijie Supplicant of such verisons, you can enable the virtual source MAC address function.

- 802.1X allows users to obtain IP addresses before accounting, meeting the requirement that an IP address is carried during user accounting. 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 the 802.1X server initiates an accounting request. The NAS does not initiate accounting if it does not obtain the IP address of the authentication client. To avoid this situation, configure the IP detection timeout interval. If the NAS does not obtain the IP address of the user within the configured timeout interval (5 minutes by default), it disconnects the user.
- 802.1X allows users to switch to the preset bypass WLAN when the RADIUS server is inaccessible. The bypass WLAN typically uses the OPEN mode and services of the bypass WLAN are unavailable by default. If 802.1X-based WLAN services are unavailable, enable the bypass 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-based authentication. If web-based authentication is enabled on an 802.1X-enabled WLAN, performing 802.1X authentication can achieve only encryption. To access the network, users need to pass web-based authentication. In this case, user data on the air interface is encrypted, enhancing security.
- 802.1X provides notifications about user login and logout logs. You can adjust the rate for generating user login and logout logs based on the user authentication rate. This prevents high CPU utilization due to frequent log generation for a large number of users that go online or 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 traffic of an authenticated user is lower than the configured threshold within the specified period, the user will be disconnected 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 that has a supplicant installed. By doing this, the device can send information about the STA to the authentication server. To prevent a wired device's failure to obtain information of the STA 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.
- Proactive authentication is required during MAB authentication, so proactive authentication must be enabled in the environment where MAB is deployed.
- 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 queried easily. Moreover, when the WLAN needs to be switched due to server inaccessibility, users can manually switch the SSID once. Because the supplicant can retain the SSID record, the SSID can be switched automatically.
- Encryption is used for 802.1X users only, authorization such as ACL assignment and rate limit assignment, is ineffective for 802.1X users. However, users need to pass web-based authentication and be authorized to access the network.

Configuration Steps

Configuring Proactive Authentication

- (Optional) The controlled port sends a proactive authentication request packet. The authentication client initiates 802.1X authentication after receiving the authentication request packet.
- Configure this function after enabling 802.1X authentication.

Command	**dot1x auto-req**
Parameter Description	N/A
Defaults	This function is enabled by default.
Command Mode	Global configuration mode
Usage Guide	The destination IP address of proactive authentication packets is a multicast address. The downlink client may not initiate an authentication proactively. In this case, you can use this command to configure the device to initiate authentication. If the controlled port is a trunk port, the device configured with this command will send an authentication request based on each VLAN on the trunk port.

Configuring the Maximum Number of Proactive Authentication Request Packets

- (Optional) Configure the maximum number of proactive authentication request packets.
- Configure this function after enabling 802.1X authentication.

Command	**dot1x auto-req packet-num** *num*
Parameter Description	*num*: Configures the maximum number of proactive authentication request packets.
Defaults	The value is not configured by default.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the maximum number of proactive authentication request packets.

Configuring User Detection for Proactive Authentication

- (Optional) Configure the controlled port not to send a proactive authentication request packet if there are authentication users on the port.
- Configure this function after enabling 802.1X authentication.

Command	**dot1x auto-req user-detect**

Parameter Description	N/A
Defaults	User detection for proactive authentication is enabled by default.
Command Mode	Global configuration mode
Usage Guide	If the controlled port is an access port, it will not send proactive authentication request packets if there are authentication users on the port. If the controlled port is a trunk port, it will not send proactive authentication request packets from the VLAN to which authentication users belong.

Configuring the Interval for the Device to Send Proactive Authentication Request Packets

- (Optional) Configure the interval for the device to send proactive authentication request packets.
- Configure this function after enabling 802.1X authentication.

Command	**dot1x auto-req req-interval** *time*
Parameter Description	*time*: Configures the interval for the device to send proactive authentication request packets.
Defaults	The value is 30 seconds by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Allowed Host List

- (Optional) Configure the allowed host list on the controlled port. Only hosts in the list are allowed for 802.1X authentication.
- Configure this function after enabling 802.1X authentication.

Command	**dot1x auth-address-table address** *mac-addr* **interface** *interface*
Parameter Description	*mac-addr*: Configures the MAC address of the host. *interface*: Configures the interface of the host.
Defaults	All hosts are allowed for authentication by default.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure the allowed host list on the controlled port.

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 based on 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, for example, in the case of Windows domain authentication. In this case, the authentication client can directly use a new account to initiate authentication while the previous account is still online. Multi-account authentication is disabled by default.

Configuring the Maximum Number of Authenticated Users on a Port

- (Optional) You can restrict the number of online users on a controlled port, including static and dynamic users.
- Configure the maximum number of authenticated users on a port after 802.1X authentication is enabled on the NAS.

Command	**dot1x default-user-limit** *num*
Parameter Description	*num*: Indicates the maximum number of online users.
Defaults	The number of online users is not limited on a port by default.
Command Mode	Interface configuration mode and VXLAN mode
Usage Guide	Configure this command when the number of authenticated users needs to be limited on a port.

Enabling IP Address-triggered Accounting

- (Optional) If IP address-triggered accounting is enabled, the NAS sends an accounting request to the authentication server after obtaining the IP address of the user.
- Enable IP address -triggered accounting after 802.1X authentication is enabled on the NAS.

Command	**dot1x valid-ip-acct enable**
Parameter Description	N/A
Defaults	IP address-triggered accounting is disabled by default.
Command Mode	Global configuration mode

Usage Guide	If both accounting and IP address-triggered accounting are enabled, the NAS initiates accounting only after obtaining the IP address of the authentication client, and disconnects the user if it fails to obtain the IP address. If accounting is disabled but IP address-triggered accounting is enabled, the NAS does not initiate accounting after obtaining the IP address of the authentication client, and disconnects the user if it fails to obtain the IP address within the timeout interval.

Configuring the Timeout Interval for Obtaining IP Addresses After Authentication

- (Optional) Configure the timeout interval for obtaining IP addresses if IP address-triggered accounting is enabled.
- Configure the timeout interval for obtaining IP addresses after 802.1X authentication is enabled on the NAS.

Command	**dot1x valid-ip-acct timeout** *time*
Parameter Description	*time:* Indicates the timeout interval for obtaining IP addresses, in minutes.
Defaults	The default value is 5 minutes.
Command Mode	Global configuration mode
Usage Guide	The default value is recommended. Configure this command when there is a need to change the timeout interval for obtaining IP addresses after users pass authentication.

Configuring the Bypass WLAN for the RADIUS Server

- Optional.
- Enable bypass WLAN for the RADIUS server after 802.1X authentication is enabled on the NAS.

Command	**dot1x event server-invalid action bypass-wlan** *wlan_id*
Parameter Description	*wlan_id:* Indicates the bypass WLAN.
Defaults	Bypass WLAN is disabled by default.
Command Mode	Global configuration mode/WLAN security configuration mode
Usage Guide	• This command applies only to wireless devices. • The default setting is recommended. Run this command to configure the bypass WLAN when the server is unreachable.

Hiding the WLAN Signals During RADIUS Authentication Escape

- Optional.
- Hide the WLAN signals during RADIUS authentication escape after the 802.1X authentication is enabled on the device.

Command	**dot1x event server-invalid original-wlan action hide**
Parameter Description	N/A
Defaults	By default, the WLAN signals are disabled during RADIUS authentication escape.
Command Mode	Global configuration mode
Usage Guide	When the RADIUS server is unreachable, this command can be used to hide the WLAN signals.

	This command takes effect only when the WLAN is enabled with client escape upon RADIUS server failures.

Configuring 802.1X Authentication for Encryption Only When 802.1X and Web-based Authentication Are Enabled

- (Optional) If both 802.1X and web-based authentication is enabled, 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	● The default setting is recommended. ● This command applies only to wireless devices.

Limiting the Rate of Generating Login and Logout Logs

- (Optional)
- You can limit the log generation rate for 802.1X users going online or offline.
- Enable the log generation rate limit after 802.1X authentication is enabled on the NAS.

Command	**dot1x logging rate-limit** *value*
Parameter Description	*value:* Indicates the log generation rate per second for 802.1X users going online or offline. Five logs are generated per second by default. The value 0 indicates that the rate is not limited.
Defaults	Five logs are generated per second by default.
Command Mode	Global configuration mode
Usage Guide	● The default value is recommended. If a large number of users frequently go online or offline, reduce the rate. ● This command applies only to wireless devices.

Enabling SNMP Trap During Login and Logout

- (Optional) The **dot1x user-trap enable** command is used to configure the NAS 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 needs to send login or logout traps to the SNMP server. You also need to enable trap on the SNMP server. For details, see *Configuring SNMP*.

Enabling Traffic Detection

- (Optional) If traffic detection is enabled, 802.1X authentication users with traffic lower than the threshold in the detection period will be disconnected to avoid incorrect accounting.
- Enable traffic detection after 802.1X authentication is enabled on the NAS.

Command	**dot1x offline-detect** [**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 enabled.
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 STA logout in a timely manner to prevent incorrect accounting.

Configuring the Default Role of Clients After They Pass the MAB Authentication

- (Optional) Configure the default role of clients after they pass the MAB authentication.

Command	**dot1x mab-default-role** *role-name*
Parameter Description	role-name: Indicates the default role name assigned to the clients after they pass the authentication.
Defaults	No default role is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	This configuration takes effect only in the standalone MAB authentication scenario.

Configuring the Default Role of Clients After They Pass the 802.1X Authentication

- (Optional) Configure the default role of clients after they pass the 802.1X authentication.

Command	**dot1x dot1x-default-role** *role-name*
Parameter Description	*role-name*: Indicates the default role name assigned to the clients after they pass the authentication.
Defaults	No default role is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	After the clients pass the combination of MAB authentication and 802.1X authentication, they are assigned with the same default role as 802.1X authentication.

Configuring the 802.1X Authentication Domain Attribute

- (Optional) It is used to specify an authentication domain for a WLAN.
- It is configured after 802.1X authentication is enabled on the device.

Command	**dot1x domain-name** *domain-name*
Parameter Description	*domain-name*: Specifies the domain name.

Defaults	No domain is configured by default.
Command Mode	WLAN security mode
Usage Guide	During domain name configuration in WLAN security mode, if the username does not include a domain name for authentication, the username will be appended with @ and the configured domain name for authentication. If the username already includes a domain name for authentication, the username will not be appended with @ and the configured domain name for authentication.

Configuring the Device to Filter Logs

- 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 generated 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 filter debugging information of specified users. Avoid too much debugging information, which may affect device performance.

Disabling the Clients to Obtain the IP Address Before They Pass the MAB Authentication

- Optional. This configuration determines whether the clients can obtain the IP address before they pass the MAB authentication.
- Configure this function after enabling the device with the MAB authentication.

Command	**dot1x no-ip-before-mab**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	WLAN security configuration mode
Usage Guide	This command is used to disable the clients to obtain the IP address before they pass the MAB authentication.

Configuring the Web Authentication After the Clients Pass the MAB Authentication

- Optional. This configuration determines whether the clients need to pass the web authentication after the MAB authentication.
- The device needs to be enabled with both MAB authentication mode and web authentication mode. If the pop-up window for authentication is not automatically displayed on some clients, visit the authentication page manually.

Command	**dot1x mab-pass-to-web**
Parameter Description	N/A
Defaults	This configuration is disabled by default.

Command Mode	WLAN security configuration mode
Usage Guide	This configuration is executed if the web authentication is required after the clients pass the MAB authentication.

1.5 Monitoring

Clearing

⚠ Authentication user information can be cleared after 802.1X is disabled.

Command	Description
no do1x port-control auto	Clears 802.1X user information.
clear dot1x user	Clears 802.1X user information.
dot1x default	Restores the default 802.1X configuration.

Displaying

Command	Description
show radius server	Displays the parameters and status of the RADIUS server.
show dot1x	Displays 802.1X status and parameters.
show dot1x auto-req	Displays the proactive authentication status.
show dot1x port-control	Displays information about controlled ports.
show dot1x probe-timer	Displays the status and parameters of host probe.
show dot1x summary	Displays information about authenticated users.
show dot1x max-req	Displays the maximum count of EAP-Request/Challenge packet retransmission.
show dot1x private-supplicant-only	Displays filtering of non-Ruijie supplicants.
show dot1x re-authentication	Displays the -eauthentication status.
show dot1x reauth-max	Displays the maximum count of EAP-Request/Identity packet retransmission.
show dot1x timeout quiet-period	Displays the quiet period after authentication fails.
show dot1x timeout re-authperiod	Displays the re-authentication interval.
show dot1x timeout server-timeout	Displays the timeout interval of the authentication server.
show dot1x timeout supp-timeout	Displays the timeout interval of the supplicant.
show dot1x timeout tx-period	Displays the interval for retransmitting EAP-Request/Identity packets.
show dot1x user mac	Displays user information based on the MAC address.
show dot1x user name	Displays user information based on the user name.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug aaa	Debugs AAA. (For details, see *Configuring AAA*.)
debug radius	Debugs RADIUS. (For details, see *Configuring RADIUS*.)
debug dot1x event	Debugs 802.1X events.
debug dot1x packet	Debugs 802.1X packets.
debug dot1x stm	Debugs 802.1X state machine (STM).
debug dot1x com	Debugs 802.1X internal communication.
debug dot1x error	Debugs 802.1X errors.

1 Configuring Local EAP

1.1 Overview

The Local Extensible Authentication Protocol (EAP) functions as a local authentication service, allowing the device to authenticate clients locally using an EAP authentication protocol, eliminating the need for an external authentication server deployment. For example, the device can authenticate STAs that use 802.1X authentication. The device that provides the local EAP function serves as an EAP server. It can function as the preferred authentication server to provide the authentication service or be used as the backup of the external authentication server to provide the authentication service when the external authentication server is unavailable. Local EAP supports Protected Extensible Authentication Protocol v0 (PEAPv0)/Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) and PEAPv1/Generic Token Card (GTC).

Local EAP also provides the EAP termination function. EAP termination enables the device to terminate EAP packets on itself and to forward EAP packets with simple authentication information to the external server. In this case, the device can be used with an external authentication server that cannot provide the required EAP mode. For example, PEAPv1/GTC is required for client authentication, and the external authentication server can only provide the PAP authentication mode.

Protocols and Standards

- RFC 3748: Extensible Authentication Protocol (EAP)
- RFC 4137: State Machines for Extensible Authentication Protocol (EAP)
- RFC 5216: The EAP-TLS Authentication Protocol
- RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

1.2 Applications

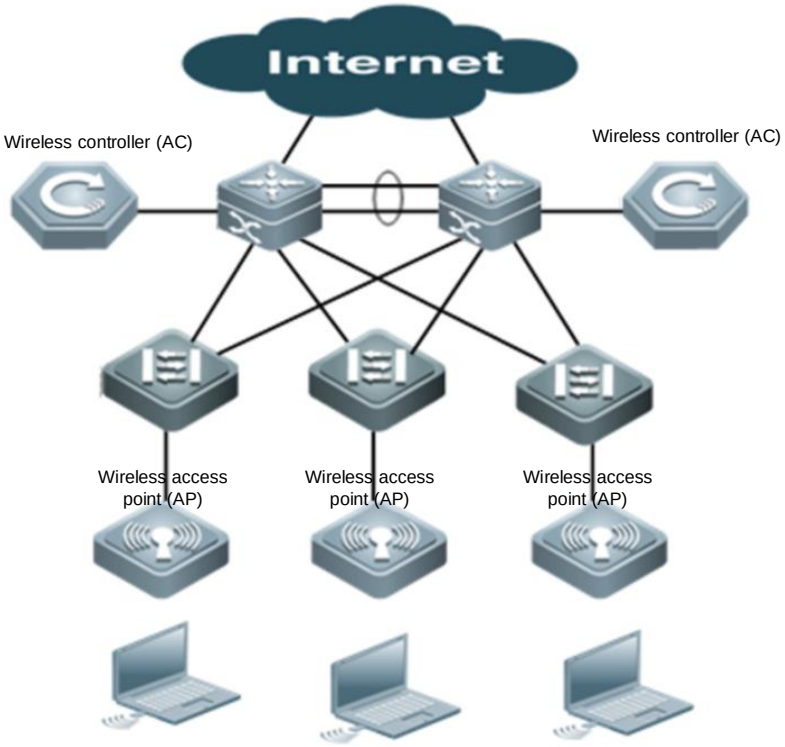
Application	Description
Local Authentication	EAP functions as a local authentication service, allowing the device to authenticate clients locally using an EAP authentication protocol, eliminating the need for an external authentication server deployment.
EAP Termination	EAP termination enables the device to terminate EAP packets on itself and to forward EAP packets with simple authentication information to the external server.

1.2.1 Local Authentication

Scenario

As shown in Figure 1-1, wireless access controllers (ACs) and wireless access points (APs) form a wireless network. The ACs are configured to adopt 802.1X authentication and local authentication of the local EAP service. The AC functions as the authentication server, without deploying an external authentication server.

Figure 1-1



Deployment

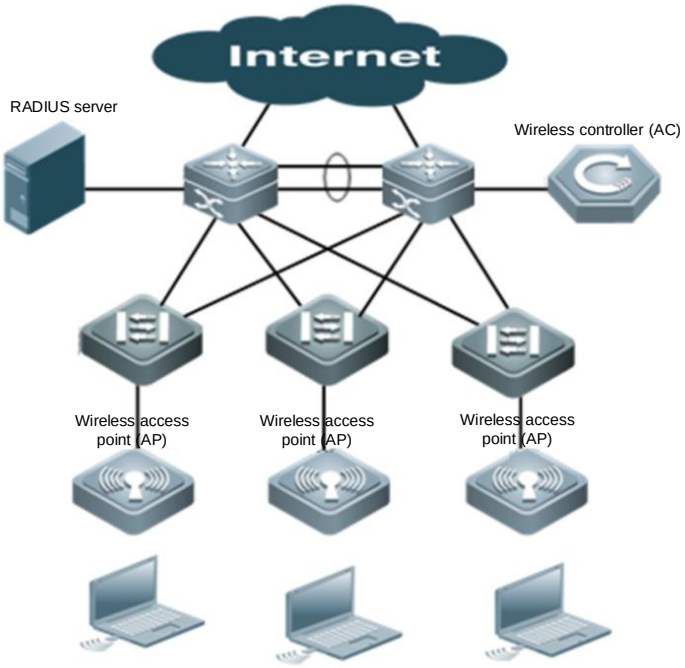
- Configure a wireless local area network (WLAN).
- Configure 802.1X authentication to ensure security of the WLAN.
- Configure the 802.1X authentication method list.
- Configure local EAP and use the account of the local authentication server as the authentication username and password.

1.2.2 EAP Termination

Scenario

As shown in Figure 1-2, ACs and APs form a wireless network, and a RADIUS authentication server is deployed on the network. 802.1X access authentication is configured on ACs. Because the RADIUS authentication server does not support EAP, the EAP termination function of the local EAP service needs to be enabled on the ACs.

Figure 1-2



Deployment

- Configure a WLAN.
- Configure the 802.1X authentication mode to ensure security of the WLAN.
- Configure the 802.1X authentication method list.
- Configure the RADIUS server.
- Enable the EAP termination function of the local EAP service.

1.3 Features

Basic Concepts

EAP

EAP is an authentication framework that defines the basic authentication process and message format, but does not define the specific authentication method. The data exchange process and encapsulation format need to be defined for each authentication protocol based on the EAP framework. Common EAP authentication protocols include EAP-MD5, EAP-GTC, EAP-TLS, EAP-MS-CHAPv2, PEAPv0/MS-CHAPv2, and PEAPv1/GTC. EAP-TLS, EAP-MS-CHAPv2, PEAPv0/MS-CHAPv2, and PEAPv1/GTC are commonly used on wireless networks.

- PEAPv0/MS-CHAPv2

  PEAPv0/MS-CHAPv2 is the most commonly used authentication protocol on wireless networks and supported most systems. It uses outer-layer PEAP to establish a Transport Layer Security (TLS) tunnel to protect authentication information; it uses inner-layer EAP-MS-CHAPv2 to verify users' identities.

- PEAPv1/GTC

PEAPv1/GTC is similar to PEAPv0/MS-CHAPv2 and is supported by most mobile devices. However, Windows OSs do not support the protocol by default. It uses outer-layer PEAP and inner-layer EAP-GTC that is used to verify users' identities.

EAP Termination

An EAP authentication protocol is run between the device enabled with the local EAP service and an authentication client, while another authentication protocol (may be not an EAP protocol) is run between the device enabled with the local EAP service and the external authentication server. The device enabled with the local EAP service functions as the agent to forward authentication packets or results between the client and external authentication server, the EAP termination function enables the device enabled with the local EAP service local EAP service to terminate EAP packets on the device, to extract necessary authentication information, and to forward it to the external authentication server. The device enabled with the local EAP service encapsulates authentication results returned by the external authentication server or authentication information that needs to be transferred to the client into the specified EAP packet, and then forwards it to the authentication client. This function is used when the device interworks with an authentication server that does not support the specified EAP authentication mode. ACs support two types of EAP termination: EAP-GTC termination and EAP-MS-CHAPv2 termination.

- EAP-GTC termination

  When EAP-GTC is run between the device enabled with the local EAP service and a client, the device obtains the username and password submitted by the client through EAP-GTC and uses the username and password to send a PAP authentication request to the external authentication server. The external authentication server determines the authentication result.

- EAP-MS-CHAPv2 termination

  When EAP-MS-CHAPv2 is run between the device enabled with the local EAP service and a client, the device obtains the challenge and peer response through EAP-MSCHAPv2, encapsulates them into an MS-CHAPv2 authentication request, and sends it to the external authentication server. The external authentication server determines the authentication result.

PKI

Some EAP modes supported by the local EAP service require the support of Public Key Infrastructure (PKI). For example, PEAP needs to adopt an asymmetric encryption algorithm to establish a trusted encrypted tunnel, such as a TLS tunnel with the client.

PKI is an identity identification and communication encryption system based on the asymmetric password system, and uses certificates. In PKI, the communication parties use a trusted third party to determine whether the identity of the peer is consistent as stated. The trusted third party is a certificate authority (CA). The identity information in PKI is identified using the X509 certificate. The certificate includes the identity information of the owner, public key of the owner, and signature of the trusted third-party to the information. In addition, certificates are classified into self-signed and CA-issued certificates.

- Self-signed certificates are signed by CAs. A CA uses a private key to sign the identity information and public key to obtain a CA certificate, and the certificate is the ID of the CA. Because the certificate of a CA contains the public key of the CA, the public key can be used to verify certificates issued by the CA. These certificates are signed using the private key of the CA and can be verified using the public key of the CA. When a CA is trusted, a

communication party can use the certificate of the CA to verify the certificate of the peer to ensure that it communicates with the correct entity.

- CA-issued certificates are obtained by using the private key of a CA to sign certificate requests. An entity can send a certificate issuing request to a CA. The request contains the identity and public key of the entity. After the CA uses its private key to sign the request, the certificate required by the entity is obtained. Then the entity can use the certificate to identify its own identity. If the peer trusts the same CA, the peer can verify the identity of the entity.

In addition to identity verification, the public and private key pairs have the asymmetric encryption and decryption function. Communication parties can use their private keys and public keys of the peer to establish an encrypted communication channel. This tunnel cannot be decrypted by others, so data transmitted in this tunnel is secure and trusted.

EAP-TLS and PEAP depend on PKI. The two protocols will establish a TLS tunnel between the authentication client and authentication server for subsequent identity authentication. To establish the tunnel, use the certificate and public and private keys of the server as well as the CA certificate (optical) for PEAP. If the client chooses not to verify the server certificate, the CA certificate is not required. To establish the tunnel, EAP-TLS needs the certificates and public and private keys of the server and client as well as the CA certificate.

Overview

Feature	Description
Local Authentication	The device locally authenticates clients that use an EAP authentication protocol, eliminating the need for an external authentication server deployment. The device can function as the preferred authentication server to provide the authentication service or be used as the backup of the external authentication server to provide the authentication service when the external authentication server is unavailable.
EAP Termination	EAP termination enables the device to terminate EAP packets on itself and to forward EAP packets with simple authentication information to the external server. In this case, the device can be used with an external authentication server that cannot provide the required EAP mode. For example, PEAPv1/GTC is required for client authentication, and the external authentication server can only provide the PAP authentication mode.

1.3.1 Local Authentication

The device locally authenticates clients that use an EAP authentication protocol, eliminating the need for an external authentication server deployment. The device can function as the preferred authentication server to provide the authentication service or be used as the backup of the external authentication server to provide the authentication service when the external authentication server is unavailable.

Working Principle

During local authentication, the working principle of the device enabled with the local EAP service is similar to that of the RADIUS server and can be regarded as an authentication server. When an external RADIUS authentication server is used, EAP authentication requests of authentication clients need to be encapsulated into RADIUS packets before being sent to the RADIUS server. When the device enabled with the local EAP service is used as the authentication server, EAP authentication requests of authentication clients are directly processed by the device.

The device enabled with the local EAP service supports various EAP modes and different internal modes of PEAP. The device will select the mode for authenticating the client based on the sequence in which the modes were configured. During EAP authentication, the EAP mode is determined by the server.

Related Configuration

Configuring the 802.1X Authentication Method List

If the device enabled with the local EAP service is used as the authentication server, the local method needs to be specified in the 802.1X authentication method list.

Run the **aaa authentication dot1x** {**default** | *list-name*} *method1* [*method2*...] command to specify the 802.1X authentication method list, for example, **aaa authentication dot1x default local**.

Authentication request packets of clients are sent to the device enabled with the local EAP service for local authentication only when the local method is specified in the 802.1X authentication method list.

Configuring the Modes Used for Identity Authentication with a Client

Configure the EAP modes of the local EAP service to authenticate identities of clients. By default, only PEAP is supported, and PEAP internal modes of EAP-MS-CHAPv2 and EAP-GTC are supported and in descending order of priroity.

Only PEAP is supported, and cannot be changed. The supported PEAP internal modes and sequence can be changed by running the **peap inner-methods** { **eap-mschapv2** [**eap-gtc**] | **eap-gtc** [**eap-mschapv2**] } command. The mode that was configured first is preferred.

1.3.2 EAP Termination

EAP termination enables the device to terminate EAP packets on itself and to forward EAP packets with simple authentication information to the external server. In this case, the device can be used with an external authentication server that cannot provide the required EAP mode. For example, PEAPv1/GTC is required for client authentication, and the external authentication server can only provide the PAP authentication mode.

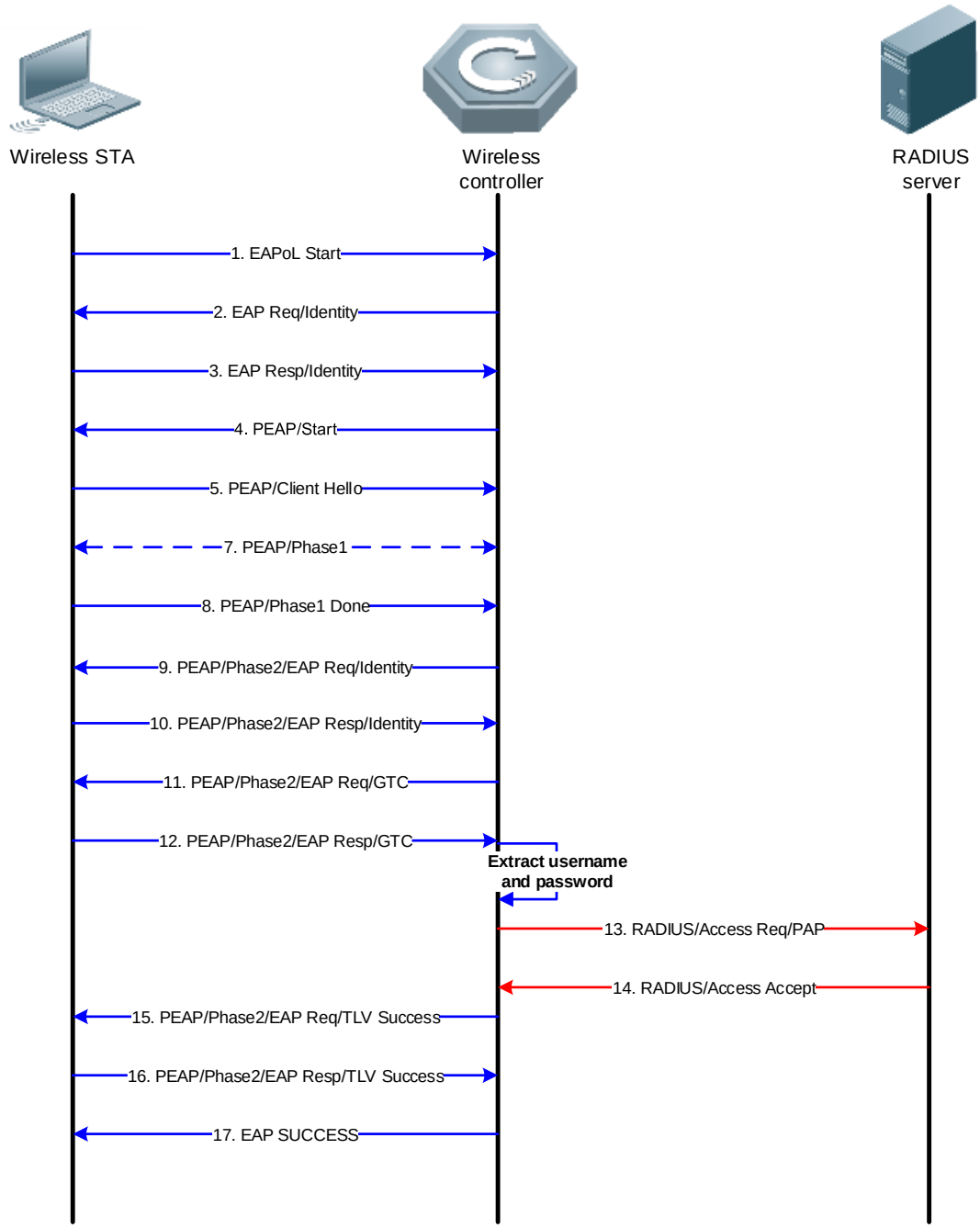
Working Principle

EAP-GTC termination is used as an example to describe the working principle of EAP termination. Figure 1-3 shows the flowchart of EAP-GTC termination. The RADIUS server supports PAP authentication only. However, PEAPv1/GTC is used between the AC and STA.

- Steps 1 to 12: The AC exchanges packets with the STA, which is required by PEAPv1/GTC. After step 12 is performed, the AC obtains the STA's authentication credential, including the username and cleartext password.
- Steps 13 to 14: The local EAP module uses the obtained authentication credential to initiate PAP authentication to the RADIUS server and obtains the result that authentication succeeds.
- Steps 15 to 17: Based on the result returned by the RADIUS server, the local EAP module continues to perform PEAPv1/GTC authentication.

In Figure 1-3, when the AC performs EAP-GTC termination, the STA does not detect the operation and regards that PEAPv1/GTC authentication is performed. However, the RADIUS server regards that the STA is experiencing PAP authentication. The flowcharts of PEAP termination and EAP-MSCHAPv2 are similar.

Figure 1-3



Related Configuration

↘ Configuring the AAA Authentication Method List and the RADIUS Authentication Server

When the EAP termination function is used, the device enabled with the local EAP service serves as the agent and forwards some information to the external server. Therefore, the external authentication server needs to be configured.

Run the **radius-server host** { *ipv4-address* | *ipv6-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] command to specify the external authentication server. Run the **aaa authentication localeap default group** { **radius |**

group-name } command to specify the external authentication server to which the authentication request packets are sent for authentication after termination.

Configuring EAP Termination

EAP termination is not configured by default.

Run the **eap-gtc terminate** command to enable EAP-GTC termination; run the **eap-mschapv2 terminate** command to enable EAP-MS-CHAPV2 termination.

1.4 Configuration

Configuration	Description and Command	
Configuring Local Authentication	(Optional) It is used to configure the device as the authentication server, without deploying an external authentication server or using the device as the backup of the external authentication server.	
	eap-methods { **peap** }	Configures the EAP mode used by the device enabled with the local EAP service to authenticate identities of clients. Only PEAP is supported.
	peap inner-methods { **eap-mschapv2** [**eap-gtc**] | **eap-gtc** [**eap-mschapv2**] }	Configures the PEAP internal mode used by the device enabled with the local EAP service to authenticate the identities of clients. The mode configured first is preferred. At least one mode needs to be selected.
Configuring EAP Termination	(Optional) It is used to configure the device to terminate EAP packets on itself and to forward EAP packets with simple authentication information to the external server. In this case, the device can be used with an external authentication server that cannot provide the required EAP mode.	
	eap-gtc terminate	Configures EAP-GTC termination.
	eap-mschapv2 terminate	Configures EAP-MS-CHAPv2 termination.
Configuring PKI	(Optional) It is used to configure whether the device enabled with the local EAP service uses the self-signed PKI information generated by the device or the PKI information in PKCS#12 format imported by using a command. The self-signed PKI information generated by the device is used by default.	
	pki-manage generate self-signed default	Enables the device to generate the self-signed PKI information when no PKI information exists on the device. In most situations, PKI information does not need to be generated using a command. In special cases (for example, security is required), this command can be used to re-generate the self-signed PKI information.

	pki-manage import pfx *filepath* [**password**]	Imports required PKI information to the device using a file in PKCS#12 format (file name extension is pfx or p12) when the self-signed PKI information generated by the device does not meet user requirements.
	server restart	Restarts the device enabled with the local EAP service for the new PKI information to take effect after the PKI information used by the device is updated.

1.4.1 Configuring Local Authentication

Configuration Effect

- Optional.
- Local authentication is performed for clients that use an EAP authentication protocol, without the need to deploy an external authentication server. The device can serve as the preferred authentication server to provide the authentication service directly or be used as the backup of the external authentication server to provide the authentication service when the external authentication server is unavailable.

Configuration Steps

↘ Configuring the EAP Mode Sequence

- Optional.
- Only PEAP is supported and the default EAP mode is PEAP., so there is no need to configure the EAP mode sequence.

↘ Configuring the PEAP Internal Mode Sequence

- Optional.
- By default, the supported PEAP internal modes are EAP-MSCHAPv2 and EAP-GTC, and EAP-MSCHAPv2 and EAP-GTC are in descending order of priority. Unless otherwise specified, the PEAP internal mode sequence does not need to be configured.

Verification

- Run the **show localeap methods** command to display the authentication mode configuration.

Related Commands

↘ Configuring the EAP Mode Sequence

Command	**eap-methods** { **peap** }
Parameter Description	N/A
Command Mode	Local EAP mode
Usage Guide	This command is used to configure the EAP modes used by the device enabled with the local EAP service for authenticating identities of clients. Only PEAP is supported.

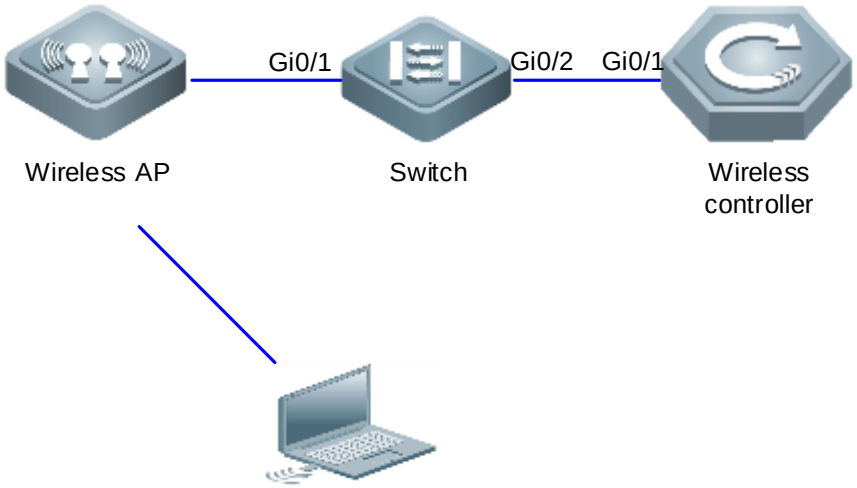
↘ Configuring the PEAP Internal Mode Sequence

Command	**peap inner-methods** { **eap-mschapv2** [**eap-gtc**] | **eap-gtc** [**eap-mschapv2**] }
Parameter Description	N/A
Command Mode	Local EAP mode
Usage Guide	This command is used to configure the PEAP internal modes used by the device enabled with the local EAP service to authenticate identities of clients. The mode configured first is preferred. At least one mode needs to be selected.

Configuration Example

Configuring Local Authentication

As shown in Figure 1-4, the AC and AP form a wireless network. The AC is configured to adopt 802.1X authentication and local authentication of the local EAP service. The AC functions as the authentication server, and no external authentication server needs to be deployed.

Scenario **Figure 1-4**	
Configuration Steps	● Configure a WLAN. ● Configure 802.1X authentication to ensure security of the WLAN. ● Configure the 802.1X authentication method list. ● Configure local EAP function and use the account of the local authentication server as the authentication username and password.

Switch	`# Assign the downlink ports of the switch to VLAN 100 to which the AP belongs.`
	`Hostname# configure terminal`
	`Hostname(config)# interface GigabitEthernet 0/1`
	`Hostname(config-if-GigabitEthernet 0/1)# poe enable`
	`Hostname(config-if-GigabitEthernet 0/1)# switchport access vlan 100`
	`# Configure the uplink ports of the switch as Trunk ports.`
	`Hostname(config)# exit`
	`Hostname(config)# interface GigabitEthernet 0/2`
	`Hostname(config-if-GigabitEthernet 0/2)# switchport mode trunk`

AC	`# Configure GigabitEthernet 0/1 connected with the switch as a Trunk port.` `Hostname# configure terminal`

```
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk
# Configure the IP address of Loopback 0 for the AC to establish a CAPWAP tunnel with the AP.
Hostname(config-if-GigabitEthernet 0/1)# exit
Hostname(config)# interface Loopback 0
Hostname(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255
# Configure AP VLAN 100 and STA VLAN 10, and configure the AC as the DHCP server for VLAN 100 and VLAN 10.
Hostname(config)#vlan 100
Hostname(config-vlan)#exit
Hostname(config)#interface vlan 100
Hostname(config-if-VLAN 100)# ip address 192.168.100.1 255.255.255.0
Hostname(config)#vlan 10
Hostname(config-vlan)#exit
Hostname(config)#interface vlan 10
Hostname(config-if-VLAN 100)# ip address 192.168.10.1 255.255.255.0
Hostname(config-if-VLAN 100)# exit
Hostname(config)# service dhcp
Hostname(config)# ip dhcp pool ap_vlan100
Hostname(dhcp-config)# option 138 ip 10.1.1.1   # Here must be the IP address of Loopback 0.
Hostname(dhcp-config)#  network  192.168.100.0  255.255.255.0  192.168.100.10 192.168.100.100
Hostname(dhcp-config)# default-router 192.168.100.1
Hostname(dhcp-config)# exit
Hostname(config)# ip dhcp pool sta_vlan10
Hostname(dhcp-config)#  network  192.168.100.0  255.255.255.0  192.168.10.10 192.168.10.100
Hostname(dhcp-config)# default-router 192.168.10.1
Hostname(dhcp-config)# exit
# Configure a WLAN.
Hostname(config)#wlan-config 1 miaosf_eap
Hostname(config-wlan)#exit
Hostname(config)#ap-group default
Hostname(config-ap-group)#interface-mapping 1 10
Hostname(config-ap-group)# exit
# Configure the 802.1X access authentication mode to ensure wireless network security.
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
```

	# Configure the 802.1X authentication method list. Hostname(config)# dot1x authentication default Hostname(config)# aaa new-model Hostname(config)# aaa authentication login default none Hostname(config)# aaa authentication dot1x default local Hostname(config)# aaa authentication enable default none # Configure local EAP function and use the account of the local authentication server as the authentication username and password. Hostname(config)# username admin password admin
Verification	Enter the username and password (**admin**) on the STA (such as a mobile phone). The STA can connect to WLAN **miaosf_eap**.

Common Errors

- The 802.1X authentication method list is incorrectly configured.

1.4.2 Configuring EAP Termination

Configuration Effect

- Optional.
- Configure the device to terminate EAP packets on itself and to forward EAP packets with simple authentication information to the external server. In this case, the device can be used with an external authentication server that cannot provide the required EAP mode.

Configuration Steps

↘ Configuring the AAA Authentication Method List and the RADIUS Authentication Server

- Mandatory.
- When EAP termination is used, the device enabled with the local EAP service serves as the agent to forward authentication information to the external authentication server. Therefore, the external authentication server needs to be configured.

↘ Configuring EAP-GTC Termination and EAP-MS-CHAPv2 Termination

- Mandatory.
- Only two types of termination are supported. You can select either one or configure both of them.

Verification

- Run the **show localeap methods** command to display the EAP termination configuration.

Related Commands

↘ Configuring the AAA Authentication Method List and the RADIUS Authentication Server

Command	**radius-server host** { *ipv4-address* | *ipv6-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] **aaa authentication localeap default group** { **radius |** *group-name* }
Parameter	*group-name*: Indicates the name of the server group from which the server is used by the device enabled

Description	with the local EAP service as the external authentication server.
Command Mode	Global configuration mode
Usage Guide	The first command is provided by the RADIUS module, and the second command is provided by the AAA module.

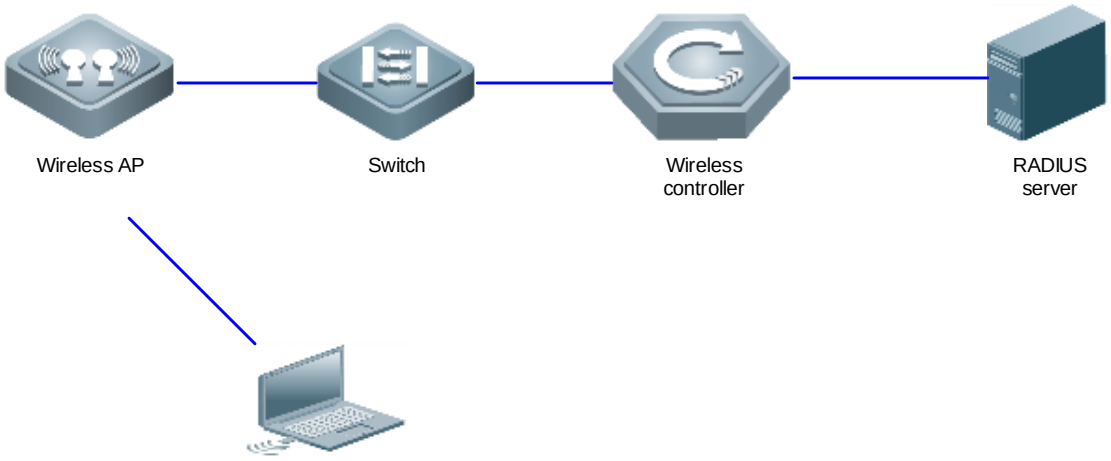
Configuring EAP-GTC Termination and EAP-MS-CHAPv2 Termination

Command	**eap-gtc terminate** **eap-mschapv2 terminate**
Parameter Description	**N/A**
Command Mode	Local EAP mode
Usage Guide	The commands are used to enable EAP-GTC termination and EAP-MSCHAPv2 termination.

Configuration Example

Configuring EAP Termination

As shown in Figure 1-5, the AC and AP form a wireless network, and the AC connects to the RADIUS authentication server. 802.1X authentication is configured on the AC. The STA adopts PEAPv1/GTC. Because the RADIUS authentication server does not support PEAPv1/GTC termination, EAP-GTC termination needs to be configured on the AC.

Scenario **Figure 1-5**	
Configuration Steps	● Configure a WLAN. ● Configure 802.1X authentication to ensure security of the WLAN. ● Configure the 802.1X authentication method list. ● Configure the RADIUS authentication server. ● Enable the EAP termination function on the device enabled with the local EAP service.
Switch	`# Assign the downlink ports of the switch to VLAN 100 to which the AP belongs.`

	Hostname# configure terminal Hostname(config)# interface GigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# poe enable Hostname(config-if-GigabitEthernet 0/1)# switchport access vlan 100 # Configure the uplink ports of the switch as Trunk ports. Hostname(config)# exit Hostname(config)# interface GigabitEthernet 0/2 Hostname(config-if-GigabitEthernet 0/2)# switchport mode trunk
AC	# Configure GigabitEthernet 0/1 connected with the switch as a Trunk port. Hostname# configure terminal Hostname(config)# interface GigabitEthernet 0/1 Hostname(config-if-GigabitEthernet 0/1)# switchport mode trunk # Configure the IP address of Loopback 0 for the AC to establish a CAPWAP tunnel with the AP. Hostname(config-if-GigabitEthernet 0/1)# exit Hostname(config)# interface Loopback 0 Hostname(config-if-Loopback 0)# ip address 10.1.1.1 255.255.255.255 # Configure AP VLAN 100 and STA VLAN 10, and configure the AC as the DHCP server for VLAN 100 and VLAN 10. Hostname(config)#vlan 100 Hostname(config-vlan)#exit Hostname(config)#interface vlan 100 Hostname(config-if-VLAN 100)# ip address 192.168.100.1 255.255.255.0 Hostname(config)#vlan 10 Hostname(config-vlan)#exit Hostname(config)#interface vlan 10 Hostname(config-if-VLAN 100)# ip address 192.168.10.1 255.255.255.0 Hostname(config-if-VLAN 100)# exit Hostname(config)# service dhcp Hostname(config)# ip dhcp pool ap_vlan100 Hostname(dhcp-config)# option 138 ip 10.1.1.1 # Here must be the IP address of Loopback 0. Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.100.10 192.168.100.100 Hostname(dhcp-config)# default-router 192.168.100.1 Hostname(dhcp-config)# exit Hostname(config)# ip dhcp pool sta_vlan10 Hostname(dhcp-config)# network 192.168.100.0 255.255.255.0 192.168.10.10 192.168.10.100 Hostname(dhcp-config)# default-router 192.168.10.1 Hostname(dhcp-config)# exit # Configure a WLAN. Hostname(config)#wlan-config 1 miaosf_eap Hostname(config-wlan)#exit

	Hostname(config)#ap-group default Hostname(config-ap-group)#interface-mapping 1 10 Hostname(config-ap-group)# exit # Configure the 802.1X access authentication mode to ensure wireless network security. 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 # Configure the 802.1X authentication method list. Hostname(config)# dot1x authentication default Hostname(config)# aaa new-model Hostname(config)# aaa authentication login default none Hostname(config)# aaa authentication dot1x default local Hostname(config)# aaa authentication enable default none Hostname(config)# aaa authentication localeap default group radius # Configure the RADIUS server. Hostname(config)# radius-server host 192.168.197.79 Hostname(config)# radius-server key Hostname
Verification	If the username and password configured on the RADIUS server are **admin**, enter the username and password on the STA (such as a mobile phone). The STA can connect to WLAN **miaosf_eap**.

Common Errors

- The 802.1X authentication method list is incorrectly configured.

1.4.3 Configuring PKI

Configuration Effect

- Optional.
- The device enabled with the local EAP service can use the self-signed PKI information generated by the device or the PKI information in PKCS#12 format imported by using a command. The self-signed PKI information generated by the device is used by default.
- The PKI information imported by using a command is prior to the PKI information generated by the device. When both the self-signed PKI information generated by the device and the imported PKI information exist, the device will use the imported PKI information. When the device finds that the preceding two types of PKI information do not exist upon startup, the device will automatically generate self-signed PKI information and use it.

Configuration Steps

↘ Configuring the Device to Re-generate the Self-signed PKI Information

- Optional.

- When no PKI information existson the device, the device automatically generates the self-signed PKI information. Typically, PKI information does not need to be generated using a command. In specified scenarios (for example, security is required), the device can be configured to re-generate the self-signed PKI information.

Importing PKI Information in PKCS#12 Format

- Optional.
- When the self-signed PKI information generated by the device does not meet user requirements, you can import the required PKI information to the device using a file in PKCS#12 format (file name extension is pfx or p12).

Restarting the Device Enabled with the Local EAP Service for New PKI Information to Take Effect

- Optional.
- After the PKI information used by the device enabled with the local EAP service is updated, the device needs to be restarted for the new PKI information to take effect in the following scenarios:
  - The self-signed PKI information is being used. However, the self-signed PKI information is re-generated, or PKI information is imported externally.
  - The PKI information imported externally is being used. However, the externally imported PKI information is deleted, or new PKI information is re-imported.
- Note: After the device enabled with the local EAP service is restarted, all STAs that go online after being authenticated by the local EAP service will go offline.

Verification

- Run the **show localeap pki** [**self-signed | pfx** command to display PKI information on the device enabled with the local EAP service.

Related Commands

Re-generating the Self-signed PKI Information

Command	**pki-manage generate self-signed default**
Parameter Description	**N/A**
Command Mode	Local EAP configuration mode
Usage Guide	When no PKI information exists on the device, the device automatically generates the self-signed PKI information. Typically, PKI information does not need to be generated using a command. In specified scenarios (for example, security is required), the device can be configured to re-generate the self-signed PKI information. After the self-signed PKI information is re-generated, the device enabled with the local EAP service needs to be restarted for the PKI information to take effect.

Importing PKI Information in PKCS#12 Format

Command	**pki-manage import pfx** *filepath* [**password** *password*]
Parameter Description	*filepath*: Indicates the path for restoring the file in PKCS#12 format in the flash memory. *password*: Indicates the password for decrypting the imported file. If the file is not encrypted, no

	password needs to be entered.
Command Mode	Local EAP mode
Usage Guide	When the self-signed PKI information generated by the device does not meet user requirements, you can import the required PKI information to the device using a file in PKCS#12 format (file name extension is pfx or p12). After the PKI information is imported or the imported PKI information is deleted, the device enabled with the local EAP service needs to be restarted for the PKI information to take effect.

Restarting the Device Enabled with the Local EAP Service for New PKI Information to Take Effect

Command	**service restart**
Parameter Description	**N/A**
Command Mode	Local EAP mode
Usage Guide	After the PKI information used by the local EAP service is updated, the device enabled with the local EAP service needs to be restarted for the new PKI information to take effect in the following scenarios: ■ The self-signed PKI information is being used. However, the self-signed PKI information is re-generated, or PKI information is imported externally. ■ The PKI information imported externally is being used. However, the externally imported PKI information is deleted, or new PKI information is re-imported. After the device enabled with the local EAP service is restarted, all STAs that go online after being authenticated by the local EAP service will go offline.

Configuration Example

Uploading the PKCS#12 File to the Device and Configuring the Device Enabled with the Local EAP Service to Import PKI Information in PKCS#12 Format

Configuration Steps	● Upload the PKCS#12 file to the device. ● Configure the device enabled with the local EAP service to import PKI information in PKCS#12 format.

	`# Upload the PKCS#12 file to the device.`
	`Hostname# copy tftp://192.168.1.1/pki.pfx flash:pki.pfx`
	`# Configure the local EAP service to import PKI information in PKCS#12 format.`
	`Hostname# config`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)#localeap`
	`Hostname(config-localeap)#pki-manage import pfx pki.pfx password filepassword`
	`Apr 29 23:03:27: %LOCALEAP-6-PKIMANAGE: Import PKI from file [pki.pfx] successfully`

Verification	● Run the **show localeap pki** [**self-signed | pfx** command to display PKI information on the device enabled with the local EAP service.

Configuration Steps	● Upload the PKCS#12 file to the device. ● Configure the device enabled with the local EAP service to import PKI information in PKCS#12 format.

	`# Upload the PKCS#12 file to the device.`
	`Hostname# copy tftp://192.168.1.1/pki.pfx flash:pki.pfx`
	`# Configure the local EAP service to import PKI information in PKCS#12 format.`
	`Hostname# config`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)#localeap`
	`Hostname(config-localeap)#pki-manage import pfx pki.pfx password filepassword`
	`Apr 29 23:03:27: %LOCALEAP-6-PKIMANAGE: Import PKI from file [pki.pfx] successfully`

Verification	● Run the **show localeap pki** [**self-signed | pfx** command to display PKI information on the device enabled with the local EAP service.

	`Hostname#show localeap pki`
	`TYPE ACTIVATED`
	`----------`
	`Self-Signed Yes`
	`* PFX-Imported Yes`

1.5 Monitoring

Displaying

Command	Description
show localeap methods	Displays information related to EAP methods.
show localeap pki [**self-signed | pfx**]	Displays PKI summary information.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug localeap pki	Debugs the device enabled with the local EAP service.
debug localeap user {verbose | error | add mac *mac-address* **| delete mac** *mac-address***}**	Debugs user authentication on the device enabled with the local EAP service.

1 Configuring Web-based Authentication

1.1 Overview

1.1.1 Web-based Authentication

Web-based authentication is a method of identity authentication that regulates user permissions for network access. It effectively manages user network access by employing the use of common web browsers, eliminating the need for dedicated authentication software on clients.

When non-authenticated users attempt to access the Internet using a browser, the network access server (NAS) forcibly redirects them to a specified site, which is a web-based authentication server, also known as a portal server. Users can access services on the portal server without authentication, such as downloading security patches and reading notices. However, if a user wants to access network resources beyond the portal server, the user must be authenticated by the portal server through a browser.

Besides providing convenient authentication, the portal server interacts with browsers by providing personalized services, such as advertisements, notices, and business links on the authentication page.

Web-based Authentication Versions

Ruijie offers three web-based authentication modes: first-generation, second-generation, and built-in portal authentication. The authentication process varies depending on the version being used. For details, see 1.3 Features.

The three web-based authentication modes differ significantly in features and configurations. You are advised to read through relevant chapters carefully before proceeding with the configuration.

Both second-generation web-based authentication and built-in portal web-based authentication support local account authentication on the NAS. Because Remote Authentication Dial In User Service (RADIUS) authentication is used in most situations, it is used as an example in 1.2 "Applications".

Web-based authentication supports user online traffic detection. For details, see *Configuring SCC*.

Web-based authentication allows for authentication of domain names, meaning that accounts can be authenticated in the format of user name@domain name. To enable this function, you must enable domain-name-based authentication, authorization, and accounting (AAA). For details, see *Configuring AAA*.

Protocols and Standards

- HTTP: RFC 1945 and RFC 2068
- HTTPS: RFC 2818
- SNMP: RFC 1157 and RFC 2578
- RADIUS: RFC 2865, RFC 2866, and RFC 3576
- For the standards related to MAC address-based SMS authentication, see the *CMCC WLAN Device Interface Standards V3.1.0_20130901 (MAC Address-Based Authentication Extension), Zhejiang CMCC WLAN 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

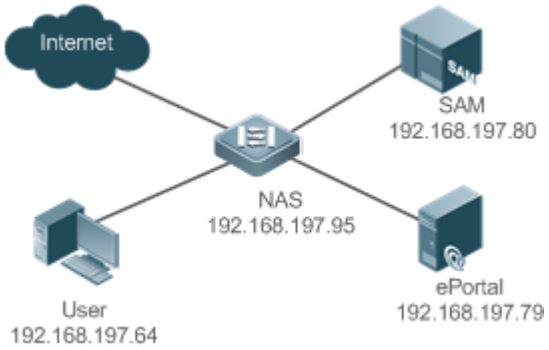
Application	Description
Basic Scenario of Web-based Authentication	In the typical Layer 2 authentication scenario, the NAS, portal server, and RADIUS server constitute an authentication system that connects clients to the NAS through the Layer 2 network.

1.2.1 Basic Scenario of Web-based Authentication

Scenario

- A web-based authentication scheme is deployed on the NAS.
- A downstream user connected to the NAS needs to pass web-based authentication before accessing the Internet.

Figure 1-1 Networking Topology of Web-based Authentication



Remarks	Web-based authentication is applicable to both Layer 2 and Layer 3 networks. On a Layer 3 network, the source MAC address and VLAN ID (VID) of a packet are changed after the packet is routed, but the source IP address remains the same and is used as the only identifier of a client. Therefore, a policy associated with web-based authentication on a Layer 3 device must adopt the IP-only binding mode. Here, the Layer 2 NAS is used as an example. RG-SAM+ is installed on the RADIUS server and RG-ePortal is installed on the portal server.

Deployment

- Enable web-based authentication on the interface to which a client is connected 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-based authentication).
- Configure Simple Network Management Protocol (SNMP) communication parameters of the ePortal server on the NAS (for only Ruijie first-generation and second-generation web-based authentication).
- Configure communication parameters on the ePortal server and SAM server (for only Ruijie first-generation web-based authentication).
- Create user accounts on the SAM server.
- Configure AAA and method lists on the NAS (for only Ruijie second-generation and iPortal web-based authentication).

- Configure the IP address of the SAM server on the NAS (for only Ruijie second-generation and iPortal web-based authentication).
- Configure names of the web-based authentication method lists on the NAS (for only Ruijie second-generation and iPortal web-based authentication).

1.3 Features

Basic Concepts

First-Generation Web-based Authentication

Ruijie first-generation web-based authentication requires the support of RG-ePortal. The server that has RG-ePortal installed (ePortal server) provides a login page to submit user authentication information, and initiates an authentication request directly to the RADIUS server. Once authentication succeeds, the NAS obtains user information delivered through SNMP, enabling control over user access permissions. This authentication mode depends on private SNMP nodes. Moreover, the ePortal server assumes the role of authentication and accounting, which relieves the NAS from service burden.

Second-Generation Web-based Authentication

Ruijie second-generation web-based authentication complies with *CMCC WLAN Service Portal Specification*. The portal server is responsible for interacting with users through web pages. The NAS interacts with the RADIUS server to implement authentication. The interaction between the portal server and NAS complies with *CMCC WLAN Service Portal Specification*. The portal server provides a login page where users can submit their information, and then informs the NAS of user information through the portal protocol. 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-based authentication is mainly completed on the NAS. This places a higher demand on the NAS's capability to handle heavy tasks. In this case, the configuration of the portal server is simplified. The widely supported *CMCC WLAN Service Portal Specification* allows various vendors to develop compatible products.

iPortal Web-based Authentication

In iPortal web-based authentication, the NAS integrates web page interaction of the portal server with partial authentication interaction of the RADIUS server. The NAS comes with a default authentication page suite, which can be customized based on instructions provided in this manual. Once configured, the page suite can be downloaded and stored on the storage medium of the NAS.

Comparison Between Different Authentication Modes

Authentication roles:

- Client:
- The functions remain the same for the three web-based authentication modes.
- NAS: In first-generation web-based authentication, the NAS implements only URL redirection and exchanges user login/logout notifications with the portal server. In second-generation web-based authentication, the NAS is

responsible for redirecting and authenticating users as well as notifying the portal server of authentication results. In iPortal web-based authentication, the NAS integrates multiple functions including URL redirection, web page interaction, and authentication.

- Portal server: In first-generation web-based authentication, the portal server is responsible for interacting with clients through web pages, authenticating users, and notifying the NAS of authentication results. In second-generation web-based authentication, the portal server is responsible for interacting with clients through web pages, notifying the NAS of users' authentication information, and receiving authentication results from the NAS. In iPortal web-based authentication, the portal server is built into the NAS and provides simplified functions, and is mainly responsible for interaction with clients through web pages.
- RADIUS server: The functions remain the same for the three web-based authentication modes.

Authentication process:

- In second-generation web-based authentication, authentication and accounting functions are transferred from the portal server to the NAS.
- In second-generation web-based authentication, because authentication is performed on the NAS, the NAS does not need to wait for the authentication results notified by the portal server.
- iPortal web-based authentication simplifies and integrates features of the portal servers into the NAS compared with first- and second-generation web-based authentication.

Logout process:

- In first-generation web-based authentication, a logout action may be triggered by a notification from the portal server, or traffic or port status detection performed by the NAS. In second-generation web-based authentication, a logout action may be triggered by a notification from the portal server, a disconnection notification from the RADIUS server, or traffic or port status detection performed by the NAS. In iPortal web-based authentication, a logout action may be triggered by logout of a user that clicks the logout button on the online page, a disconnection notification from the RADIUS server, or traffic or port status detection performed by the NAS.
- In first-generation web-based authentication, Accounting Stop packets are sent by the portal server. In second-generation and iPortal web-based authentication, Accounting Stop packets are sent by the NAS.

The web-based authentication mode selected depends on the type of the portal server in use.

Command parameters in this document may be shared by the three web-based authentication modes or not. Read through this document carefully to avoid parameter misconfiguration that will affect web-based authentication.

Overview

Feature	Description
First-Generation Web-based Authentication	The portal server is deployed and supports only first-generation web-based authentication.
Second-Generation Web-based Authentication	The portal server is deployed and complies with *CMCC WLAN Service Portal Specification*.
iPortal Web-based Authentication	The portal server is not deployed, and the NAS supports web page interaction.

Feature	Description
MAC Address-Based SMS Authentication	A non-authenticated user is allowed to access the Internet after accessing the WLAN. After the traffic used over the specified interval reaches the specified threshold, the authentication device sends a request to query the bound MAC address.
RIPT Web-based Authentication	When the AC fails or the connection between the AC and AP is terminated, the web-based authentication module of the AP can still provide authentication services.
WiFiDog Web-based Authentication	A non-authenticated user will be redirected to the authentication page for authentication.
WeChat Web-based Authentication	After assessing the WLAN, 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.
ClearPass Authentication	Non-authenticated users can be redirected to the authentication page for authentication.

1.3.1 First-Generation Web-based Authentication

- **HTTP Interception**

HTTP interception means that the NAS intercepts to-be-forwarded HTTP packets. These HTTP packets are initiated by browsers of clients connected to the NAS, but they are not destined for the NAS. For example, when a client attempts to visit www.google.com using Internet Explorer, the NAS is expected to forward the HTTP request packets to a gateway. However, if HTTP interception is enabled, these packets will not be forwarded.

Once HTTP interception is successful, the NAS redirects the client's HTTP requests to itself, establishing a session between them. Then the NAS pushes a redirection page to the client through HTTP redirection. A web page pops up on the client's browser, on which authentication, software download, or other operations can be performed.

You can specify the clients and destination interfaces to enable or disable HTTP interception for web-based authentication. In most cases, HTTP requests from non-authenticated clients will be intercepted, and those from authenticated clients will not. HTTP interception is the basis for web-based authentication, that is, web-based authentication is automatically triggered after successful HTTP interception.

- **HTTP Redirection**

As defined by HTTP, when the NAS receives an HTTP GET or HEAD request packet from a client, it replies with a packet with 200 (Ok) status code if it can provide required resources. Alternatively, a packet with 302 (Moved Temporarily) status code is returned if it cannot. The 302 packet includes another URL for redirection. After receiving the packet, the client may resend an HTTP GET or HEAD request packet to the new URL for requesting resources. This process is called redirection.

HTTP redirection is crucial in web-based authentication after HTTP interception. It utilizes the 302 status code defined in HTTP. HTTP interception creates a session between the NAS and a client. The client sends HTTP GET or HEAD request packets (originally intended for another site) to the NAS. The NAS responds with a 302 packet with a specific redirection page. As a result, the client resends the requests to the redirection page.

Because more and more applications run HTTP, the use of the 302 redirection packet may redirect a large amount of non-browser HTTP traffic to the portal server, which will affect network authentication. To address this problem, the NAS adopts noise reduction in its HTTP redirection technology, replacing the 302 packets with JavaScript scripts.

Working Principle

Figure 1-1 shows the networking topology of web-based authentication.

First-generation web-based authentication roles:

1 Authentication client: Is usually a browser running HTTP. It sends HTTP requests for accessing the Internet.

2 NAS: Is an access-layer device on 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-based authentication.

3 Portal server: Provides a web page for web-based 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 for 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 that has RG-SAM+ installed.

First-generation web-based authentication process:

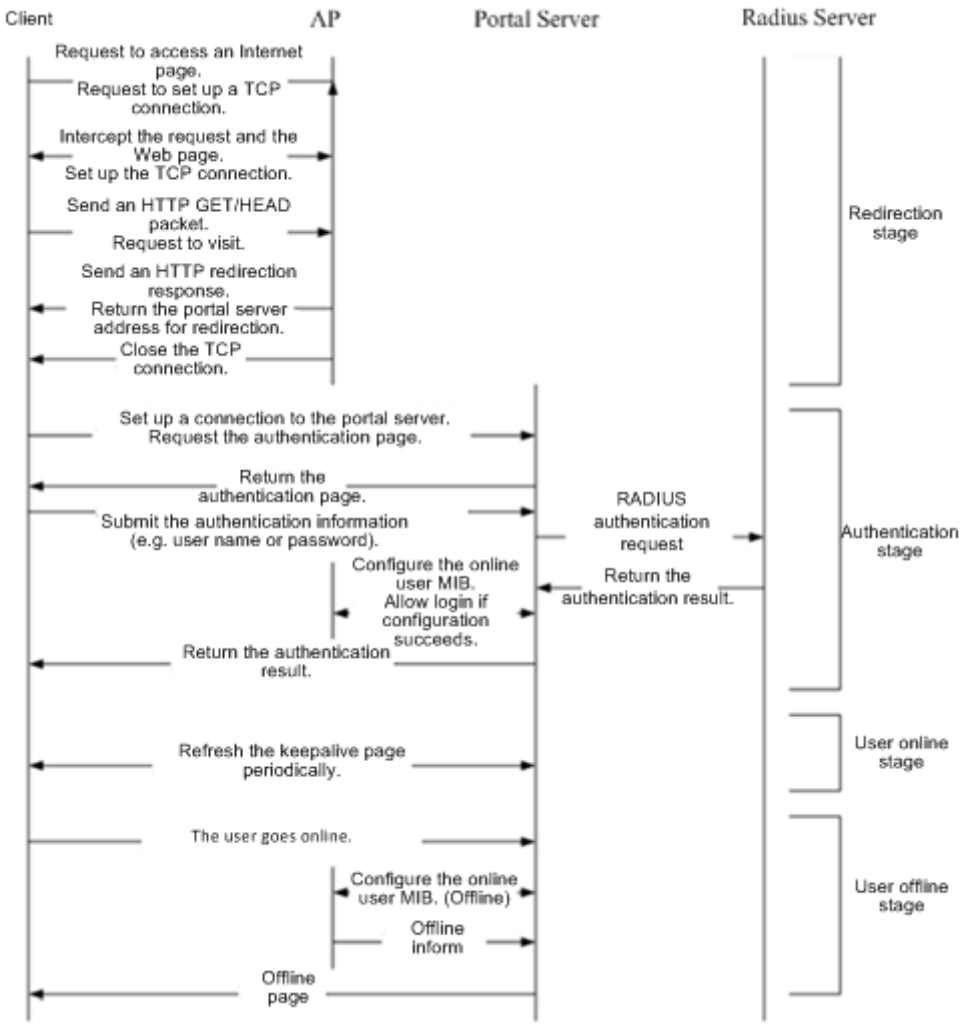
1 Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the portal server. Then an authentication page is displayed on the browser.

2 During authentication, the client enters information, for example, username, password, and verification code, on the authentication page to interact with the portal server and complete authentication.

3 After the user is authenticated, the portal server notifies the NAS that the client has passed authentication, and the NAS allows the client to access resources on the Internet.

Figure 1-2 shows the flowchart of Ruijie first-generation web-based authentication by using an AP as the NAS.

Figure 1-2 Flowchart of Ruijie First-Generation Web-based Authentication



Client logout process:

There are two scenarios of client logout. In the first scenario, the NAS detects that a client has gone offline due to reasons such as reaching the maximum online time, exceeding the traffic limit, or experiencing a disconnection in the link. The second scenario occurs when the portal server detects that a client has initiated logout by clicking the logout button on the logout page or when the keepalive page becomes unavailable.

1 Scenario 1: When the NAS detects a client logging out, it informs the portal server. Subsequently, the portal server uses SNMP to delete user information from the NAS and pushes a logout page to the client.

2 Scenario 2: When the portal server detects a client logging out, it informs the NAS through SNMP and pushes a logout page to the client.

3 In the two scenarios, the portal server sends an Accounting Stop packet to the RADIUS server, notifying it that the client has logged out.

Related Configuration

↘ Configuring the First-Generation Web-based Authentication Template

By default, the first-generation web-based authentication template is not configured.

Run the **web-auth template eportalv1** command in global configuration mode to create the first-generation web-based authentication template.

The template is used to implement web-based 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 Web-based Authentication URL of the Portal Server

By default, the web-based authentication URL of the portal server is not configured.

Run the **url** *url-string* command in template configuration mode to configure the web-based authentication URL of the portal server.

The URL to which clients are redirected is the address of the web-based authentication URL provided by the portal server.

Specifying the Web-based Authentication Binding Mode

The default web-based authentication binding mode is IP-only.

Run the **bindmode** command in template configuration mode to specify the web-based authentication binding mode.

In web-based authentication across the Layer 3 network, 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 Web-based Authentication Communication Key

By default, the web-based authentication communication key is not configured.

Run the **web-auth portal key** [**0** | **1** | **7**] *key-string* command in global configuration mode to configure the web-based authentication communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling First-Generation Web-based Authentication

By default, first-generation web-based authentication is disabled.

Run the **webauth** command in WLAN security configuration mode to enable first-generation web-based authentication.

Configuring the SNMP Server

By default, the SNMP server 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 and community string for web-based authentication.

The SNMP server is configured to receive Inform or 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 or Inform Function

By default, the SNMP Trap or Inform function is disabled.

Run the **snmp-server enable traps web-auth** command in global configuration mode to enable the SNMP Trap or Inform function.

The SNMP Trap or Inform function is configured to enable the NAS to inform the portal server of user logout.

1.3.2 Second-Generation Web-based Authentication

- **HTTP Interception**

It is the same as the HTTP interception technology of first-generation web-based authentication.

- **HTTP Redirection**

It is the same as the HTTP redirection technology of first-generation web-based authentication.

Working Principle

Figure 1-1 shows the networking topology of web-based authentication.

Second-generation web-based authentication roles:

1 Authentication client: Is usually a browser running HTTP. It sends HTTP requests for accessing the Internet.

2 NAS: Is an access-layer device on a network (for example, an AP on a wireless network). The NAS is directly connected to clients and must be enabled with web-based authentication. The NAS receives user authentication information from the portal server, sends authentication requests to the RADIUS server, determines whether users can access the Internet according to authentication results, and returns the authentication results to the portal server.

3 Portal server: Provides a web page for web-based 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 for remote clients. When a device initiates authentication to the RADIUS server, authentication packets include the following parameters: wlanuserip (user IP address), wlanacname (AC name), ssid (SSID), nasip (NAS device's IP address), mac (user MAC address), and url (URL accessed by the user before redirection). Figure 1-1 shows the RADIUS server that has RG-SAM+ installed.

Second-generation web-based authentication process:

1 Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the portal server. Then an authentication page is displayed on the browser.

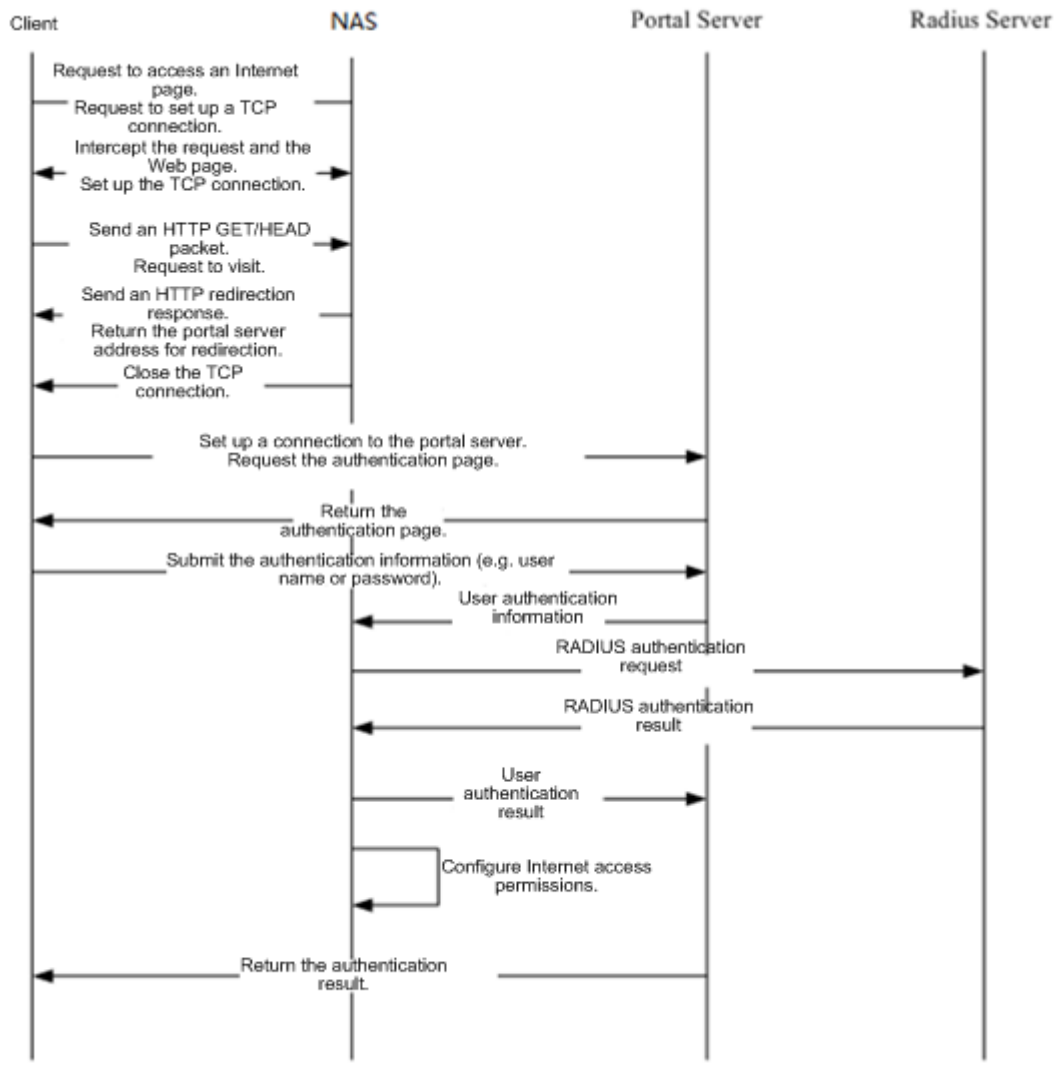
2 During authentication, the client enters information, for example, username, password, and verification code, on the web-based authentication URL to interact with the portal server.

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-based Authentication



Client logout process:

There are two scenarios of client logout. In the first scenario, the NAS detects that a client has gone offline due to reasons such as reaching the maximum online time, exceeding the traffic limit, or experiencing a disconnection in the link. The second scenario occurs when the portal server detects that a client has initiated logout by clicking the logout button on the logout page or when the keepalive page becomes unavailable.

1 When a user clicks the logout button on the online page, the portal server instructs the NAS to disconnect the user.

2 The NAS disconnects a client with traffic lower than the threshold based on parameters of user online traffic detection.

3 When the RADIUS server intends to forcibly disconnect a client based on a specific policy, the NAS instructs the portal server to push a logout page to the client.

Related Configuration

↘ Configuring the Second-Generation Web-based Authentication Template

By default, the second-generation web-based authentication template is not configured.

Run the **web-auth template** { **eportalv2** | *template-name* **v2** } command in global configuration mode to create a second-generation web-based authentication template.

The template is used to implement web-based 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 Web-based Authentication URL of the Portal Server

By default, the web-based authentication URL of the portal server is not configured.

Run the **url** *url-string* command in template configuration mode to configure the web-based authentication URL of the portal server.

The URL to which clients are redirected is the address of the web-based authentication URL provided by the portal server.

Specifying the Web-based Authentication Binding Mode

The default web-based authentication binding mode is IP-only.

Run the **bindmode** command in template configuration mode to specify the web-based authentication binding mode.

In web-based authentication across the Layer 3 network, 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 Web-based Authentication Communication Key

By default, the web-based authentication communication key is not configured.

Run the **web-auth portal key** [**0** | **1** | **7**] key-*string* command in global configuration mode to configure the web-based authentication communication key.

The communication key is used to encrypt URL parameters to avoid information disclosure.

Enabling Second-Generation Web-based Authentication

By default, second-generation web-based authentication is disabled.

Run the **webauth** command in WLAN security configuration mode to enable second-generation web-based authentication.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

Ruijie second-generation web-based authentication relies on AAA. Therefore, enable AAA before you use second-generation web-based authentication.

Configuring the RADIUS Server and Communication Key

By default, the RADIUS server and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS server and communication key.

The RADIUS server is responsible for authenticating users.

Configuring an AAA Method List for Ruijie Second-Generation Web-based Authentication

By default, no AAA method list is configured for Ruijie second-generation web-based authentication.

Run the **aaa authentication web-auth** command in global configuration mode to configure an AAA method list for Ruijie second-generation web-based authentication.

The AAA authentication method list is used for interaction during web-based authentication.

Configuring an AAA Method List for Ruijie Second-Generation Web-based Accounting

By default, no AAA method list is configured for Ruijie second-generation web-based accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for Ruijie second-generation web-based accounting.

The AAA method list for web-based accounting is used for accounting interaction during web-based authentication.

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 the AAA module.

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 the AAA module.

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-based Authentication

- **HTTP Interception**

It is the same as the HTTP interception technology of Ruijie first-generation web-based authentication.

- **HTTP Redirection**

It is the same as the HTTP redirection technology of Ruijie first-generation web-based authentication.

Working Principle

Compared with Ruijie first-generation web-based authentication shown in Figure 1-1, Ruijie iPortal web-based authentication does not require the portal server.

iPortal web-based authentication roles:

1 Authentication client: Is typically a browser running HTTP. It sends HTTP requests for accessing the Internet.

2 NAS: Is an access-layer device on a network. It is directly connected to clients on a wired or wireless network and must be enabled with Ruijie iPortal web-based authentication. The NAS resolves the account information that clients enter on a web page 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 browser.

3 RADIUS server: Provides the RADIUS-based authentication service for remote clients. Figure 1-1 shows the RADIUS server that has RG-SAM+ installed.

iPortal web-based authentication 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 web-based authentication URL to interact with the iPortal server (NAS).

3 The NAS initiates authentication to the RADIUS server and pushes the authentication result (success or failure) to the client on a page.

Client logout process:

1 The NAS disconnects a client when the user clicks the logout button on the web page.

2 The NAS disconnects a client with traffic lower than the threshold based on parameters of user online traffic detection.

3 When the RADIUS server disconnects a client offline based on a certain policy, the NAS pushes a logout page to the client.

Related Configuration

Configuring the iPortal Web-based Authentication Template

By default, the iPortal web-based authentication template is not configured.

Run the **web-auth template iportal** command in global configuration mode to create an iPortal web-based authentication template.

The template is used to configure authentication 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 Web-based Authentication Binding Mode

The default web-based authentication binding mode is IP-only.

Run the **bindmode** command in template configuration mode to specify the web-based authentication binding mode.

In web-based authentication across the Layer 3 network, 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-based Authentication

By default, Ruijie iPortal web-based authentication is disabled.

Run the **webauth** command in WLAN security configuration mode to enable iPortal web-based authentication.

Enabling AAA

By default, AAA is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA.

Ruijie iPortal web-based authentication relies on AAA. Enable AAA before you implement web-based authentication.

Configuring the RADIUS Server and Communication Key

By default, the RADIUS server and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS server and communication key.

The RADIUS server in web-based authentication is responsible for authenticating users.

Configuring an AAA Method List for Ruijie iPortal Web-based Authentication

By default, no AAA method list is configured for Ruijie iPortal web-based authentication.

Run the **aaa authentication iportal** command in global configuration mode to configure an AAA method list for Ruijie iPortal web-based authentication.

The AAA authentication method list is used for interaction during web-based authentication.

Configuring an AAA Method List for Ruijie iPortal Web-based Accounting

By default, no AAA method list is configured for Ruijie iPortal web-based accounting.

Run the **aaa accounting network** command in global configuration mode to configure an AAA method list for Ruijie iPortal web-based accounting.

The AAA accounting method list is used for accounting interaction during web-based authentication.

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 the AAA module.

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 the AAA module.

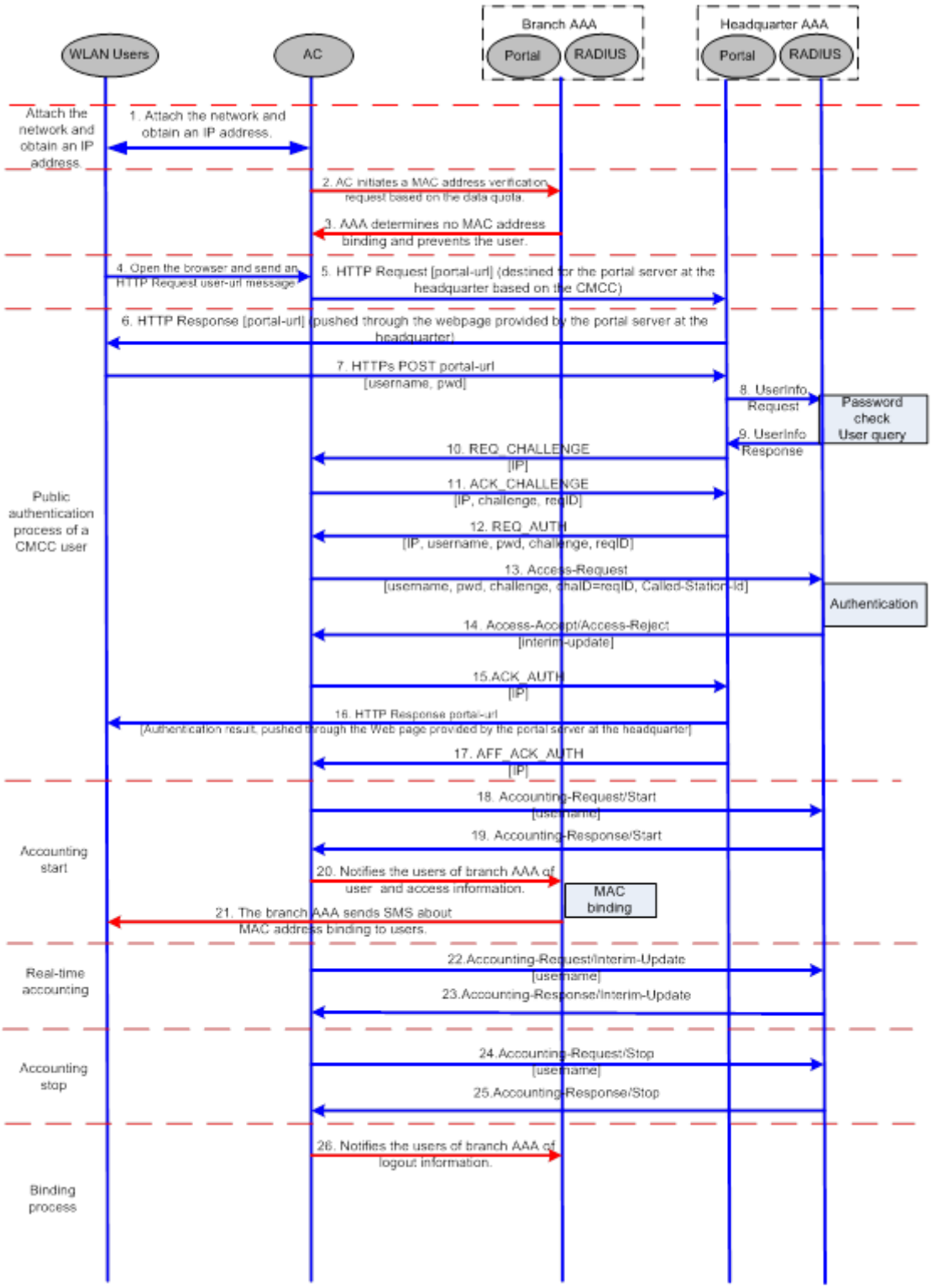
1.3.4 MAC Address-Based SMS Authentication

Working Principle

After a 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 to a MAC address, the portal server sends an authentication request. If the STA is not bound to a MAC address, the STA needs to re-perform authentication on the portal server before accessing the Internet.

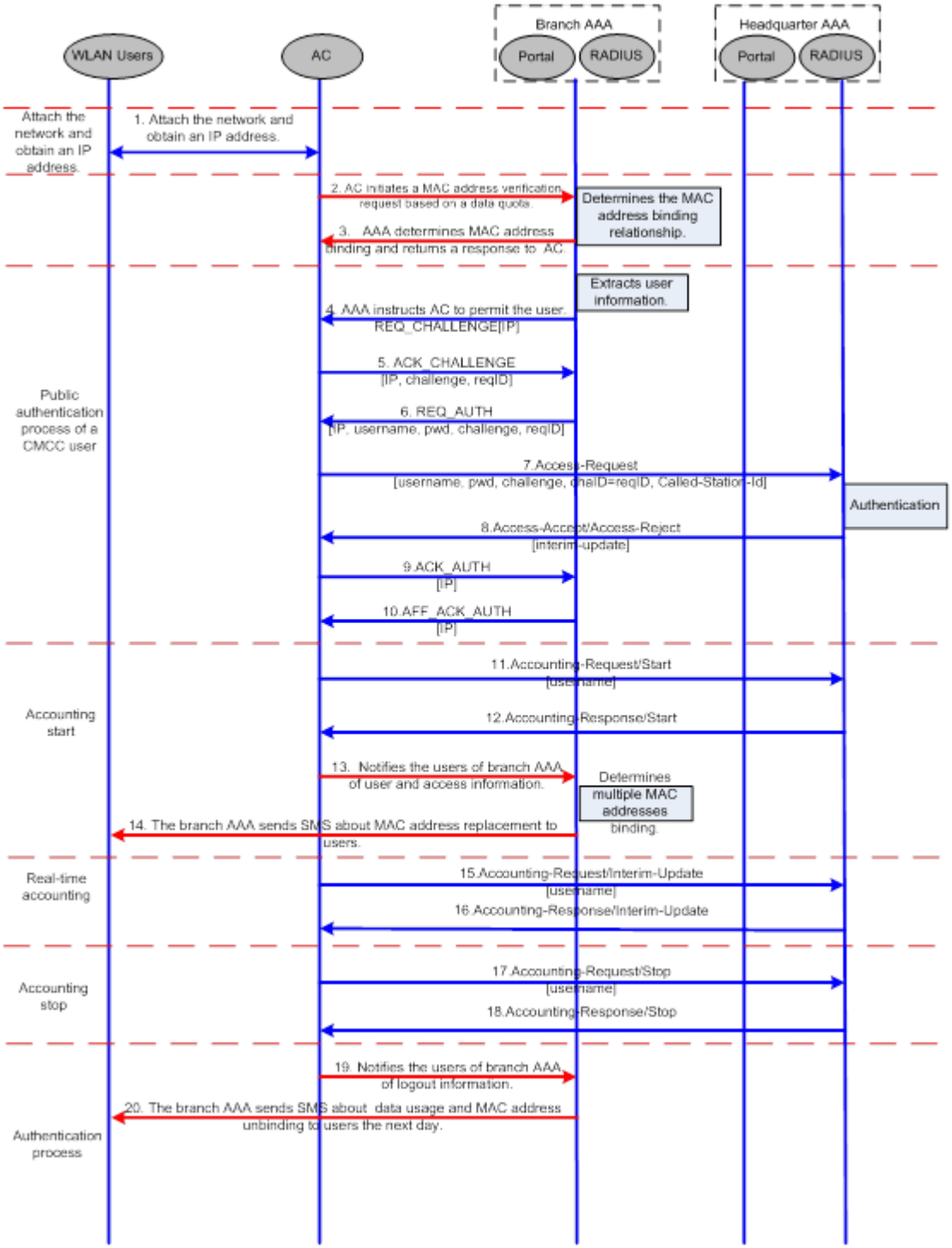
SMS Authentication Process for Unbound STAs

In the following figure, the SSID is enabled with MAC address-based SMS authentication, and a STA that is not bound to a MAC address is associated with the SSID to access the Internet. Compared with Ruijie second-generation web-based authentication, MAC address-based SMS authentication involves querying MAC address binding and notifying the bound portal server of user login or /logout. If the STA selects the binding check box when performing authentication on the portal server, the portal server will bind the STA to a MAC address. The STA can directly access the Internet during subsequent connections.



↘ SMS Authentication Process for Bound STAs

After a STA is bound to 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.



1.3.5 RIPT Web-based Authentication

Web-based authentication supports the Remote Intelligent Perception Technology (RIPT) function. When an AC is faulty or the connection between an AC and an AP is terminated, RIPT allows the AP to provide web-based authentication services.

Working Principle

To enable RIPT, configure an RIPT AP group on an AC. For details, see *Configuring RIPT*. In RIPT AP authentication mode, the configurations related to web-based authentication on the AC are delivered to the AP. The AP can function as access devices to provide the web-based authentication service externally. STAs do not need to perform web-based authentication on the AC. The information of STAs who pass authentication on the APs is synchronized to the AC and can be queried on the AC.

↘ Delivering Configurations

In RIPT AP authentication mode, the configurations of AAA and RADIUS on the AC and port-based web-based authentication control in RSNA will be issued to the APs. Then the APs can provide WLAN services externally, including the web-based authentication service.

↘ Synchronizing STA Information from the AP to the AC

If STAs pass authentication by an RIPT AP which provides the web-based authentication service externally, information about the STAs will be synchronized to the AC and can be queried on the AC.

1.3.6 WiFiDog Web-based Authentication

- **HTTP Interception**

It is the same as the HTTP interception technology of Ruijie first-generation web-based authentication.

- **HTTP Redirection**

It is the same as the HTTP redirection technology of Ruijie first-generation web-based authentication.

Working Principle

The networking topology of WiFiDog web-based authentication is the same as that shown in Figure 1-1.

Roles involved in WiFiDog web-based authentication:

1 Authentication client: Is typically a browser running HTTP. It sends HTTP requests for accessing the Internet.

2 NAS: Is an access-layer device on a network, for example, an AP on a wireless network. The NAS is directly connected to clients and must be enabled with web-based authentication. The NAS controls users' Internet access permissions, receives 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-based authentication and related operations. The portal server receives 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 web page provided by the portal server.

4 Authentication server: Provides the authentication service. The authentication server negotiates with the portal server to determine the authentication protocol (for example, RADIUS) used.

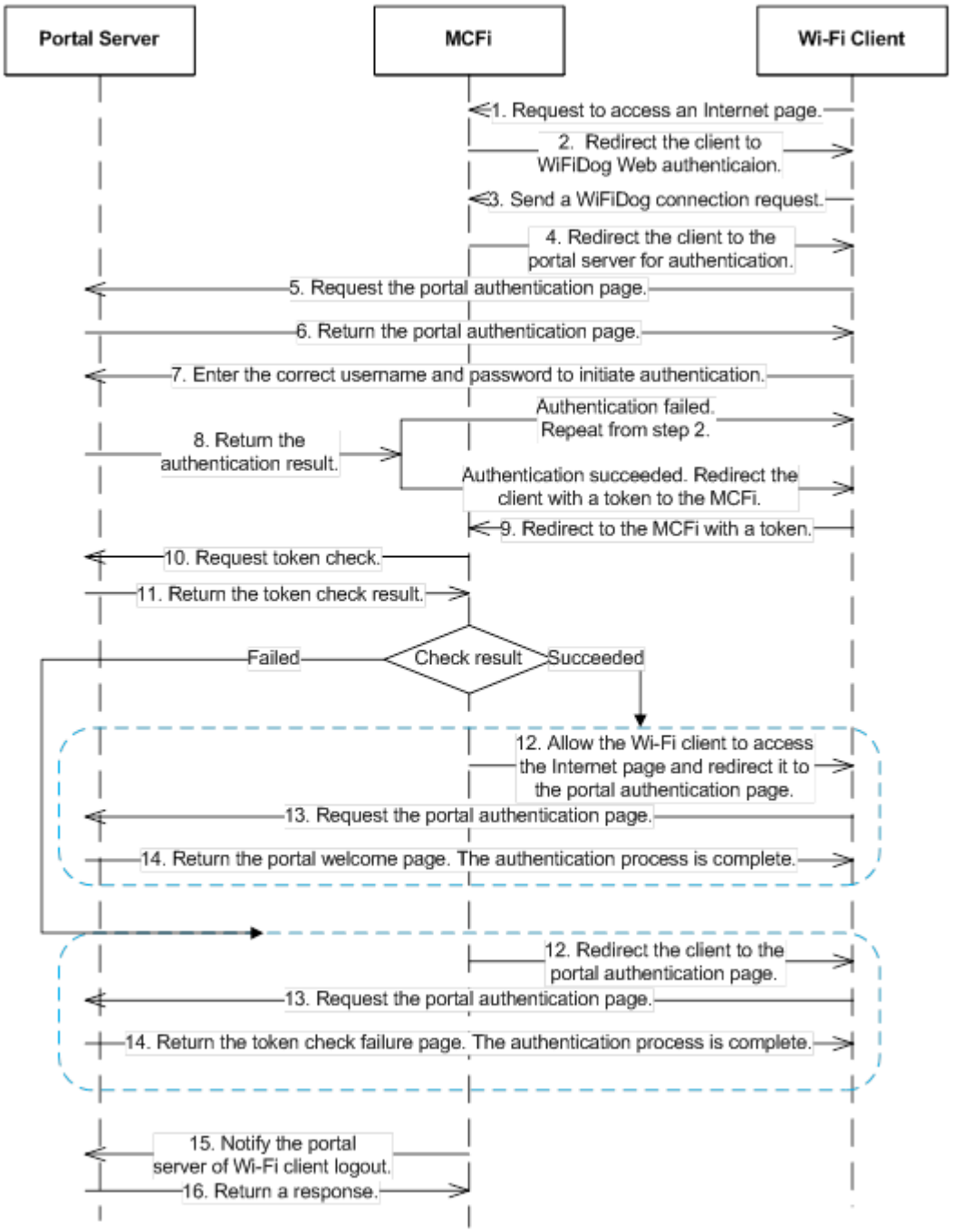
5 WiFiDog web-based authentication process: Before authentication, the NAS intercepts all HTTP requests from a client and redirects these requests to the iPortal server. Then an authentication page is displayed on the browser.

6 During authentication, the client enters information, for example, username, password, and verification code, on the web-based authentication URL to interact with the portal server.

7 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.

8 After receiving a request from the client, the NAS initiates check to the portal server. The NAS redirects the client to a web page provided by the portal server based on the check result.

Figure 1-4 Flowchart of WiFiDog Web-based Authentication



Client logout process:

There are two scenarios of client logout. In the first scenario, the NAS detects that a client has gone offline due to reasons such as reaching the maximum online time, exceeding the traffic limit, or experiencing a disconnection in the

link. The second scenario occurs when the portal server detects that a client has initiated logout 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 may be sent to the portal server and NAS at different time points, depending on the capability of the portal server.)

2 The NAS disconnects a client with traffic lower than the threshold based on parameters of user online traffic detection.

Related Configuration

Configuring a WiFiDog Web-based Authentication Template

By default, the WiFiDog web-based authentication template is not configured.

Run the **web-auth template** { **wifidog** | *template-name* **wifidog** } command in global configuration mode to create a WiFiDog web-based authentication template.

The template is used to implement web-based 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 Web-based Authentication 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 web-based authentication URL of the portal server.

The URL to which clients are redirected is the address of the web-based authentication 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 the Gateway ID

By default, the gateway ID is set to the serial number of the device. It is mandatory in hot standby and VAC scenarios. It can be set to the MAC address of a device.

Run the **gateway-id** *string* command in template configuration mode to configure the gateway ID.

This parameter is carried in the WiFiDog packets and provided for the interconnected third-party portal.

Enabling WiFiDog Web-based Authentication

By default, WiFiDog web-based authentication is disabled.

Run the **webauth** command in WLAN security configuration mode to enable the WiFiDog web-based authentication.

1.3.7 WeChat Web-based Authentication

- **HTTP Interception**

It is the same as the HTTP interception technology of Ruijie first-generation web-based authentication.

- **HTTP Redirection**

It is the same as the HTTP redirection technology of Ruijie first-generation web-based authentication.

Working Principle

The networking topology of WeChat web-based authentication is the same as that shown in Figure 1-1.

Roles involved in WeChat web-based authentication:

1 User: Sets up a Wi-Fi connection through WeChat to access the Internet.

2 In-shop AP: Is a Fat or Fit AP.

3 Authentication server: Is a portal server or other authentication server such as Marketing Cloud Platform (MCP), Wireless Marketing Cloud (WMC), or a third-party server.

4 WeChat server: Is a WeChat background server.

Process of scanning quick response (QR) codes by WeChat for authentication:

1 A user initiates a Wi-Fi connection request by scanning the QR code through WeChat.

2 The WeChat App identifies the QR code and calls the WeChat server (through the GSM by a mobile phone.)

3 The WeChat server checks the connection request based on the QR code policy.

4 The WeChat server returns an SSID to the WeChat user for its connection.

5 The WeChat user sends a connection request to the AP.

6 After connecting to the AP, the WeChat user sends a blocklist request, with the requested address being http://10.1.0.6/redirect. The request aims to inform the AP that the request is sent by a WeChat client.

7 After receiving the blocklist request, the AP sends a 302 redirection request, in which the auth parameter carries the MAC addresses of the mobile phone and AP in encryption mode.

8 After receiving the auth parameters, the WeChat client sends the WeChat server an allowlist request carrying the auth parameters for Wi-Fi connection authorization. The IP address of the WeChat server must be added to the allowlist of the AP to enable the AP to permit the authentication request to pass before authentication on the AP is complete.

9 The AP determines that the requested IP address is in the allowlist and permits the allowlisted request to pass to the WeChat server.

10 The WeChat server sends an HTTP-based authorization request to the device vendor server. The request maps interface 8. Ensure that interface 13 has been called to set the device vendor server URL and token parameter.

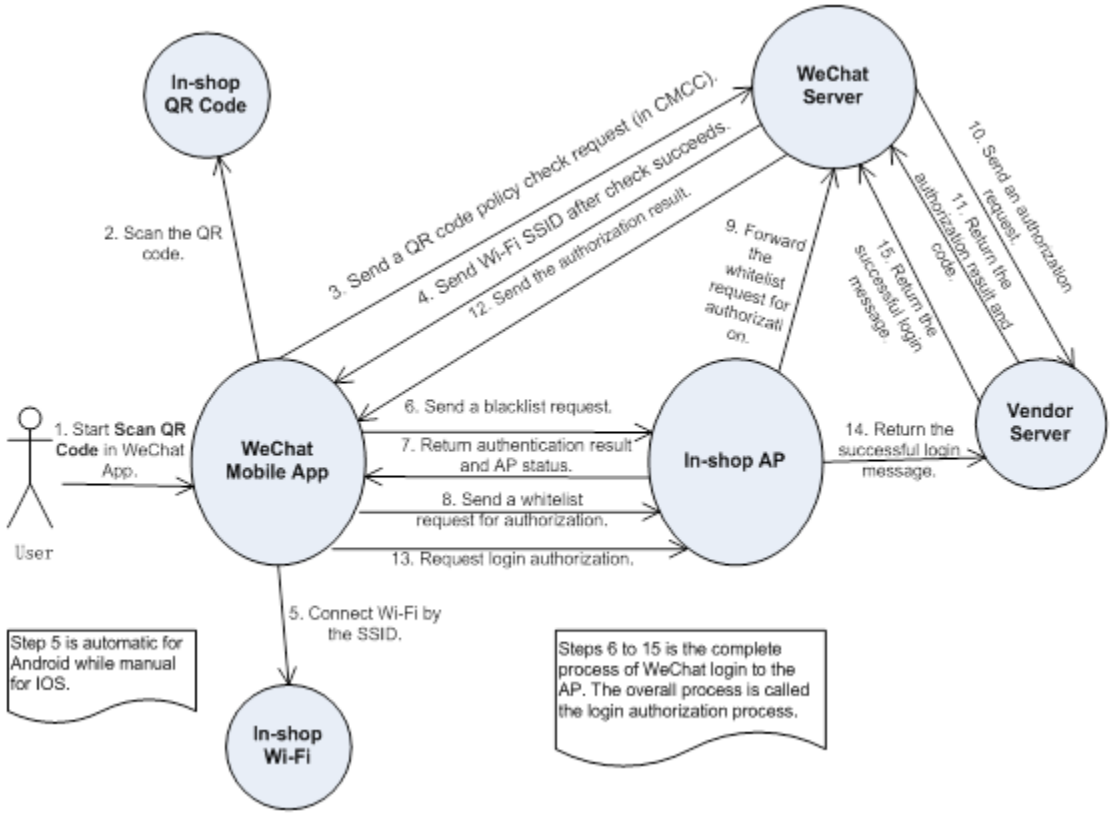
11 The device vendor server implements authorization according to the authorization request and returns an authentication address and the login parameter on interface 8.

12 The WeChat server returns the authentication address and parameter to the WeChat client.

13 The WeChat client requests the authentication address by sending a login request.

14 The AP or device vendor's server implements Internet access authentication. The AP permits the MAC address of the mobile phone to pass, and the device vendor's server calls interface 7 to notify the WeChat server of successful Internet access (see step 15 in Figure 1-5). The AP returns a 302 redirection packet carrying the res=success parameter to the WeChat client. The WeChat client determines that Internet access authorization is successful based on this parameter. A page indicating that a Wi-Fi connection is set up successfully is displayed on the WeChat client.

Figure 1-5 QR Code Scan Process in WeChat-Based Wi-Fi Connection Authentication



Process of the Internet access of multiple mobile devices by scanning dynamic QR codes on a PC:

1 Steps 1 and 2: A user starts a PC to set up a Wi-Fi connection and chooses to connect to an SSID.

2 Step 3: When the user opens the browser and accesses a website, the browser sends a network request.

3 Step 4: The AP returns a 302 packet to display a portal authentication page on the browser. To enable a mobile phone to connect to the Internet by scanning a QR code displayed on the PC, the AP sends a request to the device vendor's server.

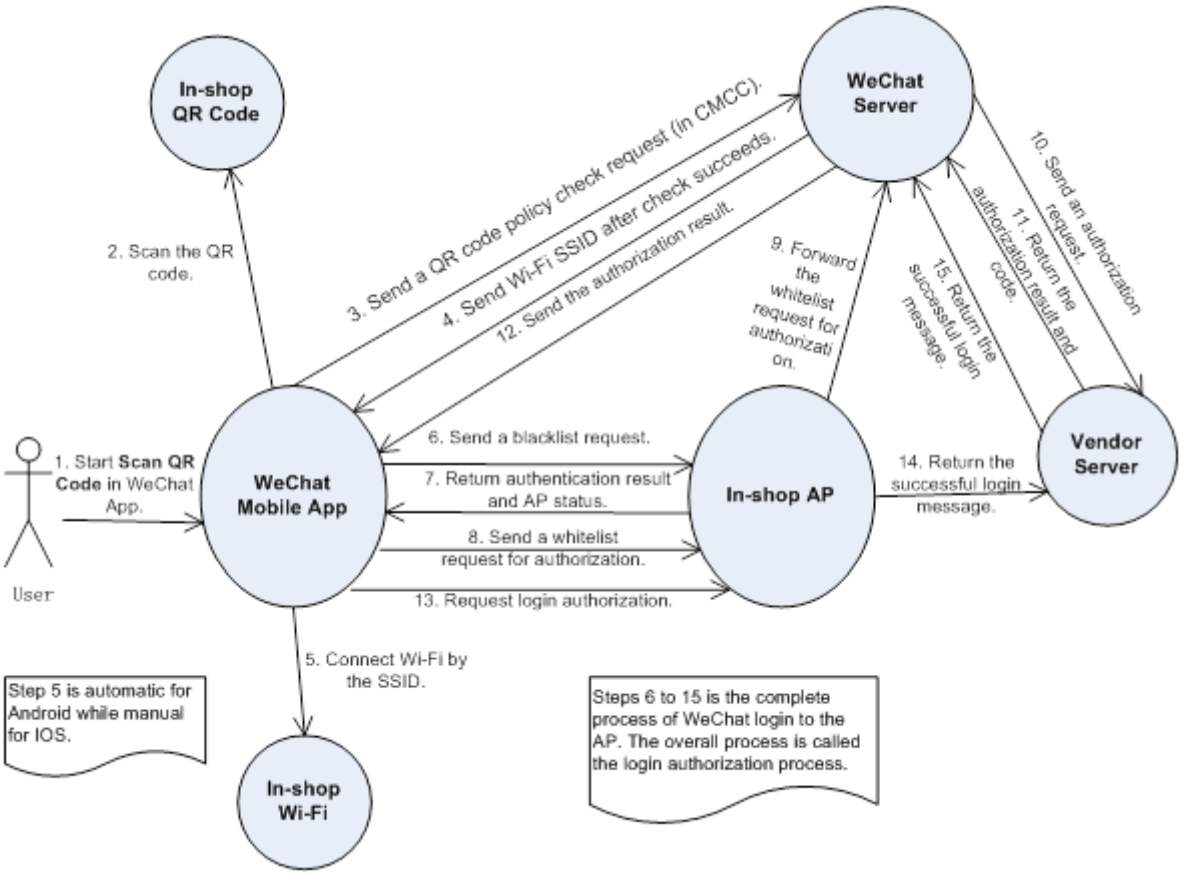
4 Step 5: The device vendor's server calls interface 2 of the WeChat server to obtain the URL of the QR code photo.

5 Step 6: The WeChat server returns the URL of the QR code photo to the device vendor's server.

6 Step 7: The device vendor's server sends the URL to the AP.

7 Steps 8 to 10: The AP sends the browser a 302 packet carrying the URL, which will be embedded into the portal authentication page. The mobile phone can scan the QR code and connect to the Internet based on the normal access process.

Figure 1-6 **Process Where Multiple Mobile Devices Access the Internet by Scanning Dynamic QR Codes on a PC**



The NAS detects logout when a user's time is reached, the data quota is reached, or the link is disconnected.

1 The NAS disconnects a client with traffic lower than the threshold based on parameters of user online traffic detection.

2 The link disconnection duration depends on anti-jitter parameters.

Related Configuration

↘ Configuring a WeChat Web-based Authentication Template

By default, the WeChat web-based authentication template is not configured.

Run the **web-auth template** { **wechat** | *template-name* **wechat** } command in global configuration mode to create a WeChat web-based authentication template.

The template is used to implement web-based 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 Web-based Authentication URL

By default, no WeChat web-based authentication URL is configured.

Run the **service-url** *url-string* command in template configuration mode to configure the WeChat web-based authentication 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. 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 the URL of the Portal Server

By default, the URL of the portal server is the SMS authentication redirection URL when both WeChat and SMS authentication are enabled.

Run the **url** *url-string* command to configure the URL of the portal server 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.

The access service IP address for WeChat web-based authentication is used for communicating with the portal server.

The access service IP address of the NAS cannot be configured as the passthrough address.

When the access service IP address is configured as the IP address of the NAS and a STA in the authentication template accesses this IP address, the NAS intercepts the request of the STA and forwards it to the server. As a result, the STA fails to access the web management page of the NAS.

If a STA in the authentication template accesses this IP address for device management, configure the access service IP address as the unused virtual service IP address, for example, 1.1.1.1 and 2.2.2.2.

If the actual IP address of a device is used to log in to the device, there are security issues. In this case, the IP address for device management is mapped to the extranet IP address. Security devices such as firewalls are deployed between the extranet and servers to ensure security, whereas no security measures are taken for access through the intranet. If the actual IP address of the device is visible, the device can be easily attacked. The virtual IP address is recommended.

Configuring the Encryption 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.

Configuring NAS ID

By default, the NAS ID is the MAC address of the NAS.

The NAS ID is mandatory in hot standby or VAC scenarios.

In AC configuration mode, run the **nas-id** *nas-id-string* command to configure the NAS ID.

Enabling Web-based Authentication

By default, web-based authentication is disabled.

Run the **web-auth portal** { **wechat** | *template-name* **wechat** } command in WLAN security configuration mode and **webauth** command to enable web-based authentication on the port connected to STAs.

After web-based authentication is enabled, the non-authenticated STAs connecting to the port will be redirected to a one-click Internet access page provided by the portal server, and the non-authenticated PCs connecting to the port will be redirected to a QR code page.

Enabling the Escape Function

By default, the 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 escape function in the WLAN security configuration mode is preferred. If the espace function is not configured in WLAN security configuration mode, the configuration in global configuration mode takes effect.

When the server fails or the escape function is required, subsequent users connected to the device enabled with the escape function can be free of authentication. The online duration of escape users is specified by **interval** *minutes*.

To disable the escape function, run the **web-auth wechat-escape recover** command in global configuration mode.

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 does not receive a response from the server or receives a response indicating that the server is unavailable within the value specified by **interval** *minutes*, subsequent users gain access without authentication.

To cancel server detection, run the **no web-auth wechat-check** command in global configuration mode.

1.3.8 ClearPass Authentication

- **HTTP Interception**

It is the same as the HTTP interception technology of Ruijie first-generation web-based authentication.

- **HTTP Redirection**

It is the same as the HTTP redirection technology of Ruijie first-generation web-based authentication.

Working Principle

The networking topology is the same as that in Figure 1-7.

Roles in web-based authentication:

1 Authentication client: Is usually a browser running HTTP. It sends HTTP requests for accessing the Internet.

2 Network device: Typically refers to an access-layer device, for example, an AP on a WLAN. Generally, a network device is directly connected to STAs and needs to be enabled with web-based authentication. The device controls user's Internet access permissions, receives token verification requests or network release requests from the authentication client, and is responsible for verifying token information for the portal server.

3 Portal server: Provides a web page for web-based authentication and allows related operations. The portal server receives HTTP-based authentication requests from an authentication client, extracts account information from the requests, performs background authentication, and transfers the authentication result to the network device through the authentication client, and requests the authentication client to redirect to the relevant page of the portal server after network device verification.

4 Authentication server: Provides user authentication services. The specific authentication protocol such as RADIU is determined through negotiation between the portal server and the authentication server.

Process of ClearPass authentication:

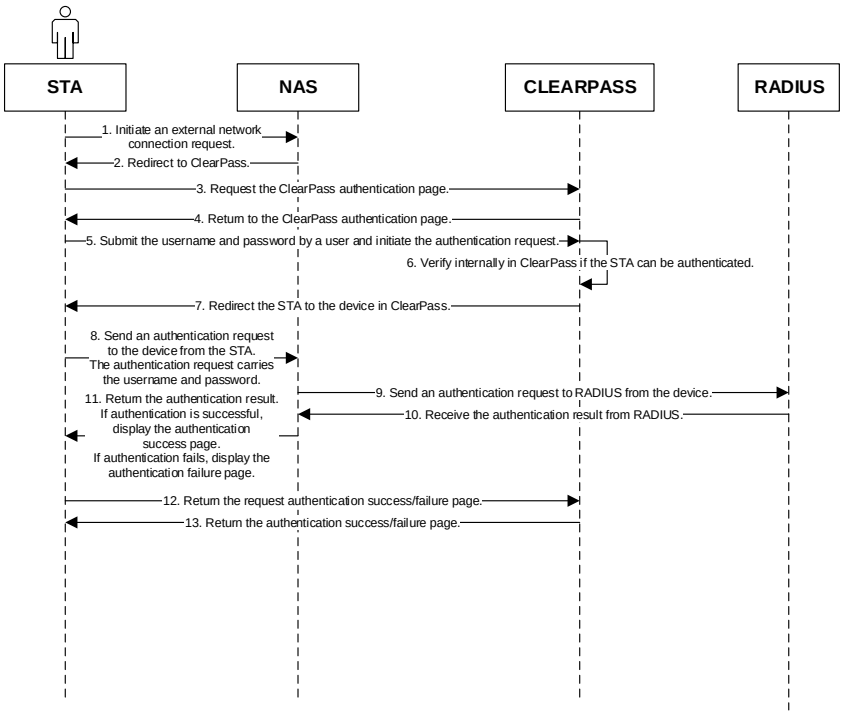
1 Before authentication, the device intercepts all HTTP requests sent by a non-authenticated user and redirects them to the portal server. Then an authentication page pops up on the browser of the user.

2 The user enters authentication information including the username, password, and verification code on the authentication page for the browser to interact with the portal server.

3 The portal server validates user information in the background. If authentication fails, the server returns a failure page to the client. Otherwise, the client is redirected to the network device.

4 Upon receiving the request from the authentication client, the network device verifies information with the portal server, and redirects the client to a page of the portal server based on the verification result.

Figure 1-7 ClearPass Authentication Process



User logout process:

There are two scenarios of client logout. In the first scenario, the NAS detects that a client has gone offline due to reasons such as reaching the maximum online time, exceeding the traffic limit, or experiencing a disconnection in the link. The second scenario occurs when a client has initiated logout by clicking the logout button on the logout page.

1 The client clicks the logout button on the web page, selects logout, and initiates logout requests to the portal server and network device simultaneously or at different time points, depending on the implementation of the portal server.

2 The NAS disconnects a client with traffic lower than the threshold based on parameters of user online traffic detection.

Related Configuration

Creating a ClearPass Template

By default, a ClearPass template is not configured.

Run the **web-auth template** { **cpweb** | *template-name* **cpweb** } command in global configuration mode to create a ClearPass template.

You can use the ClearPass template for web-based authentication.

Configuring Server IP Address

By default, the server IP address is not configured.

Run the **ip** *ip-address* command in template configuration mode to configure the server IP address.

Server access requests are allowed by the device and rate limiting can be performed on requests transmitted to the server.

Configuring Server Authentication URL

By default, the server authentication URL is not configured.

Run the **url** *url-string* command in template configuration mode to configure the URL that users will be redirected to. Typically, the portal authentication page is used.

Configuring a Response Mode After Successful Authentication

By default, the response mode is to return a page with a success message (msg mode).

Run the **login-success response** { **redirect-init-url** [**default-url** *url-string*] **| msg** *msg-string* | **redirect-url** *url-string* } command in template configuration mode to configure one of the following three response modes:

- redirect-init-url: Redirects users back to the initially accessed page, depending on the URL provided by the server. You can specify the default URL when the server does not provide a URL.
- msg: Returns a page with a specified message after successful authentication.
- redirect-url: Redirects users to a specified page after successful authentication.

Configuring a Response Mode Upon an Authentication Failure

By default, the response mode is to redirect users to the login page upon an authentication failure.

Run the **login-fail response** { **redirect-login-url** | **redirect-url** *url-string* [**errmsg-key** *key-string*] **| msg** *msg-string* } command in template configuration mode to configure one of the following three response modes:

- redirect-login-url: Redirects users back to the login page upon an authentication failure.
- redirect-url: Redirects users to a specified URL upon an authentication failure. The parameter name for error messages can be configured.

- msg: Returns a page with a specified message upon an authentication failure.

Configuring a Mode for the Device to Resolve Authentication Requests

By default, authentication paramters include username, password, and URL.

By default, passwords are not in cleartext mode and not encrypted.

Run the **http-method post** [**username-key** *key-string*] [**password-key** *key-string*] [**init-url-key** *key-string*] [**password-encrypt** { **none** | **uam** }] command in template configuration mode to configure a mode for the device to resolve authentication requests on a device.

uam: Uses ASCII to encrypt passwords.

Configuring Whether to Display a Window for Proactive Logout After Successful Authentication

NBy default, no window for proactive logout is displayed.

Run the **logout-popup-window** command in template configuration mode to configure the window for proactive logout to be displayed.

Configuring the IP Address of the NAS

By default, the device's IP address is not configured.

Run the **web-auth auth-server ip** *ip-address* command in global configuration mode to configure the IP address of the NAS.

Set the access service IP address of the device for ClearPass, which is used for communication from the server to the IP address.

The access service IP address of the NAS cannot be set to a passthrough address.

When the access service IP address is configured as the IP address of the NAS and a STA in the authentication template accesses this IP address, the NAS intercepts the request of the STA and forwards it to the server. As a result, the STA fails to access the web management page of the NAS.

If a STA in the authentication template accesses this IP address for device management, configure the access service IP address as the unused virtual service IP address, for example, 1.1.1.1 and 2.2.2.2.

If the actual IP address of a device is used to log in to the device, there are security issues. In this case, the IP address for device management is mapped to the extranet IP address. Security devices such as firewalls are deployed between the extranet and servers to ensure security, whereas no security measures are taken for access through the intranet. If the actual IP address of the device is visible, the device can be easily attacked. The virtual IP address is recommended.

Configuring the Port of the NAS

By default, the port of the NAS is not configured.

Run the **web-auth auth-server http** [***port***] command in global configuration mode to configure the port of the NAS. Then the device will start listening on this port.

The port is used by ClearPass for listening, and a STA will initiate HTTP requests to this port during authentication.

Configuring the URL for Initiating Authentication from a STA

By default, the URL is http://ip:port/login.

Run the **web-auth auth-server submit-url** command in global configuration mode to configure the URL.

The URL is used by ClearPass for STAs to initiate authentication, and must start with **http://** and cannot contain question marks (?). It must be consistent in ClearPass.

Submitting authentication information to this URL will trigger an authentication request.

Enabling AAA Authentication

By default, AAA authentication is disabled.

Run the **aaa new-model** command in global configuration mode to enable AAA authentication.

ClearPass authentication relies on AAA authentication, so AAA authentication must be enabled when ClearPass is used.

Configuring the RADIUS Server and Communication Key

By default, the RADIUS server and communication key are not configured.

Run the **radius-server host** command in global configuration mode to configure the RADIUS server and communication key.

The RADIUS server is used for web-based authentication.

Configuring the Method List for Web-based Authentication of the AAA Module

By default, the method list for web-based authentication of the AAA module is not configured.

Run the **aaa authentication cpweb** command in global configuration mode to configure the authentication method for second-generation web-based authentication.

Web-based authentication can be configured to use this method list for authentication interaction.

Configuring the Method List for Network Accounting of the AAA Module

By default, the method list for network accounting of the AAA module is not configured.

Run the **aaa accounting network** command in global configuration mode to configure the network accounting method.

Web-based authentication can be configured to use this method list for accounting interaction.

Configuring the AAA Authentication Method List Name for Web-based Authentication

By default, the default method is used.

Run the **web-auth authentication cpweb** command in global or WLAN security configuration mode to configure the method list name.

Web-based authentication initiates authentication requests to AAA authentication using this method list name.

Configuring the AAA Accounting Method List Name for Web-based Authentication

By default, the default method is used.

Run the **web-auth accounting cpweb** command in global or WLAN security configuration mode to configure the method list name.

Web-based authentication sends accounting requests to AAA authentication using this method list name.

Enabling Web-based Authentication

By default, web-based authentication is disabled.

Run the **webaut** command in interface configuration mode to enable web-based authentication on the port connected to STAs.

After authentication is enabled, non-authenticated users on the port will be redirected to the authentication page.

1.4 Configuration

Configuration	Description and Command	
Configuring First-Generation Web-based Authentication	⚠ (Mandatory) It is used to set basic parameters of Ruijie first-generation web-based authentication.	
	web-auth template eportalv1	Configures the web-based authentication template.
	ip *ip-address*	Configures the IP address of the portal server.
	context	Configures the context ID and IP address of the hot standby server.
	url *url-string*	Configures the web-based authentication URL of the portal server.
	fmt { **ace** | **default** }	Configures the URL format of the portal server.
	bindmode { **ip-mac-mode** | **ip-only-mode** }	Configures a binding mode.
	redirect { **http** | **js** }	Configures a redirection mode.
	web-auth portal key [**0** | **1** | **7**] *key-string*	Configures the web-based authentication 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.
	snmp-server enable traps web-auth	Enables the SNMP server Trap/Inform function.
	webauth	Enables web-based authentication on an interface.
Configuring Second-Generation Web-based Authentication	⚠ (Mandatory) It is used to set basic parameters of Ruijie second-generation web-based 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 and communication key.

	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for web-based authentication. (RADIUS authentication is implemented.)
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for web-based accounting. (RADIUS accounting is implemented.)
	web-auth template { **eportalv2** | *portal-name***v2** }	Configures a web-based authentication template.
	ip *ip-address*	Configures the IP address of the portal server.
	context	Configures the context ID and IP address of the hot standby server.
	url *url-string*	Configures the web-based authentication URL of the portal server.
	fmt { **cmcc-ext1** | **cmcc-ext2** | **cmcc-mtx** | **cmcc-normal** | **cmcc-ext3** | **ct-jc** | **cucc** | **default** | **custom** }	Configures the URL format of the portal server.
	bindmode { **ip-mac-mode** | **ip-only-mode** }	Configures a binding mode.
	redirect { **http** | **js** }	Configures a redirection mode.
	pack-attr { **session-id** | **bas-ip** | **nas-id** } **position first**	Configures a specific attribute at the beginning of a Portal packet.
	web-auth portal key [**0** | **1** | **7**] *key-string*	Configures the web-based authentication communication key.
	webauth	Enables second-generation web-based authentication on an interface.
Configuring iPortal Web-based Authentication	⚠ (Mandatory) It is used to set basic parameters of Ruijie iPortal web-based 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 and communication key.
	aaa authentication iportal { **default** | *list-name* } *method1* [*method2*...]	Configures an AAA method list for Ruijie iPortal web-based authentication. (RADIUS authentication is implemented.)

	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures an AAA method list for Ruijie iPortal web-based accounting. (RADIUS accounting is implemented.)
	web-auth template iportal	Configures the iPortal web-based authentication template.
	login-popup *url-string*	Configures the advertisement pushing URL before authentication.
	online-popup url-string	Configures the advertisement pushing URL after successful authentication.
	page-suit *filename*	Configures the custom page suite.
	time-interval *hour*	Configures the built-in advertisement pop-up interval.
	webauth	Enables Ruijie iPortal web-based authentication on an interface.
Configuring MAC Address-Based SMS Authentication	(Mandatory) It is used to set 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 and communication key.
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures the accounting method list.
	aaa authentication web-auth { **default** | *list-name* } *method1* [*method2*...]	Configures the web-based authentication method list.
	web-auth template { **eportalv2** | *portal-name* **v2** }	Configures a web-based authentication template.
	ip { *ip-address* | *ipv6-address* }	Configures the server IP address.
	url *url-string*	Configures the server URL.
	fmt { **cmcc-ext1** | **cmcc-normal** | **default** }	Configures the URL format of the portal server.
	web-auth portal key *key-string*	Configures the encryption key of the server.
	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 WiFiDog Authentication	(Mandatory) It is used to set 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 web-based authentication URL of the portal server.
	nas-ip *ip-address*	Configures the IP address of the NAS.
	web-auth sta-perception enable	Configures WiFiDog MAB authentication.
	gateway-id *string*	Configures the gateway ID.
	web-auth portal wifidog	Specifies a WiFiDog authentication template.
	webauth	Enables web-based authentication.
Configuring WeChat Web-based Authentication	(Mandatory) It is used to set basic parameters of WeChat authentication.	
	web-auth template { **wechat** | *portal-name* **wechat** }	Configures a WeChat web-based authentication template.
	ip *ip-address*	Configures the IP address of the portal server.
	service-url *url-string*	Configures the WeChat web-based authentication URL.
	url *url-string*	Configures the authentication page URL of the portal server.
	key *key-string*	Configures the encryption key of the portal server.
	nas-ip *ip-address*	Configures the access service IP address of the NAS.
	web-auth sta-perception enable	Configures WeChat web-based authentication.
	web-auth wechat-escape interval *minutes*	Configures the escape function.
	web-auth wechat-check interval *minutest*	Configures server detection.
	web-auth valid-ip-acct [**timeout** *seconds*]	Configures IP check.

	web-auth portal wechat	Specifies a WeChat web-based authentication template.
	webauth	Enables web-based authentication.
Configuring ClearPass Authentication	(Mandatory) It is used to configure basic parameters of WeChat Wi-Fi 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 and key.
	aaa authentication cpweb { **default** | *list-name* } *method1* [*method2*...]	Configures the method list for web-based authentication (using RADIUS authentication).
	aaa accounting network { **default** | *list-name* } **start-stop** *method1* [*method2*...]	Configures the method list for network accounting (using RADIUS accounting).
	web-auth template cpweb	Creates a ClearPass authentication template.
	ip *ip-address*	Configures the IP address of the server.
	context	Configures the context ID and IP address of the hot standby server.
	url *url-string*	Configures the URL of the server.
	login-success response { **redirect-init-url** [**default-url** *def-string*] | **msg** *msg-string* | **redirect-url** *url-string* }	Configures a response mode after successful authentication.
	login-fail response { **redirect-login-url** | **redirect-url** *url-string* [**errmsg-key** *key-string*] | **msg** *msg-string* }	Configures a response mode upon an authentication failure.
	http-method post [**username-key** *key-string*] [**password-key** *key-string*] [**init-url-key** *key-string*] [**password-encrypt** { **none**|**uam** }]	Configures a mode for the device to resolve authentication requests.
	logout-popup-window	Configures whether to pop up a window to actively go offline after successful authentication.
	web-auth auth-server ip *ip-address*	Configures the IP address of the device.
	web-auth auth-server http [*port*]	Configures the port of the device.
	web-auth auth-server submit-url *url-string*	Configures the URL for STAs to initiate authentication.

	webauth	Enables web-based authentication.
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-based authentication and Ruijie iPortal web-based 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-based authentication and Ruijie iPortal web-based 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 Web-based Authentication Binding Mode	(Optional) It is used to specify the entry binding mode in template configuration mode.	
	bindmode { **ip-mac-mode** | **ip-only-mode** }	Specifies the template binding mode.
Customizing a Page Suite	(Optional) It is used to configure the page suite used by Ruijie iPortal web-based authentication for a template.	
	page-suite *file-name*	Customizes a page suite for Ruijie iPortal web-based authentication.
Customizing a Page Suite	(Optional)	
	N/A	Complies with the page suite specifications.
Configuring the Advertisement Pushing Mode	(Optional) It is used to configure an iPortal web-based authentication advertisement URL in template configuration mode.	
	login-popup *url*	Configures the login pop-up URL.

	online-popup *url*	Configures the pop-up URL after successful authentication.
Configuring a Custom URL Format	(Optional) It is used to configure the redirection URL format for a template.	
	fmt custom encry { [**none** | **md5** | **des** | **des_ecb | des_ecb3**] } { [**user-ip** *userip-str*] [**user-mac** *usermac-str* **mac-format** [**dot | line | none | 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 web-based authentication URL.
Configuring the Redirection HTTP Port	(Optional) It is used to configure the TCP interception port for redirection, so that packets on the specified port can be redirected when interception is enabled.	
	http redirect port *port-num*	Configures the redirection TCP port.
Configuring Rate Limiting for Logging in Web-based Authentication	(Optional) It is used to configure the syslog function in web-based authentication.	
	web-auth logging enable *num*	Configures the logging rate limit for web-based authentication.
Configuring the Maximum Number of HTTP Sessions for Non-authenticated 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 non-authenticated clients.
Configuring the HTTP Redirection Timeout	(Optional) It is used to modify the timeout interval for redirection connections. The timeout interval needs to be increased to complete redirection when the network is unstable.	
	http redirect timeout *seconds*	Configures the HTTP redirection timeout interval.
Configuring the Authentication-Free Network Resource	**http redirect direct-site**	Configures the authentication-free network resource.

Configuring the Authentication-Free ARP Resource	(Optional) It is used to permit packets from the specified authentication-free ARP resource. Packets from the gateway ARP resource must be permitted to pass when ARP check is enabled.	
	http redirect direct-arp *ip-address* [*ip-mask*]	Configures the authentication-free ARP resource.
Configuring the Authentication-Free Address Range	(Optional) It is used to configure clients to access the Internet without authentication.	
	web-auth direct-host *ipv4-address* [*ip-mask*] [**arp**] [**port** *interface-name*]	Configures the range of IP or MAC addresses of clients without 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 Server Detection	(Optional) It is used to detect availability of the portal server. If it is unavailable, services are switched to the standby portal server. The active and standby portal servers must be configured.	
	web-auth portal-check [**interval** *intsec* [**timeout** *tosec*] [**retransmit** retries]	Configures the portal server detection interval, timeout interval, and timeout retransmission count.
	web-auth ping [**interval** *minutes*] [**retry** *times*]	Configures the ping detection interval and timeout retransmission count.
Configuring Portal Escape	(Optional) It is used to allow new clients to access the Internet without authentication when the portal server is unavailable.	
	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 anti-jitter. This prevents web-based authentication entries from being deleted when a link of a 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 an Allowlist and a Blocklist	(Optional) It is used to configure a blocklist to prevent authenticated clients from accessing some network resources, and to configure an allowlist to allow non-authenticated clients to access some network resources.	
	web-auth acl	Configures an allowlist and a blocklist.
Configuring Anti-jitter Accounting	(Optional) It is used to configure whether the anti-jitter duration is included into the online duration, in order to improve accounting precision. The anti-jitter duration depends on the anti-jitter 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 Source Port for Communication with the Portal Server	(Optional) It is used to configure the source port used for communication between the NAS and portal server.	
	ip portal source-interface *interface-type interface-num*	Specifies the port used for communication between the NAS and portal server.
Configuring the Anti-Noise Function	(Optional) Packets sent to the configured IP address and port will not be filtered by the device enabled with the noise reduction function.	
	web-auth anti-noise ip *ip-addr* **port** *port*	Configures the specified IP address and port, so that the corresponding packets will not be filtered by the device enabled with the anti-noise function.
Configuring an NDKEY-Compatible Web-based Authentication URL	(Optional) It is used to configure the web-based authentication URL used in web-based authentication to support the Shanghai NDKEY system.	
	web-auth dkey-compatible url-parameter *string*	Configures compatibility between the Shanghai NDKEY system and redirection web-based authentication URL.

Configuring Multi-Portal Mapping	**web-auth portal** { **eportalv2** | **eportalv1** | **iportal** | *name* } **ip-mapping** *ipv4 mask*	Configuring Multi-Portal Mapping
Enabling NAT for Ruijie iPortal Web-based Authentication	⚠ (Optional) It is used to configure Ruijie iPortal web-based authentication to support Network Address Translation (NAT).	
	iportal nat enable	Enables NAT for Ruijie iPortal web-based authentication.
Configuring the iPortal HTTP Retransmission Count	⚠ (Optional) It is used to configure the iPortal HTTP retransmission count.	
	iportal retransmit *count*	Configures the iPortal HTTP retransmission count.
Configuring Service Selection in Ruijie iPortal Web-based Authentication	⚠ (Optional) It is used to configure the service type used by Ruijie iPortal web-based authentication.	
	iportal service { **internet** *internet-name* | **local** *local-name* }	Configures the service type used by Ruijie iPortal web-based authentication.
Configuring the UA Field for iPortal Web-based Authentication User	⚠ (Optional) It is used to configure STA name corresponding to the UA field of the user.	
	iportal user-agent *ua-name* **type mobile** *ua-string*	Configures the STA name corresponding to the UA field of the user.
Customizing a Page Suite for Ruijie iPortal Web-based Authentication	**web-auth import-page-suite tftp:***path*	Imports a page suite for Ruijie iPortal web-based authentication.
Configuring the Accounting Method List of Web-based Authentication	⚠ (Optional) It is used to configure an accounting method for web-based authentication in global configuration mode.	
	web-auth accounting { **v2** | **intra** | **cpweb** } { **default** | *name* }	Configures an accounting method for web-based authentication in global configuration mode.
Configuring a Web-based Authentication Method List	⚠ (Optional) It is used to configure a web-based authentication method in global configuration mode.	
	web-auth authentication { **v2** | **intra** | **cpweb** } { **default |** *name*}	Configures a web-based authentication method in global configuration mode.
Configuring Upgrade Compatibility	**http redirect** *ip-address*	Configures the IP address of the portal server for first-generation web-based authentication.
	⚠ (Optional)	

Configuring RADIUS Authentication Escape	**web-auth radius-escape**	Configures RADIUS authentication escape.
Configuring Built-in Logo Replacement	**web customized-logo enable**	Configures the logo replacement function for iPortal web-based authentication.
Configuring Noise Reduction in Wireless Web-based Authentication	**web-auth noise** [**aging** *agmin*] [**hit** *times*]	Configures the anti-noise reduction policy for wireless web-based authentication.
Enabling iOS Automatic Pop-up Window Control in WeChat Web-based Authentication	**http redirect adapter ios**	Enables iOS automatic pop-up window control in WeChat authentication.
Enabling Smart WeChat Web-based Authentication	**web-auth sta-perception enable**	Enables MAB authentication for WeChat authentication.
Enabling IPFIX Traffic Upload	**web-auth acct-mtehod ipfix**	Enables IPFIX traffic upload.
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 Configuration Through WeChat	(Optional) It is used to enable one-click wireless configuration through Wechat connection to Wi-Fi.	
	web-auth wechat-template wlan-range portal-ip nas-ip [**ios-adapter** | **perception**]	Enables one-click wireless configuration through WeChat connection to Wi-Fi.
Configuring NAS-PORT-ID for an AP	**nas-port-id** *string*	Configures NAS-PORT-ID for an AP.
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.
Configuring the App Authentication Template	**web-auth template** { **app** | *portal-name* **app** }	Creates an app authentication template.
	web-auth portal { **app |** *name* }	Applies an app authentication template.
Configuring ISE Authentication	(Mandatory) It is used to configure Identity Service Engine (ISE) authentication parameters.	

	aaa new-model	Enables AAA.
	aaa authentication cpweb { **default** | *list-name* } *method1* [*method2*...]	Configures the web-based authentication method list (ClearPass authentication).
	web-auth template cpweb	Creates a template (ClearPass authentication).
	ip *ip-address*	Configures the IP address of the ISE server.
	url *url-string*	Configures the Uniform Resource Locator (URL) of the ISE server.
	web-auth auth-server ip *ip-address*	Configures the access service IP address of the device that performs ISE authentication.
	web-auth auth-server http [*port*]	Configures the TCP port used by a STA for initiating ISE authentication.
	web-auth auth-server submit-url *url-string*	Configures the URL used by a STA for initiating ISE authentication.
	webauth	Enables web-based authentication on an interface.
Configuring the Role-based Portal Redirection Template	**web-auth template** *template-name* **rdweb**	Creates a template.
	ip *ip-address*	Configures a Server IP Address.
	url *url-string*	Configures a Server URL.
Configuring the Default Role upon Authentication Success	**web-auth default-role** *name*	Configures the default client role after the web authentication succeeds.
Configuring Second-Generation Web-based Authentication to Support Direct Access to the Authentication Page	⚠ (Optional) It is used to configure second-generation web-based authentication to support direct access to the authentication page for authentication.	
	web-auth portal direct-auth	Configures second-generation web-based authentication to support direct access to the authentication page for authentication.
Importing and Enabling an SSL Certificate	**web-auth import-ssl** [**auth-server**] { **cert ftp:***path* | **cert tftp:***path* } { **key ftp:***path* | **key tftp:***path* }	IImports a Secure Sockets Layer (SSL) certificate.

	web-auth ssl-policy { **https-redirect** | **auth-server** }	Enables an SSL certificate.
Configuring the Lowest TLS Version	**web-auth ssl-minimum-version tls1.2**	Sets the lowest TLS version for interaction between the device and STA to TLS 1.2.

1.4.1 Configuring First-Generation Web-based Authentication

Configuration Effect

Redirect non-authenticated clients to the web-based authentication URL to perform authentication.

Notes

N/A

Configuration Steps

Configuring the Portal Server

- Mandatory. To enable web-based authentication successfully, you must configure and apply the portal server.
- When the NAS or aggregation device finds a non-authenticated client attempting to access network resources through HTTP, the device redirects the access request to the specified web-based authentication URL. Then the client can initiate authentication to the portal server through this URL. If the IP address of the portal server is configured as an authentication-free network resource, non-authenticated clients can directly visit this IP address through HTTP.

Configuring the Communication Key Between the NAS and Portal Server

- Mandatory. To enable web-based authentication successfully, you must configure the key used for communication between the NAS or aggregation device and portal server.
- When the NAS finds a non-authenticated client attempting to access network resources through HTTP, the device redirects the access request to the specified web-based authentication URL. Then the client can initiate authentication to the portal server through this URL. During authentication, 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-based authentication successfully, you must set SNMP management parameters used for communication between the NAS and portal server.
- The access or aggregation device and portal server manage authenticated clients through SNMP or MIB. The MIB is used to manage a table of authenticated clients on the NAS. The portal server accesses the MIB to obtain client statistics so as to control client login and logout. When a client logs out, the NAS or aggregation device will inform the portal server by sending SNMP-Inform packets.

Enabling Ruijie First-Generation Web-based Authentication on an Interface

- Mandatory.

- When first-generation web-based authentication is enabled in WLAN security configuration mode, web-based authentication is not enabled on any port by default. The users connecting to the port do not need to perform web-based authentication.

Verification

- Verify that non-authenticated clients are required to perform authentication.
- Verify that authenticated clients can access the Internet normally.

Related Commands

Creating a Web-based Authentication 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-based 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	Web-based authentication template configuration mode
Usage Guide	N/A

Configuring the Context ID and IP Address of the Hot Standby Server

Command	**context** *ctx-id peer-ip-address*
Parameter Description	*ctx-id*: Configures the context ID of the hot standby server. *peer-id-address*: Configures the IP address of the hot standby server.
Command Mode	Web authentication template configuration mode
Usage Guide	N/A

Configuring the Web-based Authentication URL of the Portal Server

Command	**url** *url-string*
Parameter Description	*url-string*: Indicates the Web-based authentication URL of the portal server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring the URL Format of the Portal Server

Command	**fmt** { **ace** | **default** }

Parameter Description	Indicates the URL format of the portal server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	When the **fmt** parameter is set to **ace**, association with ACEs is supported.

Specifying the Web-based Authentication Binding Mode

Command	**bindmode** { **ip-mac-mode** | **ip-only-mode** }
Parameter Description	Indicates the web-based authentication binding mode.
Command Mode	Web-based authentication 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	Web-based authentication template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

Configuring the Web-based Authentication Communication Key

Command	**web-auth portal key** [**0** | **1** | **7**] *key-string*
Parameter Description	**0**: Configures the server key encryption type as cleartext, that is, the server key is input, saved, and displayed in cleartext. **1**: Configures the server key encryption type to ciphertext storage, that is, the cleartext input and ciphertext storage and display. **7**: Configures the server key encryption type as full ciphertext, that is, ciphertext input, ciphertext storage, and ciphertext display. *key-string:* Indicates the web-based authentication communication key used for 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**: Is used for read and write operations required by the Set operation in the MIB.
Command Mode	Global configuration mode

Usage Guide	The SNMP server community string is used by the portal server to manage online clients on the NAS or aggregation device.

Configuring the SNMP Server

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, that is, 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 to receive web-based authentication messages, including the type, version, community string, and other parameters. **inform:** Enables the SNMP Inform function. The NAS or aggregation 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 that later versions of SNMPv2 support SNMP Inform. It cannot be set to SNMPv1. **web-auth**: Indicates the preceding parameters to be used for web-based authentication. For details about SNMP configuration, see *Configuring SNMP*. SNMPv2 is used as an example here. SNMPv3 is recommended if higher security is required for 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 *Configuring SNMP*.

Enabling the Device to Send Trap or Inform Messages for Web-based Authentication

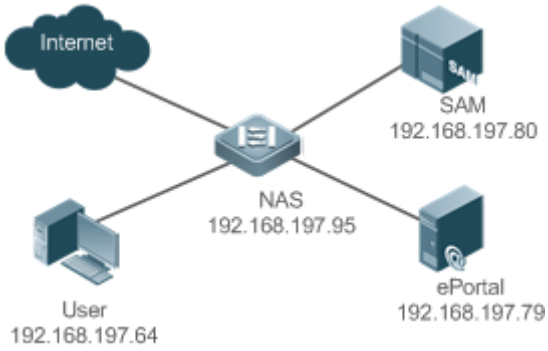
Command	**snmp-server enable traps web-auth**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the NAS or aggregation device to send Trap and Inform messages for web-based authentication. web-auth: Indicates web-based authentication messages.

Enabling Ruijie First-Generation Web-based Authentication on an Interface

Command	**webauth**
Parameter Description	N/A
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Configuring First-Generation Web-based Authentication

Scenario **Figure 1-8**	
Configuration Steps	● On the NAS, configure the IP address of the ePortal server and the key (webkey) used for communicating with the ePortal server. ● Configure the web-based authentication URL on the NAS. ● Set SNMP parameters (community string: public) used for communication between the NAS and ePortal server. ● Enable web-based authentication on the WLAN of 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-based 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
```

Common Errors

- SNMP parameters used for communication between the portal server and NAS are configured incorrectly, causing authentication failures.
- Specify the IP-MAC binding mode to deploy web-based authentication across the Layer 3 network, causing authentication failures.
- When web-based authentication is used 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-based Authentication

Configuration Effect

Redirect non-authenticated clients to the web-based authentication URL to perform authentication.

Notes

- Second-generation web-based authentication complies with *CMCC WLAN Service Portal Specification*. Furthermore, it is extended to support Ruijie portal server. Perform compatibility configuration based on the server performance in actual deployment.
- 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. In addition, the **fmt** configuration is not supported in the IPv6 template.
- 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-based authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in Ruijie second-generation web-based authentication.

Configuring the RADIUS Server and Communication Key

- Mandatory. To enable Ruijie second-generation web-based 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-based Authentication

- Mandatory. To enable Ruijie second-generation web-based authentication, you must configure an AAA authentication method list.
- An AAA authentication method list associates web-based 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-based Accounting

- Mandatory. To enable Ruijie second-generation web-based authentication, you must configure an AAA method list for web-based accounting.
- An accounting method list is used to associate an accounting method and server. In web-based authentication, accounting is implemented to record client fees.

Configuring the Portal Server

- Mandatory. To enable Ruijie second-generation web-based authentication, you must configure and apply the portal server.
- When the NAS or aggregation device finds a non-authenticated client attempting to access network resources through HTTP, it redirects the access request to the specified web-based authentication 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, non-authenticated 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-based authentication, you must configure the key used for communication between the NAS or aggregation device and portal server.
- When the NAS finds a non-authenticated client attempting to access network resources, it redirects the client to the specified web-based authentication URL, where the client can initiate authentication to the portal server. During authentication, 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-based 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-based authentication is enabled in interface configuration mode, web-based authentication is not enabled on any port by default. The users connecting to the port do not need to perform web-based authentication.

Verification

- Check whether non-authenticated 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 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. *port-number1:* Indicates the authentication port. *port-number2:* Indicates the accounting port. *string*: Indicates the key string.
Command Mode	Global configuration mode
Usage Guide	By default, the authentication port number is 1812 and the accounting port number is 1813.

Configuring an AAA Method List for Web Authentication

Command	**aaa authentication web-auth** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Creates a method list. *method1*: Configures method 1. *method2*: Configures method 2.
Command Mode	Global configuration mode
Usage Guide	Ruijie second-generation web-based authentication adopts RADIUS authentication.

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-based authentication adopts RADIUS accounting.

Configuring the Second-Generation Web-based Authentication 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-based 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	Web-based authentication template configuration mode
Usage Guide	N/A

Configuring the Context ID and IP Address of the Hot Standby Server

Command	**context** *ctx-id peer-ip-address*
Parameter Description	*ctx-id*: Configures the context ID of the hot standby server. *peer-id-address*: Configures the IP address of the hot standby server.
Command Mode	Web authentication template configuration mode
Usage Guide	N/A

Configuring the Web-based Authentication URL of the Portal Server

Command	**url** *url-string*
Parameter Description	Indicates the web-based authentication URL of the portal server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Configuring the Format of the Web-based Authentication URL

Command	**fmt** { **cmcc-ext1** | **cmcc-ext2** | **cmcc-mtx** | **cmcc-normal** | **ct-jc** | **cucc** | **default** | **custom** }
Parameter Description	Indicates the format of the web-based authentication 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** parameter 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 China Telecom. The **cucc** format is supported for Shandong China Telecom.

Configuring a User Binding Mode

Command	**bindmode** { **ip-mac-mode** | **ip-only-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	Web-based authentication template configuration mode
Usage Guide	For JavaScript-incapable Apps, you need to specify the HTTP encapsulation format to trigger redirection.

Configuring a Specific Attribute at the Beginning of a Portal Packet

Command	**pack-attr** { **session-id** | **bas-ip** | **nas-id** } **position first**
Parameter Description	**session-id**: Configures the session ID attribute at the beginning of a Portal packet. **bas-ip**: Configures the BAS IP attribute at the beginning of a Portal packet. **nas-id**: Configures the NAS ID attribute at the beginning of a Portal packet.
Command Mode	Second-generation web authentication template configuration mode
Usage Guide	

Configuring the Web-based Authentication Communication Key

Command	**web-auth portal key** [**0** | **1** | **7**] *key-string*
Parameter Description	**0**: Configures the server key encryption type as cleartext, that is, the server key is input, saved, and displayed in cleartext. **1**: Configures the server key encryption type to ciphertext storage, that is, the cleartext input and ciphertext storage and display. **7**: Configures the server key encryption type as full ciphertext, that is, ciphertext input, ciphertext storage, and ciphertext display. *key-string*: Indicates the Web-based authentication 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

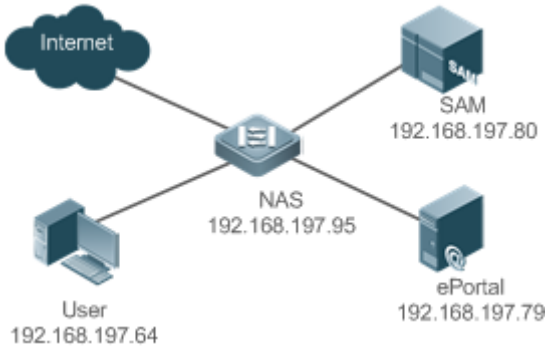
Enabling Ruijie Second-Generation Web-based Authentication

Command	**webauth**

Parameter Description	N/A
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Configuring Second-Generation Web-based Authentication

Scenario **Figure 1-9**	
Configuration Steps	● Enable AAA on the NAS. ● Configure the RADIUS server and communication key on the NAS. ● Configure the default AAA method lists for web-based authentication and accounting on the NAS. ● Configure the IP address of the portal server and the web-based authentication communication key (webkey) used for communicating with the portal server on the NAS. ● Configure the web-based authentication URL on the NAS. ● Configure Ruijie second-generation web-based authentication in global configuration mode on the NAS. ● Enable web-based authentication on the WLAN.

	`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)#exit`

	Hostname(config)# wlansec 1 Hostname(config-wlansec)# web-auth portal eportalv2 Hostname(config-wlansec)# webauth Hostname(config-wlansec)# exit
Verification	● Check whether web-based 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 webkey ... 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 *CMCC WLAN Service Portal Specification*, causing compatibility failures.

1.4.3 Configuring iPortal Web-based Authentication

Configuration Effect

Redirect non-authenticated clients to the web-based authentication URL to perform authentication. No external portal server is required.

Notes

- Some devices, such as AP110, 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 device, see the corresponding product description.
- Ruijie iPortal web-based authentication is configured on EG devices in global configuration mode.
- The customized page suite must comply with the relevant specification.

Configuration Steps

↘ Enabling AAA

- Mandatory. To enable Ruijie second-generation web-based authentication, you must enable AAA.
- The iPortal NAS is responsible for initiating authentication to the portal server through AAA in Ruijie iPortal web-based authentication.

↘ Configuring the RADIUS Server 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 Ruijie iPortal Web-based Authentication

- Mandatory. To enable Ruijie iPortal web-based 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 Ruijie iPortal Web-based Accounting

- Optional. Some servers require that authentication and accounting be enabled. Configure web-based accounting based on characteristics of the server in use.
- An AAA accounting method list associates an accounting method and server. In web-based authentication, accounting is implemented to record client fees.

↘ Configuring the iPortal Web-based Authentication 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 Ruijie iPortal Web-based Authentication Globally or on an Interface

- Mandatory.

Verification

- Check whether non-authenticated clients are redirected to the web-based authentication URL to perform authentication, and the web-based authentication 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 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. *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-based 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-based 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 Web-based Authentication Template

Command	**web-auth template iportal**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the Advertisement Mode Before Authentication

Command	**login-popup** *url-string*
Parameter Description	Indicates the advertisement URL.
Command Mode	Web-based authentication template configuration mode
Usage Guide	The URL starts with **http://** or **https://**.

Specifying the Advertisement Mode After Authentication

Command	**online-popup** url-string
Parameter Description	Indicates the advertisement URL.
Command Mode	Web-based authentication 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	Web-based authentication template configuration mode
Usage Guide	N/A

Configuring the iPortal Advertisement Interval

Command	**time-interval** *hour*
Parameter Description	Indicates the advertisement interval.
Command Mode	Web-based authentication template configuration mode
Usage Guide	N/A

Enabling Ruijie iPortal Web-based Authentication

Command	**webauth**
Parameter Description	N/A
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Configuring Ruijie iPortal Web-based Authentication

Configuration Steps	● Enable AAA on the NAS. ● Configure the RADIUS server and communication key on the NAS. ● Configure the default AAA authentication and accounting method lists on the NAS. ● Configure iPortal web-based authentication globally on the NAS. ● Enable web-based authentication on the WLAN 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 iportal default group radius Hostname(config)#aaa accounting network default start-stop group radius
	Hostname(config)#web-auth template iportal
	Hostname(config.tmplt.iportal)#exit
	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 Hostnameconfig-wlansec)# webauth
Verification	● Check whether Ruijie iPortal web-based 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 Hostname ... 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 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 MAC Address-Based SMS Authentication

Configuration Effect

Allow non-authenticated STAs connected to the WLAN to access network resources. When a STA uses up the traffic during a given period of time, the NAS initiates a MAC address binding query to the bound portal server. If the STA is bound to a MAC address, the portal server initiates an authentication request. If the STA is not bound to a MAC address, the STA needs to perform authentication on the portal server before accessing the Internet.

Notes

The configured URL of the portal server must adopt the **cmcc-ext1** format.

Configuration Steps

↘ Enabling AAA

- Mandatory. To enable Ruijie second-generation web-based authentication, you must enable AAA.
- The NAS is responsible for initiating authentication to the portal server through AAA in Ruijie second-generation web-based 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 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. *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-based Authentication

- Mandatory. To enable Ruijie second-generation web-based authentication, you must configure an AAA authentication method list on the AAA module.
- A web-based authentication method list associates web-based 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-based authentication adopts RADIUS authentication.

Configuring an AAA Method List for Web-based Accounting

- Mandatory. To enable Ruijie second-generation web-based 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-based 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	Ruijie second-generation web-based authentication adopts RADIUS accounting.

Configuring the Second-Generation Web-based Authentication Template

- Mandatory. To enable second-generation web-based authentication, you must configure and apply the portal server.

- When the NAS or aggregation device finds a non-authenticated client attempting to access network resources through HTTP, it redirects the access request to the specified web-based authentication 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, non-authenticated 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-based 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	Web-based authentication template configuration mode
Usage Guide	N/A

Configuring the Web-based Authentication URL of the Portal Server

Command	**url** *url-string*
Parameter Description	Indicates the web-based authentication 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 Web-based Authentication URL

Command	**fmt** { **cmcc-ext1** | **cmcc-normal** | **default** }
Parameter Description	Indicates the format of the web-based authentication URL.
Command Mode	Web-based authentication template configuration mode
Usage Guide	**fmt** must be set to **cmcc-ext1**.

Configuring the Web-based Authentication Communication Key

- Mandatory. To enable Ruijie second-generation web-based authentication, you must configure the key used for communication between the NAS or aggregation device and portal server.
- When the NAS finds a non-authenticated client attempting to access network resources, it redirects the client to the specified web-based authentication URL, where the client can initiate authentication to the portal server. During authentication, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

Command	**web-auth portal key** [**0** | **1** | **7**] *key-string*
Parameter Description	**0**: Configures the server key encryption type as cleartext, that is, the server key is input, saved, and displayed in cleartext. **1**: Configures the server key encryption type to ciphertext storage, that is, the cleartext input and ciphertext storage and display. **7**: Configures the server key encryption type as full ciphertext, that is, ciphertext input, ciphertext storage, and ciphertext display. *key-string*: Indicates the web-based authentication communication key used for 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 a 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 a given period of time, 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 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 web-based authentication 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 the **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.

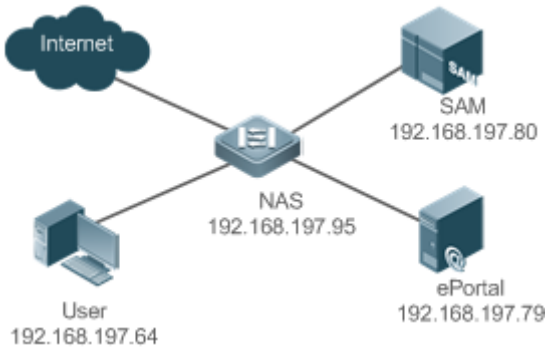
Command	**web-auth wlan-ac-ip** *ipv4*
Parameter Description	*ipv4:* Indicates the **AC IP** field.
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Verification

- Check that non-authenticated 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 and communication key on the NAS. ● Configure the default AAA method lists for web-based authentication and accounting on the NAS. ● Configure the IP address of the portal server and the web-based authentication communication key (webkey) used for communicating with the portal server on the NAS. ● Configure the web-based authentication 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 WLANSEC1 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 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)#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-based 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 ruijie 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 *CMCC WLAN Service Portal Specification*, causing compatibility failures.

1.4.5 Configuring WiFiDog Authentication

Configuration Effect

Redirect non-authenticated clients to the web-based authentication URL to perform authentication.

Notes

N/A

Configuration Steps

Configuring the Portal Server

- Mandatory. To enable web-based authentication, you must configure and apply the portal server.
- When the NAS finds a non-authenticated client attempting to access network resources through HTTP, it redirects the client's access requests to the specified web-based authentication 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. Non-authenticated 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 Web-based Authentication on an Interface

- Mandatory.
- Web-based authentication is not enabled by default. The users connecting to the port do not need to perform web-based authentication.

Verification

- Check whether non-authenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Related Commands

Configuring a WiFiDog Web-based Authentication Template

Command	**web-auth template 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-based authentication template configuration mode
Usage Guide	N/A

Configuring the Web-based Authentication URL of the Portal Server

Command	**url** *url-string*
Parameter Description	Indicates the web-based authentication URL of the portal server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	The URL starts with **http://**.

Configuring the IP Address of the NAS

Command	**nas-ip** *ip-address*
Parameter Description	Indicates the IP address of the NAS.
Command Mode	Web-based authentication template configuration mode
Usage Guide	The access service IP address of the NAS cannot be configured as the passthrough address. When the access service IP address is configured as the IP address of the NAS and a STA in the authentication template accesses this IP address, the NAS intercepts the request of the STA and forwards it to the server. As a result, the STA fails to access the web management page of the NAS. If a STA in the authentication template accesses this IP address for device management, configure the access service IP address as the unused virtual service IP address, for example, 1.1.1.1 and 2.2.2.2.

Configuring WiFiDog MAB Authentication

- Optional.

Command	**web-auth sta-perception enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This function must be used with DHCP snooping.

Configuring the Gateway ID

Command	**gateway-id** *string*
Parameter Description	*string*: Indicates the gateway ID used in WiFiDog. 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. It is mandatory in hot standby and VAC scenarios.

Specifying the WiFiDog Authentication Template

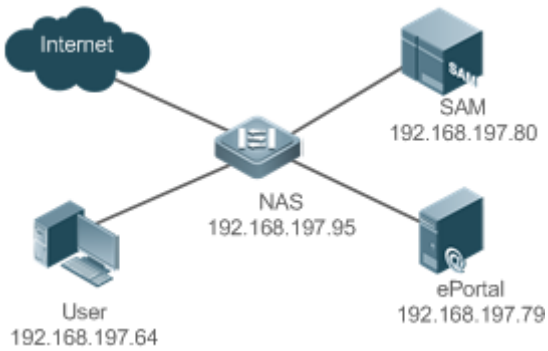
Command	**web-auth portal wifidog**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The default WiFiDog authentication template is **wifidog**.

Enabling WiFiDog Web-based Authentication

Command	**webauth**
Parameter Description	N/A
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Configuring WiFiDog Web-based Authentication

Scenario **Figure 1-11**	
Configuration Steps	● Configure the IP address of the portal server on the NAS. ● Configure the web-based authentication URL on the NAS. ● Configure the IP address used for external communication on the NAS. ● Enable WiFiDog web-based 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-if-range)# webauth Hostname(config-if-range)# exit
Verification	● Check whether WiFiDog web-based 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.

1.4.6 Configuring WeChat Web-based Authentication

Configuration Effect

- Redirect non-authenticated mobile phone users associated with a WLAN 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 non-authenticated mobile phone users to scan a QR code to perform Wi-Fi connection authentication through WeChat.
- Redirect non-authenticated PC users associated with a WLAN 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

N/A

Configuration Steps

Creating a Wechat Web-based Authentication Template

- Mandatory. To enable WeChat web-based 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-based authentication
Command Mode	Global configuration mode
Usage Guide	**wechat** is the name of the default template of WeChat web-based authentication.

Configuring the IP Address of the Portal Server

- (Mandatory) To enable WeChat web-based 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	Web-based authentication template configuration mode
Usage Guide	N/A

Configuring the WeChat Web-based Authentication URL

- (Mandatory) To enable WeChat web-based authentication, you must configure the WeChat web-based authentication URLof the portal server.

Command	**service-url** *url-string*
Parameter Description	Indicates the WeChat web-based authentication URL.
Command Mode	Web-based authentication template configuration mode
Usage Guide	Configure only the domain name. The domain name cannot start with **http://** or **https://**.

Configuring the Authentication Page Address for the Portal Server

- The function is mandatory for devices of 11.1(5)B9 and the default configuration can be used.

Command	**url** *url-string*
Parameter Description	**url**: Indicates the URL of the server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	The authentication page address starts with **http://** or **https://**.

Configuring the Web-based Authentication Communication Key

- (Mandatory) To enable WeChat web-based 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 communication between the NAS and authentication server. The key contains up to 255 characters.
Command Mode	Web-based authentication 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.

Configuring the IP Address of the NAS

Command	**nas-ip** *ip-address*
Parameter Description	Indicates the IP address of the NAS.
Command Mode	Web-based authentication template configuration mode
Usage Guide	The access service IP address of the NAS cannot be configured as the passthrough address. When the access service IP address is configured as the IP address of the NAS and a STA in the authentication template accesses this IP address, the NAS intercepts the request of the STA and forwards it to the server. As a result, the STA fails to access the web management page of the NAS. If a STA in the authentication template accesses this IP address for device management, configure the access service IP address as the unused virtual service IP address, for example, 1.1.1.1 and 2.2.2.2.

Enabling Smart WeChat Web-based Authentication

- Optional.

Command	**web-auth sta-perception enable**
Parameter Description	N/A
Command Mode	Global configuration mode

Usage Guide	Enable smart authentication based on customer's requirements. Run the **ip dhcp snooping** command before smart authentication takes effect.

Enabling the Escape Function

- With the escape function enabled, if the server is unreachable or the server allows STAs to escape, subsequently connected STAs are permitted to pass without authentication. The escape duration is specified by the **interval** *minutes* parameter.
- The configuration in WLAN security configuration mode takes precedence. If this function is not configured in WLAN security configuration mode, the configuration in global configuration mode takes effect.
- To cancel this function, run the **web-auth wechat-escape recover** command in global configuration mode.

Command	**web-auth wechat-escape interval** *minutes*
Parameter Description	*minutes*: Indicates the maximum online time for escape users, in minutes. The default value is 60 minutes.
Command Mode	Global configuration mode and WLAN security configuration mode
Usage Guide	N/A

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, in minutes. There is no default value.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring 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 disconnected forcibly.

Command	**web-auth valid-ip-acct** [**timeout** *seconds*]
Parameter Description	*seconds*: Indicates the time during which STAs can attempt to obtain IP addresses, in seconds. The default value is 30s.
Command Mode	Global configuration mode
Usage Guide	N/A

Specifying the WeChat Web-based Authentication Template

Command	**web-auth portal wechat**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The default WeChat web-based authentication template is **webchat**.

Enabling Web-based Authentication

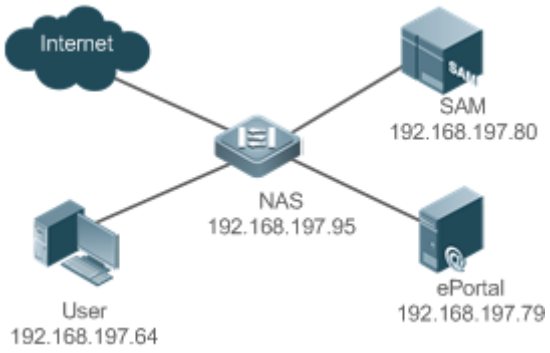
Command	**webauth**
Parameter Description	N/A
Command Mode	WLAN security mode
Usage Guide	N/A

Verification

- Check whether non-authenticated clients are required to perform authentication.
- Check whether authenticated clients can access the Internet normally.

Configuration Example

Configuring WeChat Web-based Authentication

Scenario **Figure 1-12**	
Configuration Steps	● Configure the IP address 192.168.58.110 of the domain name server on the NAS. ● Configure the WeChat web-based authentication template on the NAS. ● Configure the IP address and web-based authentication URL on the NAS. ● Configure the communication key (webkey) used for communicating with the portal server on the NAS. ● Configure the IP address used for external communication on the NAS. ● Apply the template to WLANSEC1 and enable WeChat web-based 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 1.1.1.1
	Hostname(config.tmplt.wechat)#exit
	Hostname(config)# wlansec 1 Hostname(config-wlansec)# web-auth portal wechat Hostname(config-wlansec)# webauth
Verification	● Check whether web-based 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.jsphttp://192.168.197.79:8080 /eportal/index.jsp key ruijie nas-ip 1.1.1.1 !... wlansec 1 web-auth portal wechat webauth !

Common Errors

- The key used for 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 the 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 an allowlist 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 smart authentication during second authentication.

1.4.7 Configuring ClearPass Authentication

Configuration Effect

Redirect non-authenticated clients to the web-based authentication URL to perform authentication.

Notes

N/A

Configuration Steps

Configuring the Portal Server

- Mandatory. To enable web-based authentication, you must configure and apply the portal server.
- When the NAS finds a non-authenticated client attempting to access network resources through HTTP, it redirects the client's access requests to the specified web-based authentication 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. Non-authenticated clients can directly access this IP address through HTTP.

Configuring a Response Mode After Successful Authentication

- Optional.
- It is configured as needed.

Configuring a Response Mode Upon an Authentication Failure

- Optional.
- It is configured as needed.

Configuring a Mode for the Device to Resolve Authentication Requests

- Optional.
- It is configured according to the requirements of the server to be connected.

Configuring Whether to Pop Up a Window for Proactive Logout After Successful Authentication

- Optional.
- It is configured as needed.

Configuring the Device's IP Address

- Mandatory. It is not configured by default.
- This IP address should be configured so that users can access the device.

Configuring the Device's Port

- Mandatory. It is not configured by default.
- This port should be configured for user access and should not conflict with the ports used by built-in web management of the device.

Configuring the URL for Initiating Authentication from a STA

- Optional. The URL is http://*ip*:*port*/login by default, where *ip* is the device IP and *port* is the device port.
- The URL is used for access and should be configured to be consistent with the address configured on ClearPass.

Enabling Web-based Authentication on an Interface

- Mandatory.

- It is used to enable web-based authentication on an interface. Web-based authentication is disabled on an interface by default. In this case, users connected to this interface will not experience web-based authentication.

Verification

- Check whether non-authenticated 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	Commands such as **aaa method-list** can only be entered after AAA is enabled.

Configuring the RADIUS Server and 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 server. *port-number1*: Indicates the authentication port number. *port-number2*: Indicates the accounting port number. *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 the Web-based Authentication Method List on AAA

Command	**aaa authentication cpweb** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Indicates the list name. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	ClearPass authentication uses RADIUS authentication.

Configuring the Method List for Network Accounting

Command	**aaa accounting network** { **default** | *list-name* } **start-stop** *method1* [*method2*...]
Parameter Description	*list-name*: Indicates the list name. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	ClearPass authentication uses RADIUS accounting.

Creating a Template

Command	**web-auth template cpweb**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The ClearPass authentication template is **cpweb** by default.

Configuring the Server IP Address

Command	**ip** *ip-address*
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	N/A

Configuring the Context ID and IP Address of the Hot Standby Server

Command	**context** *ctx-id peer-ip-address*
Parameter Description	*ctx-id*: Configures the context ID of the hot standby server. *peer-id-address*: Configures the IP address of the hot standby server.
Command Mode	Web authentication template configuration mode
Usage Guide	N/A

Configuring the Server URL

Command	**url** *url-string*
Parameter Description	Indicates the web-based authentication URL of the portal server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	The URL starts with **http://**.

Configuring a Response Mode After Successful Authentication

Command	**login-success response** { **redirect-init-url** [**default-url** *def-string*] | **msg** *msg-string* | **redirect-url** *url-string* }
Parameter Description	*def-string*: Indicates the default URL when the server does not provide a URL. *msg-string*: Indicates the text to be displayed after successful authentication. *url-string*: Indicates the URL to be redirected to after successful authentication.
Command Mode	Web-based authentication template configuration mode
Usage Guide	Optional.

Configuring Response Mode After Authentication Failure

Command	Configures the message displayed after the ClearPass authentication fails. **login-fail response msg** *msg-string*

	Configures the URL that redirects to the login page when the ClearPass authentication fails. **login-fail response redirect-login-url** Configures the redirect URL after the ClearPass authentication fails. **login-fail response redirect-url** *url-string* [**err-msg** *msg-key*] Configures the redirect URL in the format of http://xxx/xx?ap_mac=6c:8b:d3:37:e2:60&wlan=Guest&statusCode=5 after the ClearPass authentication fails. The **wlan** field indicates the SSID. **login-fail response redirect-url** *url-string* [**fmt ntes** [**errmsg-key** *key-string*]] Configures the redirect URL after the ClearPass authentication fails. The URL can be customized. **login-fail response redirect-url** *url-string* [**fmt custom encry** { **md5** | **des** | **des_ecb** | **des_ecb3** | **none** } { **additional** *extern-str* | **ap-mac** *ap-mac-str* **mac-format** { **dot** | **line** | **5colon** | **none** } | **ssid** *ssid-str* | **errmsg-key** *key-string* }]
Parameter Description	*msg-string*: Indicates the text to be displayed after authentication failure. **redirect-login-url**: Redirects the browser to the login page after the authentication fails. *url-string*: Indicates the URL to be redirected to after authentication failure. **ntes**: Indicates the customized URL format. *key-string*: Indicates the parameter name for error message in the URL. **custom**: Customizes the redirect URL after the authentication fails. **encry**: Configures the encryption method, including the following options: md5, des, des_ecb, des_ecb3, and none. *extern-str*: Indicates the customized extra information strings. *ap-mac-str*: Indicates the AP MAC address. **mac-format**: Configures the format of MAC addresses, including the following options: dot, line, 5colon, and none. *ssid-str*: Indicates the SSID.
Command Mode	Web authentication template configuration mode
Usage Guide	Optional.

Configuring a Mode for the Device to Resolve Authentication Requests

Command	**http-method post** [**username-key** *usrkey-string*] [**password-key** *pswkey-string*] [**init-url-key** *urlkey-string*] [**password-encrypt** { **none** | **uam** }]
Parameter Description	*usrkey-string*: Indicates the username in the authentication request. *pswkey-string*: Indicates the password in the authentication request. *urlkey-string*: Indicates the URL in the authentication request.

Command Mode	Web-based authentication template configuration mode
Usage Guide	(Optional) It is used to configure authentication request according to the requirements of the server.

Configuring Whether to Pop Up a Window for Proactive Logout After Successful Authentication

Command	**logout-popup-window**
Parameter Description	N/A
Command Mode	Web-based authentication template configuration mode
Usage Guide	(Optional) It is enabled when proactive logout is required. Note that the proactive logout window may be blocked by the STA's browser.

Configuring the Device's IP Address

Command	**web-auth auth-server ip** *ip-address*
Parameter Description	Sets the device access service IP address for ClearPass, which is used for communication from the server to this IP address.
Command Mode	Global configuration mode
Usage Guide	The access service IP address of the NAS cannot be configured as the passthrough address. When the access service IP address is configured as the IP address of the NAS and a STA in the authentication template accesses this IP address, the NAS intercepts the request of the STA and forwards it to the server. As a result, the STA fails to access the web management page of the NAS. If a STA in the authentication template accesses this IP address for device management, configure the access service IP address as the unused virtual service IP address, for example, 1.1.1.1 and 2.2.2.2.

Configuring the Device Port

Command	**web-auth auth-server http** [*port*]
Parameter Description	Indicates the TCP port used by the ClearPass STA that initiates authentication.
Command Mode	Global configuration mode
Usage Guide	It is the TCP port used by the ClearPass STA that initiates authentication. It should not conflict with the ports used by built-in web management of the device.

Configuring the URL for Initiating Authentication from a STA

Command	**web-auth auth-server submit-url** *url-string*
Parameter Description	Indicates the URL used by the ClearPass STA that initiates authentication.
Command Mode	Global configuration mode
Usage Guide	It is the URL used by the STA to initiate authentication, and must start with **http://**.

Enabling Web-based Authentication

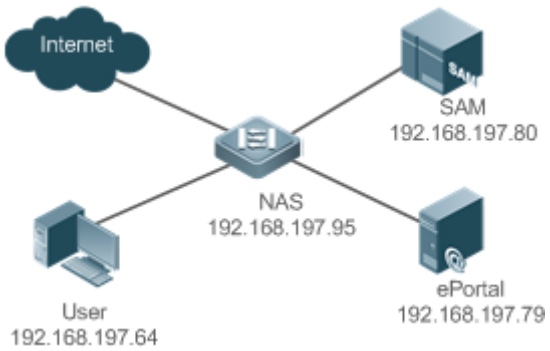
Command	**webauth**

Parameter Description	N/A
Command Mode	WLAN security mode
Usage Guide	N/A

Configuration Example

The following configuration example describes the configuration related to web-based authentication only.

Enabling ClearPass Authentication

Scenario **Figure 1-13**	
Configuration Steps	● Set the IP address of the authentication server on the network device. ● Set the URL of the authentication page on the network device. ● Set the IP address of the network device. ● Set the port of the network device. ● Set the URL for STA authentication on the network device. ● Enable web-based authentication on WLAN 10 of the network device.

	`Hostname# config`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#web-auth auth-server http port 8082`
	`Hostname(config)#web-auth auth-server ip 1.1.1.1`
	`Hostname(config)#web-auth auth-server submit-url http://1.1.1.1:8082/login`
	`Hostname(config)#web-auth template cpweb`
	`Hostname(config.tmplt.cpweb)#ip 192.168.197.79`

	`Hostname(config.tmplt.cpweb)#url http://192.168.197.79/web_login.php` `Hostname(config.tmplt.cpweb)#exit`
	`Hostname(config)# wlansec 10`

	`Hostname(config-wlansec)# web-auth portal cpweb`
	`Hostname(config-if-range)# webauth`
	`Hostname(config-if-range)# exit`

Verification	● Check whether web-based authentication is configured successfully.

	`Hostname(config)#show running-config`
	`...`
	`web-auth auth-server ip 1.1.1.1`

	web-auth auth-server http web-auth auth-server submit-url http://1.1.1.1:8082/login web-auth template cpweb ip 192.168.197.79 url http://192.168.197.79/web_login.php ... wlansec 10 web-auth portal cpweb webauth
	Hostname#show web-auth control Port Control Server Name Online User Count ------------------------- -------- -------------------- ------------- ---- wlansec 10 On cpweb 0 ...
	Hostname#show web-auth template Webauth Template Settings: --- Name: cpweb Type: cpweb Ip: 192.168.197.79 Url: http://192.168.197.79/web_login.php

Common Errors

The device IP address is not configured, causing redirection failures.

1.4.8 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 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 device to use 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	Web-based authentication 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-only-mode`
	`Type: v2`
	`Port: 50100`
	`State: Active`
	`Acctmlist: default`
	`Authmlist: mlist1`

1.4.9 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 device to use 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	Web-based authentication template configuration mode
Usage Guide	Ensure that the configured accounting method list name is consistent with that on the AAA module.

Configuration Example

↘ Specifying an Accounting Method List

Configuration Steps	● Specify the accounting method list **mlist1**.
	`Hostname(config.tmplt.eportalv2)#accounting mlist1`

Verification	● Check whether the configuration is successful.
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: eportalv2 Url: http://17.17.1.21:8080/eportal/index.jsp Ip: 17.17.1.21 BindMode: ip-mac-mode Type: v2 Port: 50100 State: Active Acctmlist: mlist1 Authmlist: mlist1

1.4.10 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 protocol, 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-based 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 used by the portal server.
- This function is applicable to Ruijie second-generation web-based authentication and iPortal web-based authentication. The two authentication modes use different default port numbers. In Ruijie second-generation web-based authentication, the configured port number is used for interaction between the NAS and portal server through the portal protocol. In Ruijie iPortal web-based authentication, the configured port number is used for packet listening on the NAS.

Configuration Steps

- Optional.
- Run the **port** *port-num* command to configure the port number 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-based authentication.
- Change the listening port of the server to 10000.
- Run the **port** *port-num* command to configure port number 10000.

- Simulate the scenario where a user performs authentication to access the Internet.
- Disconnect the user 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	Web-based authentication 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-only-mode`
	`Type: v2`
	`Port: 10000`
	`Acctmlist:`
	`Authmlist:`

1.4.11 Specifying the Web-based Authentication 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 that can be queried on the NAS are gateway addresses of STAs. Because these MAC addresses are inaccurate, the IP-only mode should be used.

Configuration Steps

- (Optional) The default web-based authentication binding mode is IP+MAC.
- Determine a binding mode based on the accuracy of user information obtained by the NAS. When IP and MAC addresses of STAs are accurate (for example, Layer 2 network deployment), IP+MAC is recommended. When the IP and MAC addresses are inaccurate, 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 Web-based Authentication Binding Mode

Command	**bindmode** { **ip-mac-mode** | **ip-only-mode** }
Parameter Description	**ip-mac-mode**: Indicates the IP-MAC binding mode. **ip-only-mode**: Indicates the IP-only binding mode.
Command Mode	Web-based authentication template configuration mode
Usage Guide	N/A

Configuration Example

Specifying the Web-based Authentication Binding Mode

Configuration Steps	● Set the binding mode to IP-only.
	`Hostname(config.tmplt.eportalv2)#bindmode ip-only-mode`
Verification	● Check whether the configuration is successful.

	`Hostname#show web-auth template`
	`Webauth Template Settings:`
	`----------`
	`Name: eportalv2`
	`Url: http://17.17.1.21:8080/eportal/index.jsp`
	`Ip: 17.17.1.21`
	`BindMode: ip-only-mode`
	`Type: v2`
	`Port: 10000`
	`Acctmlist:`
	`Authmlist:`

1.4.12 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, the page fails to be pushed, causing web-based authentication failures. The default page suite can be used if there are no special requirements.
- For details, see Customizing a Page Suite.

Configuration Steps

(Optional) By default, the default page suite is used.

Verification

- Configure iPortal web-based 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-suit** *filename*
Parameter Description	*filename*: Indicates the file name of a page suite.
Command Mode	Web-based authentication 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-suit 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

1.4.13 Configuring the Advertisement Pushing Mode

Configuration Effect

Optional. Advertisements are pushed before or after authentication.

Notes

- The advertisement URL must be configured in advance.
- By default, advertisements are pushed after successful authentication.
- 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 successful authentication.

Verification

- Configure iPortal web-based authentication.
- Configure a URL that can access the Internet.
- When a user accesses the network, check whether a new window is displayed after successful authentication and whether information on a page of a specific URI is displayed.

Related Commands

Configuring the Advertisement Pushing URL

Command	**login-popup** *url*
Parameter Description	*url*: Indicates the URL popping up before authentication or upon login.
Command Mode	Web-based 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-based authentication template configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Advertisement Pushing Mode

Configuration Steps	● Configure the advertisement pushing mode as advertisement pushing before authentication.
	`Hostname(config.tmplt.iportal)#login-popup http://www.host.com`
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`
	`time_interval: 1`
	`Login_popup: http://www.host.com`
	`Online_popup: (null)`
	`Suitename: default`
	`Authentication:`
	`Accounting:`

1.4.14 Configuring a Custom URL Format

Configuration Effect

Configure the URL used for redirecting users to the portal server based on customized parameters.

Notes

The parameter sequence of the customized URL may be different from the parameter sequence of the actual URL.

Configuration Steps

Optional.

Verification

- Configure a custom URL.
- A non-authenticated 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** [**encryp** { **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 IP address of a STA. *usermac-st*: Indicates the MAC address of a STA. *uservid-str*: Indicates the VID of a STA. *userid-str*: Indicates the ID of a STA. *nasip-st*: Indicates the NAS IP address. *nasid-str*: Indicates the NAS ID. *nasid2-str*: Indicates the NAS ID (two NAS IDs are supported). *ac-name*: Indicates the NAS name. *apmac-str*: Indicates the AP's MAC address. *apmac-str*: Indicates the original URL. *ssid-str*: Indicates the SSID. *port-str*: Indicates the authentication port. *ac-sno-st*: Indicates the AC serial number. *ap-sno-st*: Indicates the AP serial number. *extern-st*: Indicates the fixed string, which is required by some portal servers. *md5*: Indicates MD5 encryption. *des*: Indicates DES encryption. *des_ecb*: Indicates the DES_ECB mode. *des_ecb3*: Indicates the DES_ECB3 mode. *none*: Indicates no-encryption and cleartext transmission.
Command Mode	Template 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 IP address, 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 firstu`
Verification	● Check whether the configuration is successful.

	`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`

1.4.15 Configuring the Redirection HTTP Port

Configuration Effect

- When a STA accesses network resources (for example, the user accesses the Internet using a browser), the STA sends HTTP packets. The NAS or aggregation device intercepts these HTTP packets to determine whether the STA is accessing network resources. If the NAS or aggregation 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 aggregation device, such as ports 22, 23, and 53, and ports reserved by the system are not allowed to be configured as the redirection ports. All ports except port 80 with numbers smaller than 1000 are seldom used by HTTP. 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.
- To enable the NAS configured with automatic client acquisition 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 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, excluding default ports 80 and 443.

Configuration Example

↘ Configuring the Redirection HTTP Port

Configuration Steps	● Configure port 8080 as the redirection HTTP port.
	`Hostname(config)#http redirect port 8080`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show web-auth rdport`
	`Rd-Port:`
	`80 443 8080`

1.4.16 Configuring Rate Limiting for Logging in Web-based Authentication

Configuration Effect

- The web-based authentication module sends syslog messages to the administrator to display user login and logout information and events. By default, syslog messages are shielded.
- After syslog output rate limiting is configured, syslog messages are sent at the specified rate.

Notes

When the login or logout rate is high, syslog messages are output frequently, which affects device performance and results in too much information displayed.

Configuration Steps

- Optional.
- Configure syslog output rate limiting when you need to view the syslog messages about user login or logout.

Verification

- Configure rate limiting for logging in web-based authentication.
- Check whether users log in and out at the specified rate.
- Check that syslog messages are generated at the rate limit.

Related Commands

↘ **Configuring Rate Limiting for Logging in Web-based Authentication**

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 Limiting for Logging in Web-based Authentication**

Configuration Steps	● Disable rate limiting for logging in web-based authentication.
	`Hostname(config)#web-auth logging enable 0`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`web-auth logging enable 0`
	`...`

1.4.17 Configuring the Maximum Number of HTTP Sessions for Non-authenticated Clients

Configuration Effect

- When a non-authenticated user accesses network resources, the user's PC sends requests for an HTTP session connection. The NAS or aggregation device intercepts the HTTP packets and redirects the user to a web-based authentication page. To prevent a non-authenticated 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 non-authenticated user can initiate on the NAS.
- A user occupies an HTTP session when performing authentication, and the other applications of the user may also occupy HTTP sessions. It is recommended that the maximum number of HTTP sessions for a non-authenticated user be not set to 1. By default, each non-authenticated user can initiate 255 HTTP sessions globally, and each port supports up to 300 HTTP sessions initiated by non-authenticated clients.

Notes

If the authentication page cannot be displayed during web-based authentication, the maximum number of HTTP sessions may be reached. In this case, close the applications that may occupy HTTP sessions and then perform web-based authentication again.

Configuration Steps

- Optional.
- Perform this configuration when you need to change the maximum number of HTTP sessions that each non-authenticated user can initiate and the maximum number of HTTP sessions that non-authenticated clients can initiate on each port.
- Perform this configuration when you configure automatic SU client acquisition.

Verification

- Change the maximum number of HTTP sessions that a non-authenticated user can initiate.
- Simulate the scenario where a non-authenticated user constructs identical sessions to connect to the NAS continuously.

- Simulate the scenario where the non-authenticated user accesses the Internet using a browser. Check whether the access requests are redirected, and check that the NAS notifies the user that the maximum number of sessions is reached.

Related Commands

Configuring the Maximum Number of HTTP Sessions for Non-authenticated Clients

Command	**http redirect session-limit** *session-num* [**port** *port-session-num*]
Parameter Description	*session-num*: Indicates the maximum number of HTTP sessions for non-authenticated clients. The value range is from 1 to 255. The default value is 255. *port-session-num*: Indicates the maximum number of HTTP sessions on each port for authenticated clients. The value range is from 1 to 65,535. The default value is 300.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Maximum Number of HTTP Sessions for Non-authenticated Clients

Configuration Steps	● Set the maximum number of HTTP sessions for non-authenticated 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)#`

1.4.18 Configuring the HTTP Redirection Timeout Interval

Configuration Effect

Configure the HTTP redirection timeout interval to maintain redirection connections. When a non-authenticated user tries to access network resources through HTTP, the TCP connection requests sent by the user will be intercepted (a connection is established with the NAS or aggregation device). Then the NAS or aggregation device waits for the HTTP GET/HEAD packets from the user and responds with HTTP redirection packets to close the connection. The redirection timeout interval is intended to prevent the user from occupying the TCP connection for a long time without sending GET/HEAD packets. By default, the timeout interval for maintaining a redirection connection is 3s.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to change the timeout interval for maintaining redirection connections.

Verification

- Change the timeout interval.
- Use a network packet sending 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 interval is reached.

Related Commands

Configuring the HTTP Redirection Timeout Interval

Command	**http redirect timeout** *seconds*
Parameter Description	*seconds*: Indicates the timeout interval for maintaining redirection connections, in seconds. The value range is 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 Interval

Configuration Steps	● Set the HTTP redirection timeout interval 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`

1.4.19 Configuring the Authentication-Free Network Resource

Configuration Effect

- After web-based authentication or 802.1X authentication is enabled on a port, the users connecting to the port need to pass web-based authentication or 802.1X authentication before accessing network resources.
- You can configure authentication-free network resources so that the non-authenticated user can access the authentication-free network resources.
- If a website is configured as the authentication-free network resource, all users including non-authenticated clients can access the website. By default, authentication-free network resources are not configured, and non-authenticated clients are not allowed to access network resources.
- IPv6 is supported.

Notes

- The maximum number of authentication-free network resources or the maximum number of non-authenticated clients cannot exceed 1000. The actual number of available resources may be reduced because security functions occupies resources. 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, and **http redirect** is used to configure the authentication-free IP address of the web-based authentication server. The addresses configured using the two commands can be accessed without authentication, but they have different usages. You are not advised to configure the IP address of the web-based authentication server by using **http redirect direct-site**.
- When IPv6 addresses are used, configure the device to allow packets from the local-link address. 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 non-authenticated clients to access network resources.

Verification

- Configure authentication-free network resources.
- Check whether non-authenticated clients can access configured network resources using PCs.

Related Commands

Configuring the Authentication-Free Network Resource

Command	**http redirect direct-site** { *ipv6-address* | *ipv4-address* [*ip-mask*] [**arp**] | *port-number&<1-8>* }
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. *port-number*: Layer 4 port number. The parameter can be entered for a maximum of eight times. The value range is from 1 to 65535.
Command Mode	Global configuration mode
Usage Guide	To configure the authentication-free ARP resource, use the **http redirect direct-arp** command preferentially.

Configuration Example

Configuring the Authentication-Free Network Resource

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`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show web-auth direct-site`
	`Direct sites:`
	`  Address  Mask  ARP Binding Group`

```
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
```

1.4.20 Configuring the Authentication-Free ARP Resource Range

Configuration Effect

When ARP check or similar functions are enabled, ARP learning of clients is controlled. As a result, clients cannot learn ARP entries of the gateway and other devices, which affects user experience. You can configure the authentication-free ARP resource range to permit 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 the authentication-free ARP resource. 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 egress address of the PCs connecting to the Layer 2 access device is not the gateway address, configure the egress address as the authentication-free ARP resource. If multiple egresses addresses exist, configure the addresses as authentication-free ARP resources.

Configuration Steps

- Optional.
- If ARP check is enabled on the NAS, you must configure the authentication-free resources and gateway address as authentication-free ARP resources.

Verification

- Configure authentication-free ARP resources.
- Run the **arp -d** command in the Windows operating system to clear the ARP cache of the PC of a non-authenticated user.
- Run the **ping** command on the PC to access the authentication-free ARP resources.
- run the **arp -a** command in the Windows operating system to check the ARP cache on the PC 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 authentication-free resources. *ip-mask*: Indicates the mask of authentication-free resources.

Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Authentication-Free ARP Resource Range

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)#`

1.4.21 Configuring the Authentication-Free Address Range

Configuration Effect

- Users in the authentication-free address range do not need to pass web-based authentication when accessing reachable network resources. By default, no authentication-free address range is configured. All users must pass web-based authentication before accessing network resources.
- The authentication-free address range can be configured as an IP or MAC address range.

Notes

N/A

Configuration Steps

- Optional.
- Perform this configuration to allow non-authenticated clients to access network resources.

Verification

- Configure an authentication-free user.
- Check whether the user can access the Internet without authentication.

Related Commands

Configuring the Authentication-Free Address Range

Command	**web-auth direct-host** { *ipv4-address* [*ipv4-mask*] [**arp**] [**port** *interface-name interface-port*] | *ipv6-address* | *mac-address* }

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.
Command Mode	Global configuration mode
Usage Guide	The **arp** field is used for configuring the device to allow ARP packets to pass. This field must be set when ARP check is enabled. After the **port** field is set, non-authentication takes effect only on the configured interface.

Configuration Example

↘ Configuring the Authentication-Free Address Range

Configuration Steps	Configure the authentication-free address range.
	`Hostname(config)# web-auth direct-host 192.168.197.64`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show web-auth direct-host`
	`Direct hosts:`
	`  Address  Mask  Port  ARP Binding  Group  Description`
	`  ---------- ---------- ---------- ---------- -------- ----------`
	`  192.168.197.64  255.255.255.255  Off  N/A  N/A`

1.4.22 Configuring the Interval for Updating Online User Information

Configuration Effect

The NAS or aggregation device maintains and periodically updates 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 interval for updating online user information must be configured as a multiple of 60. Otherwise, the actual configuration will automatically round up to the nearest multiple of 60 for it to take effect.

Configuration Steps

- Optional.
- Perform this configuration to allow non-authenticated clients to access network resources.

Verification

- Configure the interval for updating online user information.
- View information about 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 seconds. The value range is from 30 to 3,600. The default value is 180s.
Command Mode	Global configuration mode
Usage Guide	To restore the default interval, run the **no web-auth update-interval** command in global configuration mode.

Configuration Example

Configuring the Interval for Updating Online User Information

Configuration Steps	● Set the interval for updating online user information to 60s.
	`Hostname(config)# web-auth update-interval 60`
Verification	● Check whether the configuration is successful.
	`Hostname(config)#show run | include web-auth update-interval` `web-auth update-interval 60`

1.4.23 Configuring Portal Server 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 and ClearPass 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 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 interval for each packet is specified by the **timeout** parameter. The parameter settings are also supported by Ruijie first-generation web-based authentication.
- Portal server detection takes effect for Ruijie first-generation web authetntication, ClearPass authentication, and Ruijie second-generation web authentication.
- If multiple portal servers are configured, they work 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 detection results will be inaccurate.
- The system will automatically select a detection method based on whether Ruijie first- or second-generation web-based authentication is used.

Configuration Steps

- Optional.
- Configure multiple portal server templates applicable to Ruijie first- or second-generation web-based authentication.

Verification

- Configure two portal server templates for Ruijie first- or second-generation web-based authentication: one server is unavailable server and the other is available in the templates.
- When the console displays a log indicating that the portal server is unavailable, 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 interval. The default value is 5s. *intsec*: Indicates the retransmission count. The default value is 3 (times).
Command Mode	Global configuration mode
Usage Guide	In most 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 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 with the **fmt** command. Before using this command, use the **fmt** command to configure the URL format.

Command	**web-auth ping** [**interval** *minutes*] [**retry** *times*]
Parameter Description	*minutes*: Indicates the detection interval. The default value is 1 minute. *times*: Indicates the retransmission count. The default value is 3 (times).
Command Mode	Global configuration mode
Usage Guide	In most 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 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 with the **fmt** command. Before using this command, use the **fmt** command to configure the URL format.

Configuration Example

Configuring Portal Server Detection

Configuration Steps	● Configure portal server 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`
	`...`

1.4.24 Configuring Portal Escape

Configuration Effect

Allow new users to access the Internet without authentication when the portal server is unavailable.

Notes

- To use the portal escape function, you must configure portal server detection.
- If multiple portal servers are configured, the escape function takes effect only when all the portal servers are unavailable.
- The escape function is intended only for the portal server but not the RADIUS server.

Configuration Steps

- Optional.
- Configure portal server detection.
- Configure portal escape.
- (Optional) Configure the nokick attribute.

Verification

- Configure a portal server and disable the server.
- Configure portal server detection and the escape function.
- When the NAS detects that the portal server is unavailable, 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`
	`...`

1.4.25 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-based authentication and iPortal web-based authentication.
- The requirement that clients obtain IP addresses through DHCP must be specified during network deployment. Those clients cannot use static IP addresses; otherwise, the existing clients that use static IP addresses will be affected.
- If a few clients need to use static IP addresses, configure these IP addresses as authentication-free addresses.
- If DHCP address check needs to be enabled only on some interfaces or some VLANs of interfaces, disable global DHCP address check and configure the VLAN range in which DHCP address check needs to be enabled on 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 for a client.
- Connect the client to the Internet and check that the client 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 clients who obtain IP addresses through DHCP to access the Internet. This function prevents clients with private IP addresses from performing authentication to access the Internet.

Enabling Interface-based DHCP Address Check

Command	**web-auth dhcp-check {vlan [**vlan-list**]}**
Parameter Description	vlan-list: Indicates the range of VLANs that require DHCP address check on an interface.
Command Mode	Interface configuration mode
Usage Guide	If DHCP address check is only required on certain interfaces or VLANs on an interface, you need to disable DHCP address check globally, and then configure the VLAN range to be effective on each interface separately.

Configuration Example

Enabling DHCP Address Check

Configuration Steps	● Enable global DHCP address check.
	`Hostname(config)#web-auth dhcp-check`
	● Enable interface-based DHCP address check.
	`Hostname(config-if-TenGigabitEthernet 3/1)# web-auth dhcp-check vlan 1,3-4`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`web-auth dhcp-check`
	`...`
	`interface TenGigabitEthernet 3/1`
	`web-auth dhcp-check vlan 1,3-4`
	`...`

1.4.26 Disabling Link Detection

Configuration Effect

- 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 scenarios where mobile office is required or wireless web-based authentication is deployed but wireless signals are 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, client logout is triggered only when the user clicks the logout button on the online page, the server disconnects the client, 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 *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 is high in a wireless environment where wireless connections are easily affected by signal interference, and disabling link detection helps improve wireless experience.

Configuration Steps

- Optional.
- Configure web-based authentication.
- Disable link detection.

Verification

- Configure Ruijie second-generation web-based authentication and disable link detection.

- Connect a client to the Internet and perform authentication. When the client passes 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 or 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`
	`...`

1.4.27 Disabling Portal Extension

Configuration Effect

- Enable portal extension to support Ruijie portal server and portal servers that comply with *CMCC WLAN Service Portal Specification*.
- You can select multiple redirection URL formats when the device interworks with the servers in compliance with *CMCC WLAN Service Portal Specification*.

Notes

- Only Ruijie second-generation web-based authentication supports portal extension.
- Ruijie second-generation web-based authentication extends *CMCC WLAN Service Portal Specification*. You need to determine whether to use the extension mode based on server performance.
- If the portal server of Ruijie is used, use the default mode, that is, extension mode. If the portal server complies with *CMCC WLAN Service Portal Specification*, disable portal extension.

- *CMCC WLAN Service Portal Specification* supports multiple redirection URL formats. If the portal server complies with *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 complying with *CMCC WLAN Service Portal Specification* to be used in Ruijie second-generation web-based 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 server that complies with *CMCC WLAN Service Portal Specification* is 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`
	`...`

1.4.28 Configuring an Allowlist and a Blocklist

Configuration Effect

- Configure an allowlist to allow non-authenticated clients to access some network resources, and configure a blocklist to prevent authenticated clients from accessing some network resources.
- Allowlists and blocklists are supported based on ports, URLs, and IP addresses.

Notes

- Up to 1,000 blocklists and allowlists can be configured.
- If blocklists and allowlists are configured in domain name format, DNS 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 an allowlist and a blocklist.

Verification

- Configure an allowlist and a blocklist.
- Check whether non-authenticated STAs can access the allowlisted addresses.
- Check whether authenticated STAs cannot access the blocklisted addresses.

Related Commands

Configuring an Allowlist and a Blocklist

Command	**web-auth acl** { **black-ip** *ip* | **black-port** *port* | **black-url** *name* | **white-port** *port* | **white-url** *name* }
Parameter Description	*ip*: Indicates an IP addresses blocklisted. *port*: Indicates a port numbers blocklisted or allowlisted. *name*: Indicates a URL blocklisted or allowlisted.
Command Mode	Global configuration mode (Blocklists can be configured in WLAN security configuration mode on wireless devices.)
Usage Guide	Configure an allowlist to allow non-authenticated clients to access some network resources, and configure a blocklist to prevent authenticated clients from accessing some network resources.

Configuration Example

Configuring an Allowlist and a Blocklist

Configuration Steps	● Configure an allowlist and a blocklist.
	`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`
	`...`

1.4.29 Configuring Anti-jitter Accounting

Configuration Effect

If anti-jitter or low traffic detection is configured on the NAS, the time of anti-jitter or low traffic detection will be counted into the online duration. Anti-jitter 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 when the link is disconnected for a long time or the NAS detects its low traffic.
- When anti-jitter and low traffic detection functions are enabled, the time of the function that first triggers logout is counted. For example, the anti-jitter 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 anti-jitter function first triggers web-based authentication to disconnect the client. In this case, only the 5-minute duration is deducted from the online duration in the accounting packet.

Configuration Steps

- Optional.
- Configure the accounting function.
- Configure anti-jitter or low traffic detection.
- Configure anti-jitter accounting.

Verification

- Simulate the scenario where a client goes online after authentication and then go 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 Anti-jitter Accounting**

Command	**web-auth accounting jitter-off**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to include the anti-jitter duration or low traffic detection time into the online duration in the accounting-stop packet based on the server accounting policy. By default, the time is not included.

Configuration Example

Configuring Anti-jitter Accounting

Configuration Steps	● Configure anti-jitter accounting.
	`Hostname(config)#web-auth accounting jitter-off`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`web-auth accounting jitter-off`
	`...`

1.4.30 Configuring the Source Port for Communication with the Portal Server

Configuration Effect

Configure the source port used for communication between the NAS and portal server.

Notes

Only one port can be configured for communication between the NAS and portal server.

Configuration Steps

Configure a port as the source port for communication with the portal server.

Verification

After web-based authentication is enabled, obtain a packet on the portal server during authentication and check whether the source IP address of the packet is the IP address of the specified port.

Related Commands

Configuring the Source Port for Communication with the Portal Server

Command	**ip portal source-interface** *interface-type interface-num*
Parameter Description	*interface-type*: Indicates the interface type. *interface-num*: Indicates the interface number.

Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the Source Port for Communication with the Portal Server

Configuration Steps	● Configure an aggregate port as the source port for communication with the portal server.
	`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`

1.4.31 Configuring the Anti-Noise Function

Configuration Effect

Packets sent to the configured IP address and port are not filtered by the anti-noise function.

Notes

If there are too many packets of this type, normal authentication packets may be discarded.

Configuration Steps

Configuring the Anti-Noise Function

In global configuration mode, configure the IP address and port number to be configured with the anti-noise function.

Command	**web-auth anti-noise ip** *ip-addr* **port** *port*
Parameter Description	*ip-addr*: Indicates the destination address of a packet. *port*: Indicates the Layer 4 port number of a packet.
Command Mode	Global configuration mode
Usage Guide	Multiple IP addresses can be configured.

Verification

Send packets that comply with the configuration and packets that do not. The packets that comply with the configuration are not discarded by the line card.

Configuration Example

Configuring the Anti-Noise Function

Configuration Steps	● Configure the IP address and port with the anti-noise function.
	`Hostname(config)# web-auth anti-noise ip 192.168.1.1 port 80`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`web-auth anti-noise ip 192.168.1.1 port 80`

1.4.32 Configuring an NDKEY-Compatible Web-based Authentication URL

Configuration Effect

Configure the web-based authentication URL used in web-based authentication to support Shanghai NDKEY system.

Notes

N/A

Configuration Steps

Configuring an NDKEY-Compatible Web-based Authentication 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 Anti-noise 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`
	`...`
	`web-auth dkey-compatible url-parameter login`

1.4.33 Configuring Multi-Portal Mapping

Configuration Effect

Users from different network segments can be configured to use different portals for authentication.

Notes

- Multiple mappings can be configured. If a user is out of the mapping range, the default portal is used for authentication.
- Different mapping ranges cannot overlap.

Configuration Steps

Configuring Multi-Portal Mapping

Configure mapping parameters in global configuration mode.

Command	**web-auth portal** { **eportalv2** | **eportalv1** | **iportal** | *name* }
Parameter Description	*name*: Indicates the name of the template in use.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Use different network segments for authentication. Users can authenticate using different portals.

Configuration Example

Configuring Multi-Portal Mapping

Configuration Steps	● Configure network segment mappings.

	`Hostname(config)# web-auth portal eportalv2 ip-mapping 192.168.1.0 255.255.255.0`
	`Hostname(config)# web-auth portal eportalv1 ip-mapping 192.168.2.0 255.255.255.0`
	`Hostname(config)# web-auth portal eportalv2`

Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`web-auth portal eportalv2`
	`web-auth portal eportalv2 ip-mapping 192.168.1.0 255.255.255.0`
	`web-auth portal eportalv1 ip-mapping 192.168.2.0 255.255.255.0`

1.4.34 Enabling NAT for Ruijie iPortal Web-based Authentication

Configuration Effect

Configure Ruijie iPortal web-based authentication to support NAT.

Notes

NAT takes effect only in Ruijie iPortal web-based authentication.

Configuration Steps

Enabling NAT for Ruijie iPortal Web-based 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-based authentication can be implemented after NAT is enabled.

Configuration Example

Enabling NAT for Ruijie iPortal Web-based Authentication

Configuration Steps	● Enable NAT for Ruijie iPortal web-based authentication.
	`Hostname(config)#iportal nat enable`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`iportal nat enable`

1.4.35 Configuring the iPortal HTTP Retransmission Count

Configuration Effect

Configure the iPortal HTTP retransmission count.

Notes

The retransmission count takes effect only for the HTTP connections pushed by an iPortal page.

Configuration Steps

Configuring the iPortal HTTP Retransmission Count

Set the retransmission count in global configuration mode.

Command	**iportal retransmit** *count*
Parameter Description	*count*: Indicates the retransmission count.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Configure the device to send an iPortal web-based authentication request and disconnect the device from the network. Check whether the NAS resends an HTTP connection request.

Configuration Example

Configuring the Retransmission Count

Configuration Steps	● Configure the retransmission count.
	`Hostname(config)#iportal retransmit 5`
Verification	● Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	`...`
	`iportal retransmit 5`

1.4.36 Configuring Service Selection in Ruijie iPortal Web-based Authentication

Configuration Effect

Configure the service type used by Ruijie iPortal web-based authentication.

Notes

N/A

Configuration Steps

Configuring the Service Type Used by Ruijie iPortal Web-based 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.

	`Hostname(config)#show running-config`
	`...`
	`iportalservice local local-srv`

1.4.37 Configuring the UA Field for iPortal Web-based Authentication Users

Configuration Effect

It is used to configure the STA name corresponding to the UA field of a user.

Notes

This command is invalid because STA recognition should be used instead.

Configuration Steps

Configuring the UA Field for iPortal Web-based Authentication Users

Configure the UA field in global configuration mode

Command	**iportal user-agent** *ua-name* **type mobile** *ua-string*
Parameter Description	*ua-name*: Indicates the name of the UA field. *ua-string*: Indicates the content of the UA string.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

N/A

1.4.38 Importing a Page Suite for Ruijie iPortal Web-based Authentication

Configuration Effect

- Import a page suite used by Ruijie iPortal web-based authentication.

Notes

- N/A

Configuration Steps

Importing a Page Suite for Ruijie iPortal Web-based Authentication

Command	**web-auth import-page-suite tftp:***path*
Parameter Description	*path*: Indicates the file path
Defaults	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Enable the TFTP server and store the file to be imported on the server.

Verification

- After a page suite is imported, run the **page-suite** command in template configuration mode to check whether the configuration is successfu.

Configuration Example

Importing a Page Suite

Configuration Steps	● Import a page suite. `Hostname# web-auth import-page-suite tftp://10.104.8.66/custom.zip`
Verification	● Check whether the configuration is successful. `Hostname#show running-config`

1.4.39 Configuring the Accounting Method List of Web-based Authentication

Configuration Effect

In global configuration mode, specify an accounting method for web-based authentication.

Notes

If no accounting method is configured for web-based authentication, the default method is used.

Configuration Steps

Configuring an Accounting Method

Configure an accounting method in global configuration mode.

Command	**web-auth accounting** { **v2** | **intra** | **cpweb** } { **default** | *name* }
Parameter Description	*name*: Indicates the name of the accounting method list to be used.
Command Mode	Global 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)#web-auth accounting v2 test`
	`Hostname(config)# web-auth accounting intra test`
	`Hostname(config)# web-auth accounting cpweb test`

Verification	● Check whether the configuration is successful.

	`Hostname#show running-config`
	`...`
	`web-auth accounting v2 test`
	`web-auth accounting intra test`
	`web-auth accounting cpweb test`

1.4.40 Configuring a Web-based Authentication Method List

Configuration Effect

In global configuration mode, specify a web-based authentication method.

Notes

If no Web authentication method is configured, the default method is used.

Configuration Steps

Configuring a Web-based Authentication Method List

Configure a web-based authentication method in global configuration mode.

Command	**web-auth authentication** { **v2** | **intra** | **cpweb** } { **default** | *name* }
Parameter Description	name: Indicates authentication method list name. The value can contain up to 63 characters.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

View the destination IP address of authentication packets.

Configuration Example

Configuring a Web-based Authentication Method

Configuration Steps	● Configure a web-based authentication method.

	`Hostname(config)#web-auth authentication v2 test`
	`Hostname(config)# web-auth authentication intra test`
	`Hostname(config)# web-auth authentication cpweb test`

Verification	● Check whether the configuration is successful.

	`Hostname#show running-config`
	`...`
	`web-auth authentication v2 test`
	`web-auth authentication intra test`
	`web-auth authentication cpweb test`

1.4.41 Customizing a Page Suite

Configuration Effect

- Customize a webpage to display logos or advertisements in Ruijie iPortal web-based authentication.
- A single page suite supports two page sets to adapt to the screen sizes of terminals, for example, mobile terminals with a small screen.

Notes

- The preparation of a page suite must comply with the relevant specification; otherwise, the customized page suite cannot be used.
- The maximum number of files in a page suite (including the files displayed on PCs and mobile terminals) is 50, and the maximum length of the file name of each page is 32 bytes.
- A new page suite must be downloaded to the ./portal directory and the name must not be the same as that of the default page suite; otherwise, the default page suite will be overwritten.
- Some NASs do not have a default page suite. When Ruijie iPortal web-based authentication is implemented, prepare a page suite in accordance with the relevant specification and import the page suite to the flash memory.

Configuration Steps

N/A

Verification

Simulate the scenario where a STA connects to the Internet and opens the browser to perform authentication. Check that the customized page is displayed.

Related Commands

Page File Naming Specification

Page File Name (with a File Name Extension)	Usage

login.htm	Login page
online.htm	Online page (which is displayed when users pass authentication)
offline.htm	Offline page
login_mobile.htm	Login page for mobile terminals
online_mobile.htm	Online page for mobile terminals (which is displayed when users pass authentication)
offline_mobile.htm	Offline page for mobile terminals

Login Page Preparation Specification

According to the page file naming specification, the file name of the login page for PCs is **login.htm**, and that for mobile terminals is **login_mobile.htm**. The login page content specification is described as follows.

- Form elements

The login page must contain a form, and the form submission method has a fixed value of POST. The PC login page is used as an example. Assume that the PC login page is stored in the **/portal** directory. The HTML code of the form is as follows (the HTML code of the form of the mobile terminal login page is similar):

```
<form method="post" action="/portal/login.htm">
...
</form>
```

The form of the login page must contain the following page elements:

1 (Mandatory) User name text box: allows a user to enter the user name. The text box ID is username.

2 (Mandatory) Password text box: allows a user to enter the password (which is not displayed in cleartext mode). The text box ID is password.

3 (Mandatory) Login button: allows a user to submit a form using the POST method.

4 (Optional) Tab showing an authentication failure cause: The ID of the tab is errormsg. The tab is displayed on the login page to show why the current user fails authentication. When the login page is loaded, an error message request is sent using the GET method, and the request results will be displayed on the errormsg tab. You can configure whether to display the errormsg tab on the login page as required. The following script is used to request the error message content from the server (the script is only one example):

```
< script language="javascript">
//Request the error message content from the server.
function requestErrorMsg() {
   var _errormsg=document.getElementById("errormsg");
    var script=document.createElement("script");
script.src="errormessage"+location.search;
_errormsg.appendChild(script);
}

//Call the init function when the login page is loaded.
function init() {
```

```
...
requestErrorMsg();
}
...
</script>
```

- Form submission

A form is submitted in the format of username=[AAAA]&password=[BBBB]&lang=[CCCC]. The meanings of the fields are described in the following:

[AAAA]: (Optional) Indicates the user name that the user enters in the user name text box.

[BBBB]: (Optional) Indicates the password that the user enters in the password text box.

[CCCC]: (Optional) Indicates the language environment. The value **1** indicates Simplified Chinese, and the value **2** indicates English. Other languages are not defined. The default language environment is Simplified Chinese. When English is used, the submitted form must contain the language environment information; otherwise, the content of the errormsg tab is in Chinese.

The form of the login page must contain at least the following three input fields (tabs): username, password, and login button. If the login page provides the Chinese and English language options, the form may also contain the language input field, which is invisible.

The HTML source code of the login page is as follows:

```
<html>
<head>
<title>Web-based authentication login page</title>
</head>
<script language="javascript">
//Request errormsg. Errormsg is empty and not displayed when a user passes authentication
or the login page is loaded for the first time.
   function requestErrorMsg() {
   var _errormsg=document.getElementById("errormsg");
    var script=document.createElement("script");
script.src="errormessage"+location.search;
_errormsg.appendChild(script);
   }

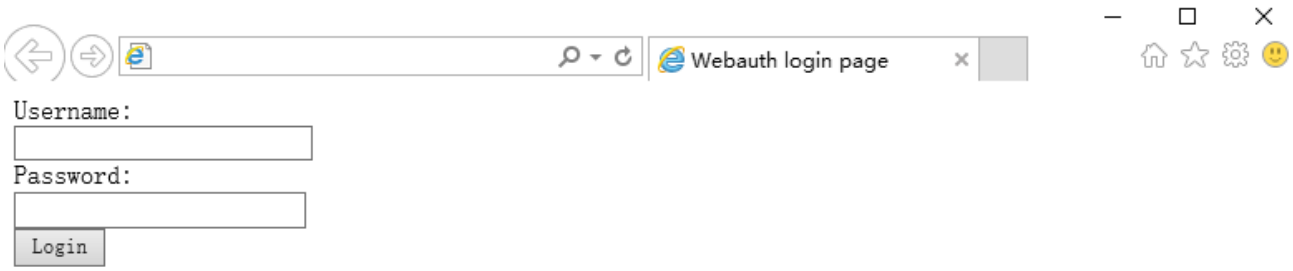
function init() {
...
requestErrorMsg();
}

//Script that is executed when a user clicks the login button
function login() {
  document.getElementById('loginForm').action = "./login.htm"+location.search;
    document.getElementById('loginForm').submit();
    window.onbeforeunload = null;
```

```
    window.onunload = null;
}
...

</script>
<body onload="init()">
<form method="post" id="loginForm">
User name:<br>
<input type="text" name="username" accesskey="u" size="25" value="" id="usrename">
<br>
Password:<br>
<input type="password" name="password" accesskey="p" size="25"
       value="" id="password">
<br>
<input type="button" onclick="login()" value="Login" id="loginButton">
<input type="hidden" name="lang" value="" id="lan">
    <p name="errormsg" id="errormsg"></p>
</form>
</body>
</html>
```

The following figure shows the login page that the iPortal server pushes to users.



The login page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

Online Page Preparation Specification

The online page is designed to inform a user that the user has passed authentication and can use network resources normally. The file name of the login page for PCs is **login.htm**, and that for mobile terminals is **login_mobile.htm**.

- Form elements

The online page must contain a form, which is used to submit an offline request. For this reason, the form must contain the logout button. The form submission method has a fixed value of POST. The PC online page is used as an example. Assume that the PC online page is stored in the /portal directory. The HTML code of the form is as follows (the HTML code of the form of the mobile terminal online page is similar):

```
<form method="post" action="/portal/online.htm">
...
</form>
```

The form of the online page must contain the following page elements:

1 (Optional) Tab with the username ID: displays information about the online user.

2 (Optional) Tab with the userip ID: displays the IP address of the online user.

3 (Optional) Tab with the usermac ID: displays the MAC address of the online user.

4 (Optional) Tab with the ssid ID: displays the SSID of the online user.

5 (Optional) Tab with the availtime ID: displays the available time during which the user can access the Internet.

6 (Mandatory) Logout button: allows the user to go offline and requests the display of the offline page.

When the online page is loaded, a request is sent using the GET method to retrieve user information from the server, including the user name, IP address, MAC address, and associated SSID of the online user, and available time. The URI is getonlineinfo. The onload method of the body in the HTML code must be used. The following script is used to request user information from the server (the script is only one example):

```
<script language="javascript">
//Obtain information about the online user, including the user name, IP address, MAC
address, and associated SSID of the online user, and available time.
   function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement("script");
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
    }

    function init() {
        requestOnlineInfo();
    }
</script>
<body onload="init()">
...
</body>
```

The HTML source code of the online page is as follows:

```
<html>
<head>
```

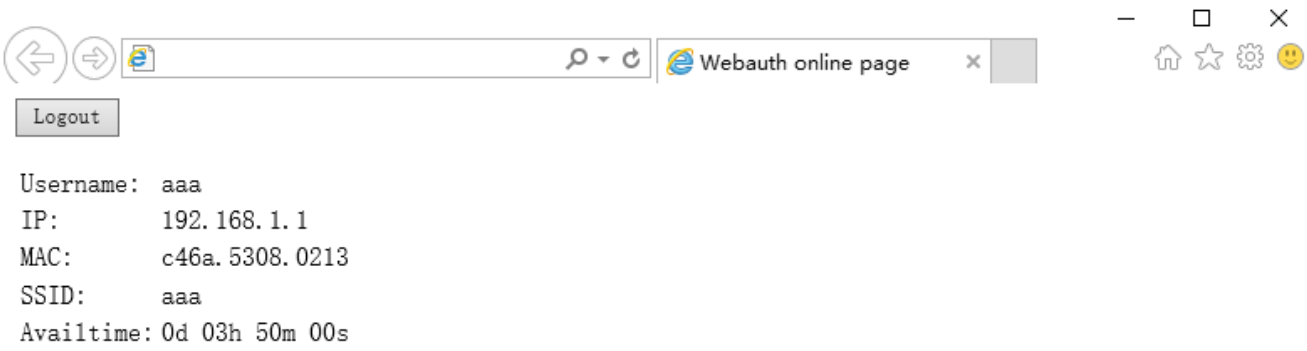
```
<title>Web-based authentication online page</title>
</head>
<script language="javascript">
//Obtain information about the online user, including the user name, IP address, MAC
address, and associated SSID of the online user, and available time.
   function requestOnlineInfo() {
        var _availTime=document.getElementById("availtime");
        var script=document.createElement("script");
        script.src="getonlineinfo"+location.search;
        _availTime.appendChild(script);
    }

    function init() {
        requestOnlineInfo ();
    }
    //Script that is executed when the user clicks the logout button. The request URI is
offline.htm.
    function logout() {
       document.logoutform.action = "./offline.htm"+location.search;
       document.logoutform.submit();
       window.onbeforeunload = null;
        window.onunload = null;
    }

</script>

<body onload="init()">
<form method="post" action="/portal/offline.htm" id="logoutform">
<input type="button" onclick="logout()" value="Logout" id="logoutButton">
</form>
    <table>
    <tr><td>User name:</td><td id="username"></td></tr>
    <tr><td>IP address:</td><td id="userip"></td></tr>
    <tr><td>MAC address:</td><td id="usermac"></td></tr>
    <tr><td>Associated SSID:</td><td id="ssid"></td></tr>
    <tr><td>Available time:</td><td id="availtime"></td></tr>
    </table>
</body>
</html>
```

The following figure shows the login page that the iPortal server pushes to users.



The login page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

Offline Page Preparation Specification

The offline page is displayed when a user clicks the logout button on the online page. The offline page is designed to inform the user that the user logs out successfully. If the user needs to access the Internet after logout, the user must perform authentication. The file name of the offline page for PCs is **offline.htm**, and that for mobile terminals is **offline_mobile.htm**.

The offline page has the following elements:

1 (Optional) Tab with the timeused ID: displays the time that has used by the user to access the Internet.

2 When the offline page is loaded, a request is sent using the GET method to retrieve the used-time information from the server. The request URI is getofflineinfo. The onload method of the body in the HTML code must be used. To obtain the used-time information, you can create a dynamic script. For example, you can create **script.src="getofflineinfo"** to include the field information to be sent in the **src** of the script. The following script is used to request the used time from the server (the script is only one example):

```
<script language="javascript">
//Obtain the used time information.
   function requestOfflineInfo() {
   var _timeused =document.getElementById("timeused");
      var script=document.createElement("script");
      script.src="getofflineinfo"+location.search;
    _timeused.appendChild(script);
    }

    function init() {
        requestUserInfo();
    }
</script>
<body onload="init()">
...
</body>
```

The HTML source code of the offline page is as follows:

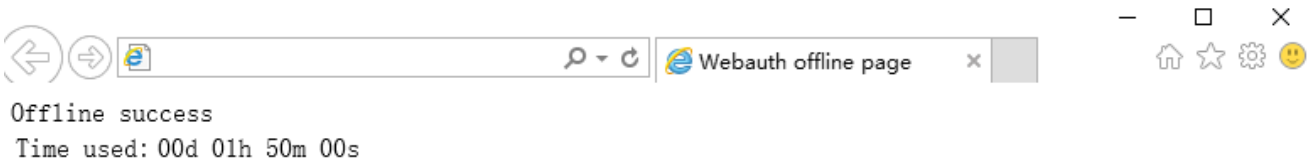
```
<html>
```

```
<head>
<title>Web authentication offline page</title>
</head>
<script language="javascript">
//Obtain the used time information.
   function requestOfflineInfo() {
        var _timeused=document.getElementById("timeused");
        var script=document.createElement("script");
        script.src="getofflineinfo"+location.search;
        _timeused.appendChild(script);
    }

    function init() {
        requestOfflineInfo();
    }
</script>

<body onload="init()">
Logout succeeded<br>
    <table>
    <tr><td>Used time:</td><td id="timeused"></td></tr>
    </table>
</body>
</html>
```

The following figure shows the offline page that the iPortal server pushes to users.



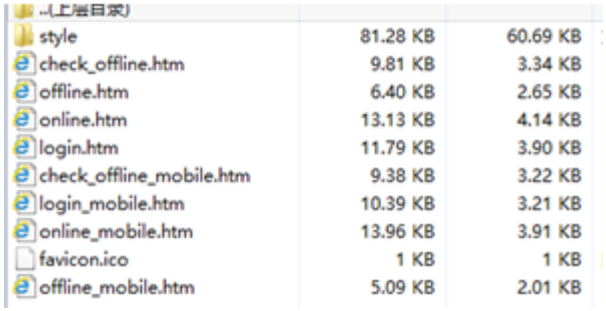
The offline page shows only the mandatory elements. Other functions can be added. For example, you can add a background and set the styles of page elements.

Page Compression Specification

After you prepare the login page, online page, and offline page in accordance with the preceding specification, you need to compress the pages and related elements and upload them to the NAS. Then you can apply the page suite. The page compression specification is as follows:

1 Compress the prepared pages and related element files (such as image files and style sheet files) into a **.zip** package, for example, **portal1_page.zip**.

2 You can create directories in a page suite. For example, the **portal1_page.zip** package shown in the following figure has the **style** directory, which contains the CSS files of pages and other image files.



After you compress the pages into a page suite, use TFTP or other tools to upload the page suite to **/portal/zip/** of the flash memory on the NAS. Then configure the portal server to use the page suite (that is, associate the portal server with the page suite). For details, see the configuration manual related to web-based authentication. A directory named after the page suite package is created in **/portal/ext_zip/** of the flash memory. For example, if the page suite package is named **portal1_page.zip**, **/portal/ext_zip/protal1_page/** of the flash memory is created, and the package is automatically decompressed in the directory. The portal server can push web-based authentication pages to users based on the page suite.

Configuration Example

Customizing a Page Suite

Configuration Steps	● Customize a page suite.
	`Hostname(config.tmplt.iportal)#page-suit hostepage`
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`

1.4.42 Configuring Upgrade Compatibility

Configuration Effect

- Some configuration commands have been optimized in the software of 11.X, resulting in format changes.
- The software of 10.X can be upgraded smoothly without any loss of functionality. However, after the upgrade, some old commands will be converted into new commands.
- For the software of 11.X, executing the **no** form of old commands will fail. You need to use the new format of commands.

Notes

N/A

Configuration Steps

You are advised to use new formats of commands with format changes.

Verification

- When the software of 10.X is upgraded to 11.X, there is no loss of functionality. Some old commands will be converted into new commands, which are displayed and saved.
- The functions of commands in new formats are the same as those of old commands.

Related Commands

Configuring the IP Address of the Portal Server for First-generation Web-based Authentication

Command	**http redirect** *ip-address*
Parameter Description	*ip-address*: Configures the IP address of the ePortal server for first-generation web-based authentication.
Command Mode	Global configuration mode
Usage Guide	When the device version is upgraded to 11.X, this command is automatically converted into the command format supported by 11.X.

Configuring the URL of the ePortal Server for First-generation Web-based Authentication

Command	**http redirect homepge** *url*
Parameter Description	*url*: Configures the URL of the ePortal server for first-generation web-based authentication.
Command Mode	Global configuration mode
Usage Guide	When the device version is upgraded to 11.X, this command is automatically converted into the command format supported by 11.X.

Configuring the Portal Server

Command	**portal-server** [**eportal1** | **eportalv2**]

Parameter Description	**eportav1**: indicates portal information about first-generation web-based authentication. **eportav2**: indicates portal information about second-generation web-based authentication.
Command Mode	Global configuration mode
Usage Guide	When the device version is upgraded to 11.X, this command is automatically converted into the command format supported by 11.X.

Configuring Interface Control for Web-based Authentication

Command	**web-auth port-control**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	In 11.X, this command is changed to **web-auth enable <type>**. **type** refers to first-generation or second-generation web-based authentication. The value is first-generation web-based authentication by default.

Configuring the Binding Mode as IP-Only

Command	**web-auth port-control ip-only-mode**
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	When the device version is upgraded to 11.X, this command is automatically converted into the command format supported by 11.X.

Configuring Web-based Authentication for VLANs

Command	**web-auth allow-vlan** *list*
Parameter Description	*list*: Configures a VLAN list for web-based authentication.
Command Mode	Global configuration mode
Usage Guide	In 11.X, this command is changed to a command without SCC.

Display the Configuration of First-generation Web-based Authentication

Command	**show http redirect**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	In 11.X, the old command is unavailable. It is changed to **show web-auth template**.

Displaying Interface Control Information

Command	**show web-auth port-control**

Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	In 11.X, the old command is unavailable. It is changed to **show web-auth control**.

Configuration Example

Configuring First-generation Web-based Authentication

Configuration Steps	● Configure the device to use 10.X and allocate the IP address of the first-generation web-based authentication server. `Hostname(config)# http redirect 192.168.197.64`

Verification	● Upgrade the software version to 11.X.
	● Run the **show running-config** command. Check that the new command format is used.
	`Hostname#sh running-config`
	`web-auth template eportalv1`

1.4.43 Configuring RADIUS Authentication Escape

Configuration Effect

After RADIUS authentication escape is enabled, web-based authentication users can still perform authentication to access the Internet in the case of a RADIUS server failure.

Notes

This function must be used with the 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 authentication in the case of a RADIUS server failure.

Configuration Example

Configuring RADIUS Authentication Escape

Configuration Steps	● Enable RADIUS authentication escape. `Hostname(config)# web-auth radius-escape`
Verification	● Check whether the configuration is successful. `Hostname(config)#show running-config`

1.4.44 Configuring Built-in Logo Replacement

Configuration Effect

Configure the built-in logo replacement function, which allows for replacement of the logo on all pages of the built-in portal.

Notes

The logo upload directory is **/data/portal/logo** and the filename must be **free_login_logo.jpg**.

Configuration Steps

Configuring the Built-in Logo Replacement Function

Command	**web customized-logo enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Upload an image and check whether the logo on the built-in portal pages has been replaced.

Configuration Example

Configuring the Logo Replacement Function

Configuration Steps	● Enable the logo replacement function. ● (Optional) You can enable this function only when the logo on the built-in authentication page needs to be replaced. `Hostname(config)# web customized-logo enable`
Verification	● Check whether the configuration is successful. `Hostname(config)#show running-config`

1.4.45 Configuring Noise Reduction in Wireless Web-based Authentication

Configuration Effect

When the number of times a STA accesses an IP address reaches the configured threshold, the subsequent packets that the STA sends to the IP address will be dropped, achieving noise reduction.

Notes

Configure the aging time and hit count for noise reduction based on the network situation to avoid dropping of normal packets, which will affect redirection.

Configuration Steps

Configuring Noise Reduction in Wireless Web-based Authentication

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*: Indicates the number of times a STA accesses an IP address. If the number of times a STA accesses an IP address reaches the the value specified by this parameter, noise is considered to occur. The default value is 3.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Simulate the scenario where a 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 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-based Authentication

Configuration Steps	● Set parameters of noise reduction in wireless web-based authentication. `Hostname(config)#web-auth noise aging 1 hit 3`
Verification	● Check whether the configuration is successful. `Hostname(config)#show running-config`

1.4.46 Enabling iOS Automatic Pop-up Window Control in WeChat Web-based Authentication

Configuration Effect

Enable iOS clients to support 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 clients can use the WeChat app without login when the device is configured to allow WeChat traffic.

Notes

- iOS automatic pop-up window control must be used on the device that is configured to allow WeChat traffic (run the **web-ctrl free-auth weixin** command to enable this function).
- Redirection performance will deteriorate after iOS automatic pop-up window control is enabled.

- iOS automatic pop-up window control will be invalid when the device is configured to allow traffic from 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 WeChat Web-based Authentication

Command	**http redirect adapter ios**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Check that iOS clients show pop-up windows and display Wi-Fi signal reception during WeChat web-based authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication). iOS clients can use the WeChat app without login when the device is configured to allow WeChat traffic.

Configuration Example

Enabling iOS Automatic Pop-up Window Control in WeChat Web-based Authentication

Configuration Steps	• Enable iOS automatic pop-up window control. • (Optional) The configuration is valid for the WeChat web-based 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`

1.4.47 Enabling Smart WeChat Web-based Authentication

Configuration Effect

When a STA is associated with an SSID for the second time during WeChat web-based authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication), the STA goes online without authentication.

Notes

You need to run the **ip dhcp snooping** command before the smart authentication function takes effect.

Configuration Steps

Enabling the Smart WeChat Web-based Authentication

Command	**web-auth sta-perception enable**

Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Simulate the scenario where a STA is associated with an SSID for the second time during WeChat web-based authentication (including WeChat follow-up authentication and WeChat-based Wi-Fi connection authentication). Check whether the STA goes online without authentication.

Configuration Example

Enabling Smart WeChat Web-based Authentication

Configuration Steps	● Enable smart WeChat web-based authentication. ● The configuration is optional.
	`Hostname(config)#web-auth sta-perception enable`
Verification	● Check whether the configuration is successful. `Hostname(config)#show running-config`

1.4.48 Enabling IPFIX Traffic Upload

Configuration Effect

Configure IPFIX traffic upload. If it is enabled, traffic packets are encapsulated using IPFIX and uploaded to the server.

Notes

This function needs to be used with the IPFIX function.

Configuration Steps

Enabling IPFIX Traffic Upload

Command	**web-auth acct-mtehod ipfix**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Users can be successfully authenticated and go online. Traffic will be encapsulated into IPFIX packets and sent to the server.

Configuration Example

Configuring IPFIX Traffic Upload

Configuration Steps	● Enable IPFIX traffic upload. `Hostname(config)# web-auth acct-method ipfix`
Verification	● Check whether the configuration is successful. `Hostname(config)#show running-config`

1.4.49 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-based authentication server supports transparent transmission of the 0x05 attribute in the following scenarios:

- When the device interworks with a third-party device through the portal protocol of China Mobile, the web-based authentication server encapsulates the error flag into the 0x05 attribute (ErrID) and transparently transmits it to the portal server.
- When the device interworks with a third-party device through Huawei portal protocol 2.0, the web-based authentication server encapsulates information from the third-party authentication device such as the RADIUS server to the 0x05 attribute (TextInfo) and transparently transmits it 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

Command	**web-auth portal-attribute 5**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	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	Enable this function on the portal server (using Huawei portal protocol 2.0) when a device needs to upload information (TextInfo) from a third-party authentication device such as the RADIUS server.

Verification

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`

1.4.50 Configuring Uniqueness Check of Portal Authentication Accounts

Configuration Effect

Configure uniqueness check of portal authentication accounts. After this function is enabled, the web-based 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-based authentication server directly responds to the portal server with ErrCode 2-contained ACK_AUTH. After receiving such response, some portal servers push information about terminal preemption to users.

Notes

This function is disabled by default.

Configuration Steps

- Optional.
- Configure the function when the portal server needs to push information about terminal preemption to users.

Related Commands

Configuring Uniqueness Check of Portal Authentication Accounts

Command	**web-auth portal-valid unique-name**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Configure the function when the portal server needs to push information about terminal preemption to users.

Verification

When finding that the same account is used by another user and is online, the web-based authentication server with this function enabled 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`

1.4.51 Enabling the One-click Configuration Through WeChat

Configuration Effect

Use one command to configure WeChat template information, port control, iOS window display, and MAB 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 Configuration Through WeChat

- Optional.

Command	**web-auth wechat-template** *template-name* **wlan-range** *wlanid-start wlanid-end* **portal-ip** *portal-ip-address* **nas-ip nas-ip-address** [**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*: Applies 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 MAB authentication. **ios-adapter**: Configures the automatic window display function.
Command Mode	Global configuration mode
Usage Guide	Before performing one-click configuration, you must enter the security configuration mode. Otherwise, the device monitoring and management configuration fails to be performed.

Verification

Run the **show run** command to check whether the configuration is normal.

Configuration Example

Enabling the One-click Configuration Through WeChat

Configuration Steps	● Enable the one-click configuration through WeChat.
	`Hostname(config)# web-auth wechat-template aaa interface tenGigabitEthernet 3/2 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.

1.4.52 Configuring NAS-PORT-ID for an AP

Configuration Effect

The Guangdong branch of China Mobile requires that the **NAS-PORT-ID** parameter be configured for each AP. The **NAS-PORT-ID** parameter is carried in portal and RADIUS packets sent to portal and RADIUS servers.

Notes

The **NAS-PORT-ID** parameter can be configured only for single APs.

Configuration Steps

Configuring NAS-PORT-ID for an AP

- Optional.

Command	**nas-port-id** *string*
Parameter Description	*string*: Indicates the NAS-PORT-ID name allocated to an AP.
Command Mode	AP configuration mode
Usage Guide	This command sets the **NAS-PORT-ID** parameter only for single APs. To cancel the configuration, run the **no nas-port-id** command.

Verification

Run the **show ap-config running** command to check whether the configuration is normal.

Configuration Example

Configuring NAS-PORT-ID for an AP

Configuration Steps	● Configure the **NAS-PORT-ID** parameter.
	`Hostname(config)# ap-config ap740` `Hostname(config-ap)# nas-port-id guangdongyidong`
Verification	● Run the **show ap-config running** command to check whether the configuration is successful.

1.4.53 Enabling the Device to Automatically Add a Domain Name to the Authentication Username

Configuration Effect

If second-generation web-based authentication and iPortal web-based authentication are 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 display 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-based 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 the device to automatically add 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)#`

1.4.54 Configuring the App Authentication Template

Configuration Effect

After the template is configured, authentication through WeChat, WeChat Work, and DingTalk can be implemented.

Notes

The configuration commands in template configuration mode are the same as those for WeChat authentication.

Configuration Steps

- Optional.
- This configuration can be performed when authentication through WeChat, WeChat Work, and DingTalk is configured.

Verification

- Run the **show run** command to check whether the configuration is normal.
- Perform authentication through WeChat, WeChat Work, and DingTalk, and check whether the authentication is normal.

Related Commands

↘ Configuring the App Authentication Template

Command	**web-auth template** { **app** | *portal-name* **app** }
Parameter Description	Indicates the name of the user-defined portal server.
Command Mode	Global configuration mode
Usage Guide	The app authentication template is **app** by default.

↘ Applying the App Authentication Template

Command	**web-auth portal** { **app** | *name* }
Parameter Description	Indicates the user-defined template name.
Command Mode	Global configuration mode or WLAN security configuration mode
Usage Guide	The app authentication template is **app** by default.

Configuration Example

Configuring App Authentication

Configuration Steps	● Configure app authentication template on the network device. ● Configure the IP address and service URL of the server on the network device. ● Configure the encryption key (**ruijie**) for communication with the server on the network device. ● Configure the IP address of the device on the network device. ● Apply the app authentication template to WLANSEC1 and enable app authentication.
	Hostname#configure Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#web-auth template app Hostname(config.tmplt.app)#ip 192.168.197.79 Hostname(config.tmplt.app)#service-url wmc.ruijie.com.cn Hostname(config.tmplt.app)#key ruijie Hostname(config.tmplt.app)#nas-ip 1.1.1.1 Hostname(config.tmplt.app)#exit Hostname(config)# wlansec 1 Hostname(config-wlansec)# web-auth portal app Hostname(config-wlansec)# webauth
Verification	● Check whether the web-based authentication configuration is successful.
	Hostname(config)#show running-config web-auth template app ip 192.168.197.79 service-url wmc.ruijie.com.cn http://192.168.197.79:8080/eportal/index.jsp key ruijie nas-ip 1.1.1.1 !... wlansec 1 web-auth portal app webauth !

1.4.55 Configuring ISE Authentication

Configuration Effect

Redirect non-authenticated users to the authentication page for authentication.

Notes

N/A

Configuration Steps

Configuring the Portal Server

- Mandatory. To implement web-based authentication, you must configure and apply a portal server.
- When a device detects that a non-authenticated user attempts to access network resources through HTTP, the device redirects the user's access request to the specified portal authentication page. In this way, the user can initiate an authentication request to the authentication server. The portal server address is configured as a special network resource that does not require authentication. Non-authenticated users can communicate over this address directly through HTTP.

Configuring a Response Mode Used After Successful Authentication

- Optional.
- It is configured as needed.

Configuring the Response Mode Used Upon an Authentication Failure

- Optional.
- It is configured as needed.

Configuring a Mode for the Device to Parse Authentication Requests

- Optional.
- It is configured according to requirements of the interconnected server.

Configuring Whether to Pop Up a Page for Proactive Logout After Successful Authentication

- Optional.
- It is configured as needed.

Configuring the Device's IP Address

- Mandatory. No IP address is configured by default.
- An IP address accessible by users needs to be configured.

Configuring the Device's Port

- Mandatory. No port is configured by default.
- As the port is configured for user access, it must not conflict with the port used by the built-in or web network management system (NMS).

Configuring the URL Used by a STA for Initiating Authentication

- Mandatory. The default URL is **http://***ip***:***port***/login http://ip:port/login**, where *ip* is the device's IP address, and *port* is the device's port.

Enabling Web-based Authentication on a Port

- Mandatory.
- When web-based authentication is enabled on a port, STAs connected to the port will not undergo web-based authentication. Web-based authentication is disabled on a port by default.

Verification

- Non-authenticated users need to be authenticated.
- Authenticated users can use the network normally.

Related Commands

Enabling AAA

Command	**aaa new-model**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Commands related to the AAA method list can be entered only after the function is enabled.

Configuring the Web-based Authentication Method List on AAA

Command	**aaa authentication cpweb** { **default** | *list-name* } *method1* [*method2*...]
Parameter Description	*list-name*: Indicates the name of a method list. *method1*: Indicates method 1. *method2*: Indicates method 2.
Command Mode	Global configuration mode
Usage Guide	ISE authentication is performed by using the ClearPass authentication method. For details, see ClearPass authentication.

Creating a Template

Command	**web-auth template cpweb**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	ISE authentication is performed by using the ClearPass authentication template. For details, see ClearPass authentication.

Configuring the Server's IP Address

Command	**ip** { *ip-address* }
Parameter Description	Indicates the IP address of the portal server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	N/A

Configuring the Server's URL

Command	**url** *url-string*

Parameter Description	Indicates the URL of the authentication page of the portal server.
Command Mode	Web-based authentication template configuration mode
Usage Guide	Log in to the ISE server and click **Portal test URL** on the portal page to obtain the portal page URL in the format similar to https://192.168.197.79:8443/portal/PortalSetup.action?portal=401e25d0-2e02-11e8-ba71-005056872c7f. Replace the question mark (?) in the URL with a pound sign (#). In the **Authentication Success Settings** area, set the URL to that of any valid page to prevent a login success page from being displayed when a STA fails to be authenticated. By default, it is set to **http://www.cisco.com**.

Configuring the Device's IP Address

Command	**web-auth auth-server ip** *ip-address*
Parameter Description	*ip-address*: Configure the access service IP address of the device that performs ISE authentication. The server initiates communication to the IP address.
Command Mode	Global configuration mode
Usage Guide	The access service IP address of the NAS cannot be configured as the passthrough address. When the access service IP address is configured as the IP address of the NAS and a STA in the authentication template accesses this IP address, the NAS intercepts the request of the STA and forwards it to the server. As a result, the STA fails to access the web management page of the NAS. If a STA in the authentication template accesses this IP address for device management, configure the access service IP address as the unused virtual service IP address, for example, 1.1.1.1 and 2.2.2.2.

Configuring the Device's Port

Command	**web-auth auth-server** { **http** | **https** } [**port** *port*]
Parameter Description	Configures the TCP port used by a STA for initiating ISE authentication.
Command Mode	Global configuration mode
Usage Guide	This command configures the TCP port used by a STA for initiating ISE authentication. The port cannot conflict with the port used by the built-in or web NMS.

Configuring the URL Used by a STA for Initiating Authentication

Command	**web-auth auth-server submit-url** *url-string*
Parameter Description	Configures the URL used by a STA for initiating ISE authentication.
Command Mode	Global configuration mode
Usage Guide	This command configures the URL used by a STA for initiating authentication, and the URL must start with **http://**.

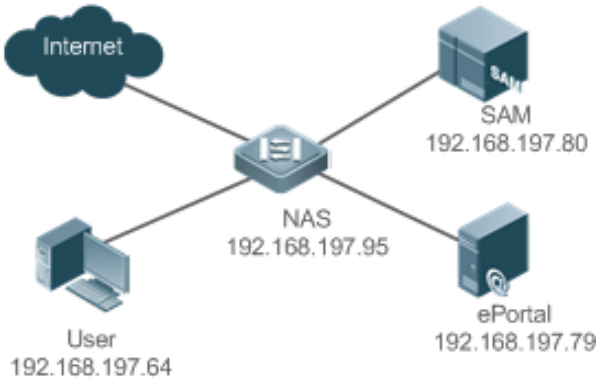
Enabling Web-based Authentication on an Interface

Command	webauth
Parameter Description	N/A
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuration Example

The following configuration example describes the configuration related to web-based authentication only.

ISE Authentication

Scenario Figure 1-14	
Configuration Steps	● Configure the IP address of the authentication server on the network device. ● Configure the homepage address of the authentication page on the network device. ● Configure the IP address of the network device. ● Configure the port of the network device. ● Configure the URL for STA authentication on the network device. ● Enable web-based authentication for WLAN 10 on the network device.

	`Hostname# config`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#web-auth auth-server http port 8082`
	`Hostname(config)#web-auth auth-server ip 1.1.1.1`
	`Hostname(config)#web-auth auth-server submit-url`
	`http://1.1.1.1:8082/login`
	`Hostname(config)#web-auth template cpweb`
	`Hostname(config.tmplt.cpweb)#ip 192.168.197.79`

	`Hostname(config.tmplt.cpweb)#url`
	`https://192.168.197.79:8443/portal/PortalSetup.action#portal=401e25d0`
	`-2e02-11e8-ba71-005056872c7f`
	`Hostname(config.tmplt.cpweb)#exit`

	`Hostname(config)#wlansec 10`
	`Hostname(config-wlansec)# web-auth portal cpweb` `Hostname(config-if-range)# webauth`

	Hostname(config-if-range)#exit
Verification	● Check whether the web-based authentication configuration is successful.
	Hostname(config)# show running-config ... web-auth auth-server ip 1.1.1.1 web-auth auth-server http web-auth auth-server submit-url http://1.1.1.1:8082/login web-auth template cpweb ip 192.168.197.79 url https://192.168.197.79:8443/portal/PortalSetup.action#portal=401e25d0-2e02-11e8-ba71-005056872c7f ... wlansec 10 web-auth portal cpweb webauth
	Hostname#show web-auth control Port Control Server Name Online User Count ------------------------- -------- ---------------------- ------------ ------ wlansec 10 On cpweb 0 ...
	Hostname#show web-auth template Webauth Template Settings: ---------- Name: cpweb Type: cpweb Ip: 192.168.197.79 Url: https://192.168.197.79:8443/portal/PortalSetup.action#portal=401e25d0-2e02-11e8-ba71-005056872c7f

Common Errors

The device's IP address is not configured, causing a redirection failure.

1.4.56 Configuring the Role-based Portal Redirection Template

Configuration Effect

The role-based portal redirection template redirects the clients associated with a certain role when they go online.

Notes

N/A

Configuration Steps

Configuring the Portal Redirection Template

- Mandatory. Configure an available portal redirection template before you bind the role to the portal redirection template.
- When the device finds that the client associated with the role with restricted network access attempts to visit network resources through HTTP, it redirects the access request to the specified portal page. The portal server IP address will be set as an authentication-free network resource, which the clients associated with the role with restricted network access can directly access.

Binding the Role with the Portal Redirection Template

- Mandatory.
- The client associated with the role will be redirected upon access only when the role is bound with the portal redirection template,

Verification

- The client associated with the role with restricted network access is redirected upon access.
- The client associated with the role with no restriction can log in normally.

Related commands

Creating the Template

Command	**web-auth template** *template-name* **rdweb**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Server IP Address

Command	**ip** *ip-address*
Parameter Description	*ip-address*: Indicates the portal server IP address.
Command Mode	Portal template configuration mode
Usage Guide	N/A

Configuring the Server URL

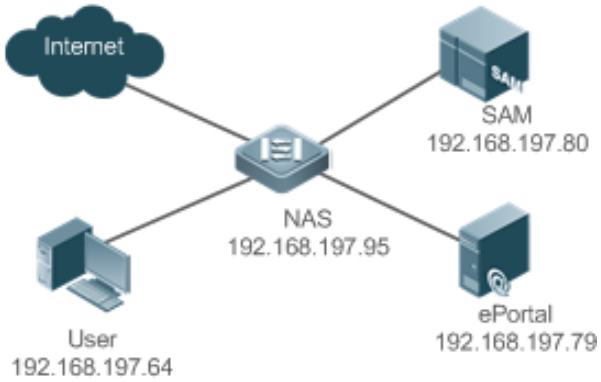
Command	**url** *url-string*
Parameter Description	*url-string*: Indicates the redirect URL of the portal server.
Command Mode	Portal template configuration mode
Usage Guide	N/A

Configuration Example

The following configuration example describes the configuration related to roles only.

Configuring Role-based Portal Redirection Template

Scenario Figure 1-9



Configuration Steps

- Configure the IP address of the redirection server for redirection template **rdweb** on the NAS.
- Configure the URL of the portal page for the redirection template on the NAS.
- Bind role **limit** with redirection template **rdweb**.

```
Hostname# config terminal

Enter configuration commands, one per line.  End with CNTL/Z.

Hostname(config)# web-auth template rdweb

Hostname(config.tmplt.rdweb)# ip 192.168.197.79
```

```
Hostname(config.tmplt.rdweb)# url
http://192.168.197.79:8443/portal/login Hostname(config.tmplt.rdweb)#
exit
```

```
Hostname(config)# user-role limit
```

```
Hostname(config.user-role)# captive-portal rdweb

Hostname(config-if-range)# exit
```

Verification

Run the **show running-config** command to verify the configuration result.

```
Hostname(config)# show running-config

...

web-auth template rdweb

 ip 192.168.197.79

 url http://192.168.197.79:8443/portal/login
```

```
...
user-role limit
 captive-portal rdweb
```

```
Hostname# show web-auth template
Webauth Template Settings:
-------------------------------------------------------------
  Name:          rdweb
  Type:          rdweb
  Ip:            192.168.197.79
  Url:           http://192.168.197.79:8443/portal/login
```

Common Errors

N/A

1.4.57 Configuring the Default Role upon Authentication Success

Configuration Effect

- The client is assigned with the default role after the web authentication succeeds.

Notes

- Create a role before configuring it as the default role.

Configuration Steps

Configuring the Default Role of the Client after the Web Authentication Succeeds

Command	**web-auth default-role** *name*
Parameter Description	*name*: Indicates the role name.
Defaults	No default role is configured by default.
Command Mode	WLAN security configuration mode
Usage Guide	Create a role before configuring it as the default role.

Verification

- Check whether the client is assigned with the default role after the client authentication succeeds.

Configuration Example

Configuring the Default Role

Configuration Steps

- Configure the default role.

```
Hostname(config)# wlansec 1

Hostname(config-wlansec)# web-auth default-role teacher
```

Verification

- Run the following command to verify the configuration result.

```
Hostname(config)# show running-config
```

1.4.58 Configuring Second-Generation Web-based Authentication to Support Direct Access to the Authentication Page

Configuration Effect

When a client accesses the network, the client is allowed to directly access the portal page for authentication, eliminating the need to proactively initiate an HTTP request for redirection.

Notes

- This command applies only to second-generation web-based authentication. After this command is configured, clients are allowed to directly access the authentication page for authentication only in second-generation web-based authentication.
- After this function is enabled in a VAC scenario, if user information of a client associated with a non-active AC is lost when the client accesses the network (for example, run the **clear web-auth user** command to clear user information or user entries time out), the client cannot directly access the authentication page and needs to be redirected to the authentication page by sending a HTTP request.

Configuration Steps

Configuring Second-Generation Web-based Authentication to Support Direct Access to the Authentication Page

Command	**web-auth portal direct-auth**
Parameter Description	N/A
Defaults	Direct access to the authentication page for authentication is not supported by Rijie second-generation web-based authentication.
Command Mode	Global configuration mode
Usage Guide	1. In a VAC scenario, when a client associated with a non-active AC access the network, the client needs to be redirected to the authentication page by sending a HTTP request if user information is deleted due to user entry timeout. Otherwise, the authentication fails. 2. This command takes effect only when second-generation web authentication is used.

Verification

If specified end users do not exist on the AC or fat AP (that is, no specified user is displayed in the output of the **show web-auth user all** command), the user can directly access the authentication page to implement authentication after associating with the network.

Configuration Examples

Configuring Second-Generation Web-based Authentication to Support Direct Access to the Authentication Page

Configuration Steps	Configure second-generation web-based authentication to support direct access to the authentication page for authentication. `Hostname(config)# web-auth portal direct-auth`

Verification	Check whether the configuration is successful.
	`Hostname(config)#show running-config`
	`...`
	`web-auth portal direct-auth`
	`...`
	`!`
	`end`

1.4.59 Importing and Enabling an SSL Certificate

Configuration Effect

- After configuration, the browser will not prompt alarms when the HTTPS protocol is used for redirection in web-based authentication or upon interconnection with the ClearPass server.

Notes

- N/A

Configuration Steps

Importing an SSL Certificate

Command	**web-auth import-ssl** [**auth-server**] { **cert ftp:***path* | **cert tftp:***path* } { **key ftp:***path* | **key tftp:***path* }
Parameter Description	*path*: Indicates the path of the certificate and key.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Enabling the SSL Certificate

Command	**web-auth ssl-policy** { **https-redirect** | **auth-server** }
Parameter Description	**https - redirect:** Enables the HTTPS redirection certificate. **auth-server:** Enables the ClearPass authentication certificate.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- When a user accesses the HTTPS page for redirection in web-based authentication, the browser does not prompt an alarm. When a user submit the username and password to the ClearPass server to initiate authentication, the browser will not prompt an alarm either.

Configuration Examples

Importing and Enabling an SSL Certificate

Configuration Steps	• Import the certificate key. • Enable the certificate.

	`Hostname# web-auth import-ssl auth-server cert tftp://10.104.8.66/cpwebsrv.pem key tftp://10.104.8.66/cpwebkey.pem`
	
	`Hostname(config)# web-auth ssl-policy auth-server`

Verification	• Check whether the configuration is successful.

	`Hostname(config)#show running-config`
	
	`web-auth ssl-policy auth-server`

1.4.60 Configuring the Lowest TLS Version

Configuration Effect

- After configuration, the lowest TLS version for interaction between the device and STA is TLS 1.2 during web authentication redirection for access to the HTTPS page or when the device is connected to the ClearPass server.

Notes

- N/A

Configuration Steps

- Optional.

- Perform the operation based on user requirements.

Verification

- The lowest TLS version for interaction between the device and STA is TLS 1.2 during web authentication redirection for access to the HTTPS page. When the device is connected to the ClearPass server, the lowest TLS version for interaction between the device and STA is TLS 1.2 after the username and password are submitted to initiate authentication.

Related Commands

Setting the Lowest TLS Version for Interaction Between the Device and STA to TLS 1.2

Command	**web-auth ssl-minimum-version tls1.2**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring the TLS Version for Interaction Between the Device and STA

Configuration Steps

- Set the lowest TLS version for interaction between the device and STA to TLS 1.2.

```
Hostname(config)# web-auth ssl-minimum-version tls1.2
```

Verification

- Check whether the configuration is successful.

```
Hostname(config)#show running-config

web-auth ssl-minimum-version tls1.2
```

1.5 Monitoring

Clearing

Command	Description
clear web-auth user { **all** | **id** *session-id* | **ip** *ip-address* | **mac** *mac-address* | **name** *name-string g* | **id** *id-num* }	Disconnects users.
clear web-auth direct-site	Clears all the authentication-free network resources.
clear web-auth direct-host	Clears all the authentication-free users.
clear web-auth acl [**white-url**]	Clears the web-based authentication blocklist and allowlist configuration.
clear web-auth free-acct ip	Clears all authentication-free IP addresses.

Command	Description
clear web-auth free-acct url	Clears all authentication-free URLs.
clear web-auth direct-arp	Clears all authentication-free ARP resources.
clear web-auth user diag	Clears all user tracks.

Displaying

Command	Description
show web-auth acl	Displays the web-based authentication blocklist and allowlist configuration.
show web-auth parameter	Displays basic parameters of web-based authentication.
show web-auth template	Displays the web-based authentication template configuration.
show web-auth direct-host	Displays the authentication-free host range.
show web-auth direct-site	Displays the authentication-free address range.
show web-auth direct-arp	Displays the authentication-free ARP resource range.
show web-auth rdport	Displays the TCP interception port.
show web-auth control	Displays the web-based authentication configuration on a port.
show web-auth user { **all** | **ip** *ip-address* | *ipv6-address* | **mac** *mac-address* **| name** *name-string* | **by-ap** *ap-name* | **by-ap-group** *ap-group-name* }	Displays online information about all users or specified users.
show web-auth portal-check	Displays the web-based authentication portal check information.
show web-auth noise	Displays the noise reduction configuration of web-based authentication.
show web-auth syslog ip *ip-address*	Displays user login and logout records.
show web-auth authmng [**statistic** | **abnormal**]	Displays authentication experience data.
show web-auth auth-server	Displays basic information about the local HTTP server.
show web-auth user diag { **all** | **ip** *ip-address* | **mac** *mac-address* }	Displays track information of all users or a specified user.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug web-auth all	Debugs web-based authentication.
debug web-auth dump memory	Displays memory usage statistics.
debug web-auth dump msg-rate	Displays the processing rate of redirection and authentication requests.

1 Configuring ROLE-MGMT

1.1 Overview

ROLE-MGMT is a component used for user role management on access controllers (ACs)/access points (APs). It is responsible for creating roles on the device. When a wireless client is connected to the network and is assigned a user role, this component maintains the role entries for the client and binds specific policies to the role.

1. Create roles.
2. Assign roles.
3. Bind policies to roles (as described in the *Policy Component Configuration Guide*).

Protocols and Standards

- N/A

1.2 Applications

Application	Description
Role-based Portal Redirection	Controls network access permissions of a client based on its role.
Role-based Key Service Assurance	Configures the key service assurance feature for roles.
Role-based Uplink DSCP Priority Policy Control	Configures DSCP marking for uplink packets from clients under a specific role upon reaching the AP.
Role-based ACL Policies	Configures ACL-based packet filtering for roles.
Role-based Preferred Network Access Policies	Configures role-based QoS policy for wireless applications under a role.
Role-based QoS Policy Control for Wireless Application Recognition	Configures role-based QoS policy for wireless applications under a role.
Role-based VLAN Redirection	Configures role-based VLAN redirection. On a wireless network, different clients access the network and are assigned different roles after successful authentication. If a client access the network after being authenticated through 802.1X authentication (the account and password are correct), the server delivers role information and specifies a VLAN for redirection based on the VLAN information configured in the role.

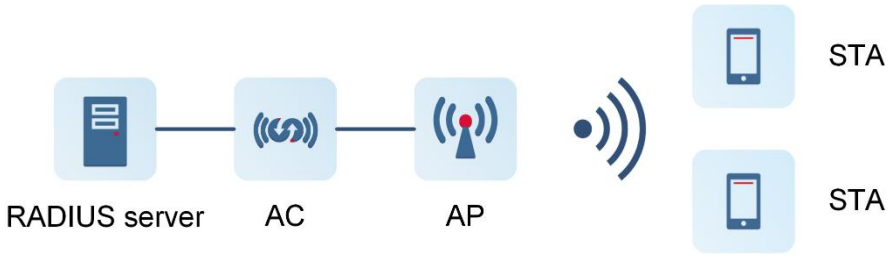
1.2.1 Role-based Portal Redirection

Scenario

On a wireless network, different clients access the network and are assigned different roles after successful authentication. If the role assigned to a client has restricted network access, the client will be redirected to a specified page based on the

configured portal redirection. For example, if a wireless client access the network after being authenticated through 802.1X authentication (the account and password are correct), but the number of accounts exceeds the limit, the client will be prohibited from accessing the Internet. HTTP service requests are redirected to a specified page, and a prompt will be displayed on the page.

The typical topology is as follows:



Deployment

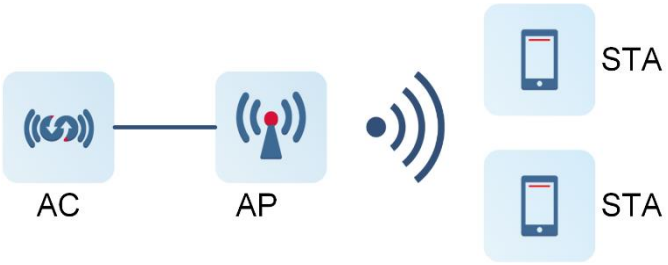
- Configure a portal redirection template (including the URL address and IP address).
- Create a role on the AC for portal redirection. Bind the portal redirection template to the role.
- When a client is connected to the wireless network after being authenticated, the server assign a role to the client (the role name is the name of the role that has been configured with the portal redirection template on the device).

1.2.2 Role-based Key Service Assurance

Scenario

On a wireless network, multiple users may simultaneously contend for air interface resources, causing air interface congestion. The dynamic rate limiting feature can be enabled to restrict client traffic. When a role is configured with key service assurance, users under this role will be guaranteed with higher bandwidth.

The typical topology is as follows:



Deployment

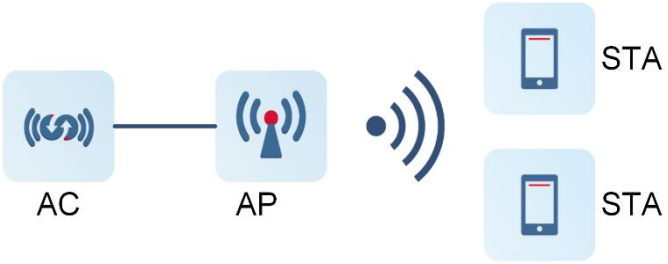
- Enable the Wireless Quality of Service (WQoS) dynamic rate limiting feature.
- Configure role-based key service assurance for a user role.
- Key users will be guaranteed with higher bandwidth when the wireless air interface is congested.

1.2.3 Role-based Uplink DSCP Priority Policy Control

Scenario

A client's uplink traffic reaches an AP through the Wireless Local Area Network (WLAN) and is subsequently forwarded through the wired network. The client's uplink traffic is tagged with a specific DSCP mark when passing through the AP over the WLAN and can be scheduled based on the DSCP priority queue at the core layer of the wired network, thereby ensuring the uplink wired network experience of key users and restricting unnecessary uplink wired forwarding of non-key users.

The typical topology is as follows:



Deployment

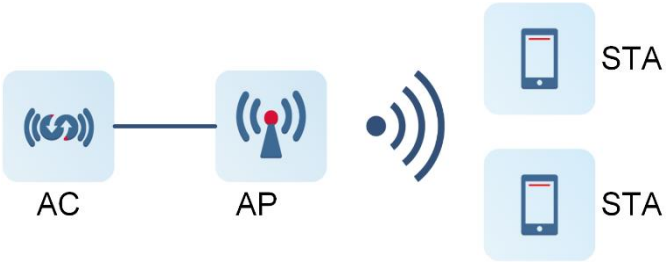
- Configure role-based DSCP priority policy control for a role.
- Configure DSCP marking for uplink packets from clients under this role upon reaching the AP.

1.2.4 Role-based ACL Policies

Scenario

After a client is connected to the network, if the ACL policy has been applied to the associated user role, the client's packets will be filtered and will be either permitted or discarded. Client network access control can be achieved through the ACL policy, such as allowing access only to specified services (for example, allowing access only to WWW and email services while prohibiting others like Telnet), allowing access only within a specified period, or only allowing specific clients to access the Internet.

The typical topology is as follows:



Deployment

- Configure an ACL policy used for filtering packets.

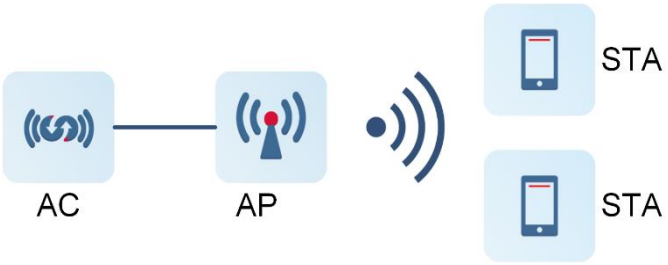
- Apply the created ACL policy to a role.
- When a client is connected to the wireless network and obtains the role's ACL policy, the client is only allowed to access network resources permitted by the ACL.

1.2.5 Role-based Preferred Network Access Policies

Scenario

When a client is connected to the network, if the number of online clients connected to the Radio, AP, WLAN, or AC reaches any of the configured thresholds, the client is allowed to access the network successfully only if the role associated with the client is configured with the preferred network access policy. At the same time, since the number of connected clients has reached the upper limit, the system will force the first user to go offline in order of MAC addresses among non-VIP-FIRST users with poor communication quality or role users not configured with the high-priority access policy.

The typical topology is as follows:



Deployment

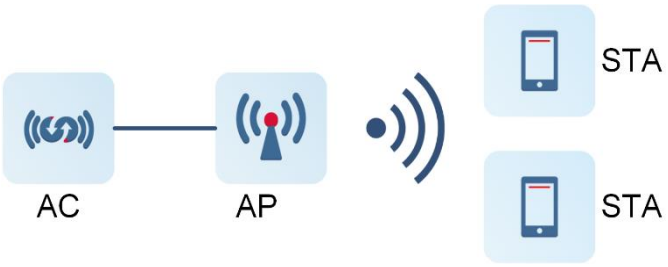
- Configure the role-based preferred network access policy for a role.
- When a user with high-priority network access permissions connects to the Radio, AP, WLAN, or AC under which the number of connected clients has reached the upper limit, the client will be allowed to successfully access the network, and the system will force a user to go offline among non-VIP-FIRST users with poor communication quality or role users not configured with the high-priority network access policy.

1.2.6 Role-based QoS Policy Control for Wireless Application Recognition

Scenario

The application recognition component on the AC can identify applications based on the characteristics of data flows. For different applications of role users, you can set the downlink DSCP value. When packets reach the AP, the WMM function on the AP converts the DSCP value of the packets to the corresponding 802.11e priority, and then schedules the packets based on the priority to implement priority control for different applications. You can configure the device to discard packets of specific applications of a role to block the traffic of unauthorized applications of the role. You can set different rate limits for different applications of a role user. For example, you can limit the rate of download applications to prevent them from occupying excessive bandwidth.

The typical topology is as follows:



Deployment

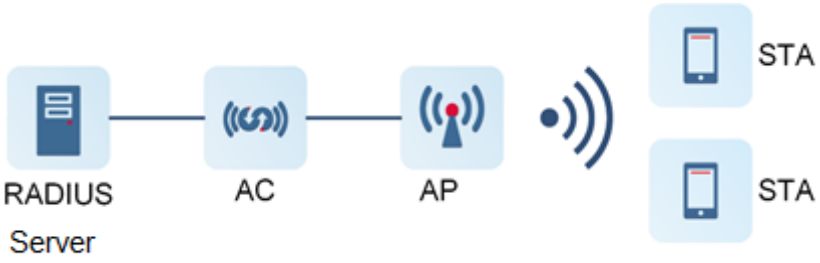
- Configure QoS policy control for wireless applications of the role.
- Perform downlink DSCP priority control, application traffic blocking, and application rate limiting for specified applications on STAs of this role.

1.2.7 Role-based VLAN Redirection

Scenario

On a wireless network, different clients access the network and are assigned different roles after successful authentication. If a client access the network after being authenticated through 802.1X authentication (the account and password are correct), the server delivers role information and specifies a VLAN for redirection based on the VLAN information configured in the role.

The typical topology is as follows:



Deployment

- Create a role on the AC and bind the VLAN to be redirected to the role.
- When a client passes 802.1X authentication and accesses the wireless network, the server assigns a role to the client (the role name is the name of the role configured on the AC).

1.3 Features

Basic Concepts

↘ **User Role**

- Create a user role on the device. The client permission is controlled based on different roles. Up to 256 roles can be created.

Overview

Feature	Description
Role Management	Creates a role on the device and binds a policy to the role.

1.3.1 Role Management

Create a role on the device and maintain role entries for the clients under the role.

Working Principle

The administrator creates a role on the AC and binds a policy (such as a portal template) to the role. When a client accesses the wireless network and is assigned a role, the client will be controlled by the policy bound to the role when accessing the network.

Related Configuration

Configuring a User Role

Use the **user-role** *name* command to create a role.

Use the **captive-portal** { *portal-name* } command to bind a portal template to the role.

Use the **critical-business guarantee enable** command to configure key service assurance for the role.

Use the **user-upstream-dscp** *dscp-value* command to configure an uplink DSCP priority policy for the role.

Use the **access-group** { *acl-id* | *acl-name* } [**priority** *value*] command to configure a role-based ACL policy.

Use the **user-priority-assoc high** command to configure a preferred access policy for the role.

Use the **vlan-id vlan-id** command to configure role-based VLAN redirection.

1.4 Configuration

Configuration	Description and Command	
Role Management	(Mandatory) It is used to create a role.	
	user-role	Creates a role.
	captive-portal	Binds a portal template.
	critical-business guarantee enable	Enables key service assurance.
	user-upstream-dscp	Configures an uplink DSCP priority policy for a role.
	access-group	Configures a role-based ACL policy.
	user-priority-assoc high	Configures a role-based preferred access policy.
	app-profile	Configures a role-based QoS policy profile for wireless application recognition.

	vlan-id	Configures role-based redirection to a specified VLAN.

1.4.1 Role Management

Configuration Effect

- A role should be created first before it is assigned to the client connected to the wireless network.

Precautions

- The assigned role name must have been created on the device.

Configuration Steps

↘ Creating a User Role

- Mandatory.

Command	**user-role** *name*
Parameter Description	*name*: Indicates the name of a role.
Defaults	No custom role exists.
Command Mode	Global configuration mode
Usage Guide	A role needs to be created on the AC before the authentication server assigns the role information.

↘ Binding a Portal Template to a Role

- Mandatory.

Command	**captive-portal** { *portal-name* }
Parameter Description	*portal-name*: Indicates the name of a portal template.
Defaults	No template is bound.
Command Mode	User role configuration mode
Usage Guide	A portal template needs to be created before binding.

↘ Configuring Key Service Assurance

- Mandatory.

Command	**critical-business guarantee**
Parameter Description	N/A
Defaults	Key service assurance is disabled.

Command Mode	User role configuration mode
Usage Guide	1. Before key service assurance is configured, the WQoS dynamic rate limiting feature needs to be enabled. 2. After key service assurance is configured for a role, users associated with this role will be guaranteed with higher bandwidth.

Configuring an Uplink DSCP Priority Policy for a Role

- Mandatory.

Command	**user-upstream-dscp** *dscp-value*
Parameter Description	*dscp-value*: Configures an uplink DSCP value for a role.
Defaults	No uplink DSCP value is configured.
Command Mode	User role configuration mode
Usage Guide	After an uplink DSCP policy is configured for a user role, the uplink packets of the clients associated with this role will be tagged with a specific DSCP value upon reaching the AP. Services of key users are guaranteed through the DSCP policy.

Configuring a Role-based ACL Policy

- Mandatory.

Command	**access-group** { *acl-id* | *acl-name* } [**priority** *value*]
Parameter Description	*acl-id*: Indicate the ID of an ACL. *acl-name*: Indicate the name of an ACL. *value*: Indicates the priority of an ACL. The value range is from 1 to 16. **1** indicates the highest priority, whereas **16** indicates the lowest priority. This parameter is optional. The default value is 16.
Defaults	No ACL is configured.
Command Mode	User role configuration mode
Usage Guide	1. Up to 16 different ACL policies can be configured for a single role. The priority of an ACL can be specified through the **priority** parameter. The **priority** value only specifies the order of ACLs and will not be saved as configuration. 2. Packets are filtered in descending order of the ACL policy priorities. The device stops matching the packets against ACL rules when the packets match one rule. 3. When any ACL rule is applied, it will end with a rule against which all packets will be discarded. If a packet does not match any rules in the ACL, the packet will be discarded.

Configuring a Role-based User Preferred Access Policy

- Mandatory.

Command	**user-priority-assoc high**

Parameter Description	N/A
Defaults	No high-priority network access policy is configured.
Command Mode	User role configuration mode
Usage Guide	1. The high-priority network access permissions of role users have the same priority as the network access permissions of VIP users configured with VIP-FIRST. 2. Since the user role can only be obtained after a client is authenticated, up to 500 clients can be connected to the AC when the number of associated clients has reached the upper limit. If a new user is not configured with high-priority network access permissions and is not a VIP user, the new client will fail to access the network when the number of online clients has reached the upper limit.

Configuring Role-based QoS Policy Control for Wireless Application Recognition

- Mandatory.

Command	**app-profile** *profile-name*
Parameter Description	*profile-name*: Configures the name of the application recognition policy associated with a role.
Defaults	No application recognition policy is associated.
Command Mode	User role configuration mode
Usage Guide	1. After a user role is associated with a wireless application recognition policy, the packets of clients associated with the role will be assigned to the application group of the associated policy and subject to the application group policy. 2. A role and a WLAN are associated with different wireless application recognition policies. If both the role and WLAN match the two policies, the application recognition policy associated with the role is preferentially used. 3. Before associating an application recognition policy with a role, create the application recognition policy.

Configuring Role-based VALN Redirection

- Optional. After a client is authenticated by the server and role information is delivered, the client will be redirected to the VLAN specified based on the role.
- Configure this function after 802.1X authentication is enabled.

Command	**vlan-id** *vlan-id*
Parameter Description	*vlan-id*: Indicates the ID of the VLAN to be redirected for the role.
Defaults	Role-based VLAN redirection is not configured.
Command Mode	Role configuration mode

Usage Guide	1. After this function is configured, if a client passes 802.1X authentication, the server assigns a role to the client and searches for the VLAN ID bound to the role. This VLAN ID must be configured in the VLAN group associated with the WLAN. Otherwise, redirection cannot be performed. 2. The priority of the VLAN bound to the role is lower than that of the VLAN delivered through the RADIUS attribute. 3. After VLAN redirection is enabled for the role in the Change of Authorization (CoA) message, the network is unreachable because the IP address of the client cannot be changed.

Verification

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

Configuration Examples

Binding a Portal Template to a User Role

Configuration Steps	Use this command to configure a portal redirection template.
	Hostname(config)#web-auth template rdweb Hostname(config.tmplt.rdweb)#ip 10.10.10.10 Hostname(config.tmplt.rdweb)#url http://10.10.10.10/warning Use this command to create a user role and configure the portal redirection template for the role. Hostname(config)#user-role limit Hostname(config.user-role)#captive-portal rdweb

Configuring Key Service Assurance for a User Role

Configuration Steps	Use this command to enable the dynamic rate limiting feature.
	Hostname(config)#ap-config all Hostname (config-ap)#smart-rate-control enable Use this command to create a user role and configure key service assurance for the role. Hostname(config)#user-role teacher Hostname(config.user-role)#critical-business guarantee

Configuring an Uplink DSCP Priority Policy for a User Role

Configuration Steps	Use this command to create a user role and set the uplink DSCP priority of this role to 56. Hostname(config)#user-role teacher Hostname(config.user-role)#user-upstream-dscp 56

Configuring a Role-based ACL Policy for a User Role

Configuration Steps	Use this command to configure an ACL.

	Hostname(config)#ip access-list standard 1 Hostname (config-std-nacl)#permit host 1.1.1.1 Hostname(config-std-nacl)#exit Hostname(config)#ip access-list standard 2 Hostname (config-std-nacl)#permit host 1.1.1.1 Use this command to create a user role and apply the ACL to the role. Hostname(config)#user-role test Hostname(config.user-role)#access-group 1 Hostname(config.user-role)#access-group 2 priority 1 Use this command to display the configured ACL. Hostname(config.user-role)#show this Building configuration... ! access-group 2 access-group 1 ! end

Configuring a Preferred Access Policy for a User Role

Configuration Steps	Use this command to create a user role and configure a high-priority access policy for the role. Hostname(config)#user-role teacher Hostname(config.user-role)#user-priority-assoc high

Configuring Role-based QoS Policy Control for Wireless Application Recognition

Configuration Steps	Set the **teacher** role to associate with the **P-Tencent** application recognition policy. Hostname(config)#user-role teacher Hostname(config.user-role)#app-profile P-Tencent

Configuring Role-based VLAN Redirection

Configuration Steps	Create a user role and configure the VLAN ID to be redirected based on the role.
	Hostname(config)#user-role teacher Hostname(config.user-role)# vlan-id 2

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show user-role	Displays the role information of a client.
show access-group [**role** *role-name*]	Displays the ACL policy information of a role.
show role priority-assoc	Displays high-priority access permissions of a role.

Debugging

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

Command	Description
debug role-mgmt event	Enables event debugging.
debug role-mgmt error	Enables serious error debugging.

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. This allows the access control and network security services to be transmitted on one device, meeting diversified access and security control requirements in various scenarios.

Typical access control services include 802.1X authentication, web-based authentication, Address Resolution Protocol (ARP) check, and IP source guard (IPSG). Network security services include Access Control List (ACL), Network Foundation Protection Policy (NFPP), ARP anti-spoofing, and others. When two or more preceding access control or network security services are simultaneously enabled on a device, the SCC coordinates these services based on 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

Application	Scenario
Access Control of Extended Layer 2 Campus Networks	Students on a campus network can access the Internet through 802.1X client authentication or web-based authentication. ARP spoofing between the students needs to be prevented. In addition, clients of some departments (such as the principal's office) can access the Internet without authentication.

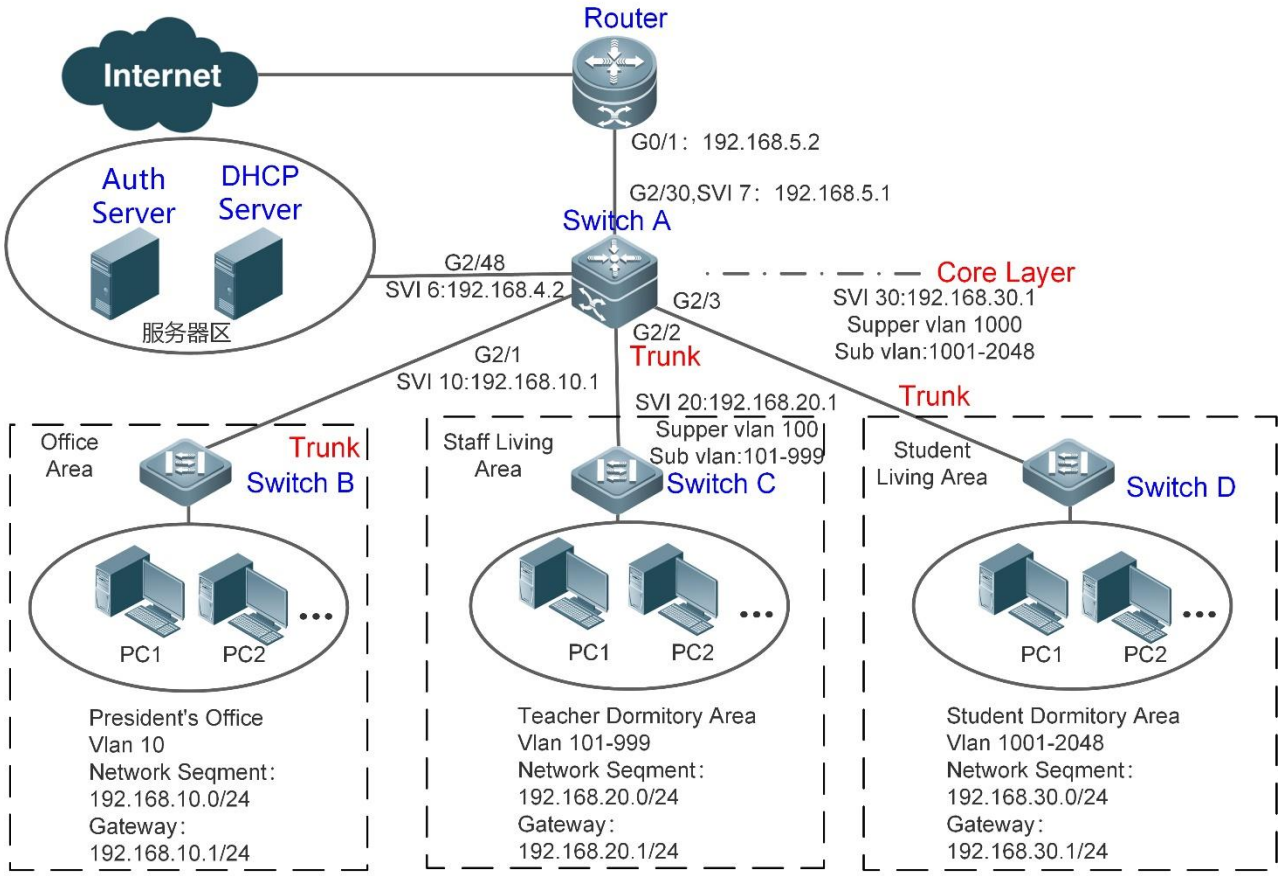
1.2.1 Access Control of Extended Layer 2 Campus Networks

Scenario

Students on a campus network usually need to pass 802.1X or web-based authentication before accessing the Internet to facilitate accounting and guarantee security of a university.

- The students can access the Internet through 802.1X client authentication or web-based authentication.
- ARP spoofing between the students needs to be prevented to guarantee network stability.
- Clients of some departments (such as the principal's office) can access the Internet without authentication.

Figure 1-1



Notes	A traditional campus network is hierarchically designed with the access layer, aggregation layer, and core layer, in which the access layer performs user access control. On an extended Layer 2 campus network, however, user access control is performed by a core switch that is directly connected to access switches without any aggregation device deployed. The ports between the core switch and access switches (switches B, C, and D in Figure 1-1) are all trunk ports. Switches B, C, and D connect to PCs of various departments through access ports, and VLANs correspond to sub-VLANs configured on the downlink ports of the core switch. Therefore, access users are located in different VLANs to prevent ARP spoofing. Core switch A connects to various servers, such as the authentication server and DHCP server. Super-VLANs and sub-VLANs are configured on the downlink ports. One super-VLAN is associated with 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 is (or a group of access users are) allocated to one VLAN. Ports on each access switch that connect to downlink users are configured as access ports, and one VLAN is assigned to each access user based on VLAN planning. The core switch does not forward ARP request packets and replies to ARP request packets from authenticated users only to prevent ARP spoofing. On core switch A, user VLANs are configured as sub-VLANs, super-VLANs are configured, and Switched Virtual Interfaces (SVIs) corresponding to the super-VLANs are configured as user gateways.

- On downlink ports of the core switch (switch A in this example) that connect to access switches of the teachers' living area and students' living area, both 802.1X and web-based authentication are enabled. Users can freely select either authentication mode for Internet access.
- A special department (the principal's office in this example) can be allocated to a particular VLAN that is configured as an authentication-free VLAN, so users of this department can access the Internet without authentication.

1.3 Basic Concepts

IPv4 User Capacity

To ensure network stability for online users and stable operation of devices, you can limit the number of IPv4 access users.

The number of IPv4 access users is not limited by default. A large number of authenticated users are allowed to go online until the number of online users reaches the maximum value allowed by the hardware.

IPv4 access users include 802.1X authentication users (such as authorized IP users), web-based authentication users, and users with manually configured IP addresses (including IP source guard and ARP check).

User Online Status Detection

For user accounting, accounting starts immediately after the user passes authentication and goes online. The accounting process does not end until the user actively goes offline. Some users, however, forget to get offline after stopping Internet access, or cannot go offline because of client problems. Then the users suffer economic losses as the accounting process continues. To more precisely determine whether a user is online, we can preset a traffic value. When the user's traffic is lower than the preset value or no traffic is detected in a given period of time, the device considers that the user is not accessing the Internet and therefore disconnects the user.

Overview

Feature	Description
IPv4 User Capacity	Limit IPv4 user capacity on a specified interface to ensure network stability for online users.
User Online Status Detection	Specify whether to detect traffic of online users and automatically disconnect a user when the user traffic is lower than a preset value in a given period of time.
User Policy Rules	Parse the name of a control policy to obtain corresponding policy rules that will take effect after the rules are enforced.

1.3.1 IPv4 User Capacity

To ensure stable operation of the device and prevent brute-force attacks by unauthorized users, limit the total number of IPv4 access users on a specific interface.

Working Principle

If the number of IPv4 access users is limited, new users exceeding the limit are not allowed to access the network.

By default, the device does not limit the number of IPv4 access users, and the number of access users depends on the hardware capacity of the device.

The IPv4 access users in this context include IPv4 authorized users generated by 802.1X authentication, web-based authentication, and various binding functions. The limit on IPv4 access users is configured on a per-interface basis, so the limit involves both IPv4 users generated on the interface and globally generated IPv4 users. For example, if the maximum number of IPv4 access users is configured as 2 on Gi 0/1, and a command is used to bind one IPv4 user and then one global IPv4 user on the interface, the actual number of access users on this interface has reached the maximum value of 2. In this case, binding another IPv4 user on this interface or another global IPv4 user will fail.

1.3.2 User Online Status Detection

After stopping Internet access, a user may forget to go offline or cannot actively get offline due to client faults. In this case, the user will keep being charged and therefore suffer economic loss. To protect benefits of users on the Internet, the device detects whether the users are online. If the device considers that a user is not online, the device will proactively disconnect the user.

Working Principle

A specific detection interval is preset on a device. If a user's traffic is lower than a certain value in this interval, the device considers that the user is not accessing the network and therefore directly disconnects the user.

- User online status detection applies only to users that go online through 802.1X or web-based authentication.

1.3.3 User Policy Rules

After a user is successfully authenticated, a server may assign control policy names to the user. The SCC needs to parse these control policy names to obtain corresponding policy rules that will take effect after they are installed.

Working Principle

Configure a policy name on a device and configure a specific rate limit policy and filtering policy for the policy name. After a user passes authentication and the policy name is associated with the user, the corresponding rate limit policy and filtering policy will take effect.

You can also apply a filtering policy to a user group to control the user group based on the policy.

- One filtering policy can be associated with only one ACL.
- The filtering policy that is referenced by a user group cannot be modified or deleted.
- A policy can be configured only for users that go online through 802.1X or web-based authentication.

1.4 Configuration

Configuration	Description and Command	
Configuring the IPv4 User Capacity	(Optional) It is used to limit the number of access users on a specific interface.	
	[**no**] **nac-author-user maximum**	Configures the maximum number of IPv4 users that can connect to an interface.
Configuring User Online Status Detection	(Optional) It is used to specify whether to enable user online status detection.	
	offline-detect interval threshold	Configures parameters of user online status detection.
	no offline-detect	Disables user online status detection.
	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 the rate limit policy configuration mode.
	upstream average-rate burst-rate	Configures the average value and burst value for uplink traffic.
	no upstream	Deletes the uplink traffic limit configuration.
	downstream average-rate burst-rate	Configures the average value and burst value for downlink traffic.
	no downstream	Deletes the downlink traffic limit configuration.
	[**no**] **filter-policy**	Enters the filtering policy configuration mode.
	filter_acl	Configures a security ACL associated with a filtering policy.
	no filter_acl	Deletes a security ACL associated with a filtering policy.
	[**no**] **service-policy**	Enters the user policy configuration mode.
	rate-policy apply	Configures a rate limit policy to be used.
	no rate-policy	Deletes a rate limit policy in use.
	filter-policy apply	Configures a filtering policy to be used.
	no filter-policy	Deletes a filtering policy in use.

1.4.1 Configuring the IPv4 User Capacity

Configuration Effect

The maximum number of access users that can connect to an interface can be limited by configuring the IPv4 user capacity.

Notes

N/A

Configuration Steps

Configuring the IPv4 User Capacity

- (Optional) To limit the maximum number of access users that can connect to an interface, you must configure the IPv4 user capacity. The maximum number of access users that can connect to an interface is not limited by default. If the maximum number of access users is configured and the number of authenticated users reaches the limit on an interface, new users cannot be authenticated or go online until a user logs off.
- It is configured on the access device.

Command	**nac-author-user maximum** *max-user-num* **no nac-author-user maximum**
Parameter Description	**no**: Indicates that the IPv4 user capacity limit is canceled on an interface. *max-user-num*: Indicates the maximum number of IPv4 users on a specified interface. The value range is from 1 to 1,024.
Defaults	The maximum number of access users that can connect to an interface is not limited by default.
Command Mode	Interface configuration mode
Usage Guide	You can use this command to limit the number of IPv4 access users on a specified interface.

Verification

You can use the following methods to verify the configuration of the IPv4 user capacity on an interface:

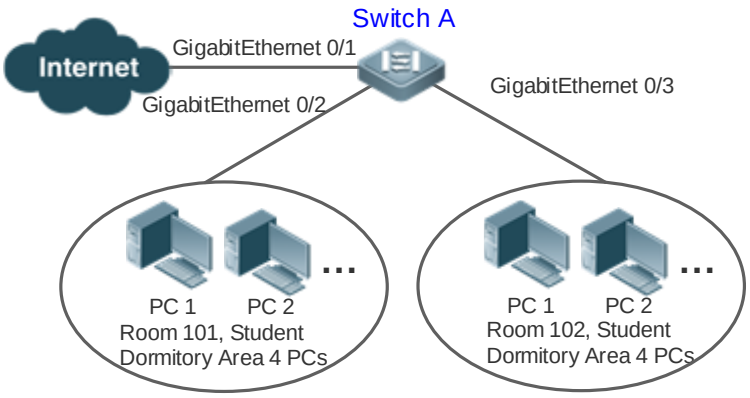
- In 802.1X authentication mode, configure the maximum number of 802.1X authentication clients on an interface. Check whether a new user can be authenticated and go online successfully.
- In web-based authentication mode, configure the maximum number of web-based authentication clients on an interface. Check whether a new user can be authenticated and go online successfully.
- Run the **show nac-author-user** [**interface** *interface-name*] command to check the IPv4 user capacity configuration on the device.

Command	**show nac-author-user** [**interface** *interface-name*]
Parameter Description	*interface-name*: Indicates the interface name.
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	Global configuration mode

Configuration Example

The following configuration example describes SCC-related configuration only.

Limiting the Number of IPv4 Users on an Interface to Prevent Excessive Network Traffic Caused by Many Internet Devices

Scenario **Figure 1-2**	
Configuration Steps	● Assume that the 802.1X authentication environment on switch A has been configured. Enable 802.1X authentication on GigabitEthernet 0/2. ● Set the maximum number of IPv4 users on GigabitEthernet 0/2 to 4.
Switch A	`SwitchA(config)#int GigabitEthernet 0/2` `SwitchA(config-if-GigabitEthernet 0/2)#nac-author-user maximum 4`
Verification	● Authenticate and connect four PCs in the dormitory using 802.1X authentication. Then try to connect an additional terminal to the network and attempt to perform 802.1X authentication to check whether the terminal can be successfully authenticated. ● Run the **show nac-author-user** command to check whether the configuration takes effect.

Switch A	`SwitchA(config)#show nac-author-user`
	`Port Cur_num Max_num`
	`-------- ------- -------`
	`Gi0/1 0 4`

1.4.2 Configuring User Online Status Detection

Configuration Effect

After user online status detection is configured, if a user's traffic falls below the threshold within a given period of time, the device will automatically disconnect the user to prevent unnecessary economic loss due to continuous accounting.

Precautions

Typically, a user's client runs software such as 360 Total Security by default. The software sends packets sometime. Therefore, if you configure user logout when no traffic is detected, the user will be disconnected only when the user's client is powered off.

Configuration Method

↘ Configuring User Online Status Detection

- Optional. By default, a user will be disconnected if the user's client does not generate traffic for 8 hours.

- You can configure user online status detection on an access, aggregation, or core device based on the user distribution. This configuration takes effect only on the configured device but not other devices on the same network.

If **thredshold** is set to **0**, zero-traffic detection is performed.

Command	**offline-detect interval** *interval* **threshold** *threshold* **no offline-detect** **default offline-detect**
Parameter Description	*interval*: Indicates the offline status detection interval, in minutes. The value range is from 1 to 65,535. The default value is 8 hours, that is, 480 minutes. *threshold*: Indicates the traffic threshold, in bytes. The value range is from 0 to 4,294,967,294. The default value is 0, indicating that a user is disconnected when no traffic of the user is detected. **no offline-detect**: Disables user online status detection. **default offline-detect**: Restores the default value. That is, an online user will be disconnected if no traffic of the user is detected for 8 hours.
Defaults	8 hours
Command Mode	Global configuration mode
Usage Guide	Use this command to configure user online status detection. That is, an online user will be disconnected when its traffic is lower than a specified threshold within a specified period of time. Use the **no offline-detect** command to disable user online status detection, or use the **default offline-detect** command to restore the default detection mode.

Verification

You can use the following method to check the configuration effect of authenticated user online status detection:

- When user online status detection is configured and a user goes online on a client, power off the authenticated client. Wait for a while, and run the online user query command associated with 802.1X or web-based 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 to Disconnect a User That Does Not Generate Traffic Within 5 Minutes

Scenario **Figure 1-3**	
Configuration Steps	● Enable 802.1X authentication on Gi 0/2 and configure authentication parameters. MAC address authentication is used. ● Configure user online status detection and specify that a user needs to be disconnected if the user's client does not generate traffic within 5 minutes.
Switch A	`sw1(config)# offline-detect interval 5 threshold 0`
Verification	● Perform 802.1X authentication through an SU client on a PC of the R&D department. The user gets online on the PC. Then power off the PC. Wait for 6 minutes, and run the online user query command corresponding to 802.1X authentication on switch 1 to confirm that the user on the PC is already offline.
Switch A	`sw1(config)#show running-config | include offline-detect` `offline-detect interval 5`

1.4.3 Configuring User Policy Rules

Configuration Effect

When a policy name is applied to an authenticated user, rate limiting can be performed on the user based on the configured policy rule.

Notes

An authentication server is required to assign corresponding policy attributes.

A filtering policy can be associated only with one security ACL.

Configuration Steps

↘ **Configuring User Policy Rules**

- Optional.
- Configure the rate limit policy and filtering policy first. Then specify the name of the rate limit policy in a user policy rule.

The burst limit values for uplink and downlink traffic must be larger than or equal to the average rate limits.

Command	**rate-policy** *name* { **downstream** | **upstream** } **average-rate** *avg-threshold* **burst-rate** *burst-threshold*
Parameter Description	*name*: Indicates the name of a rate limit policy. *avg-threshold*: Indicates an average rate limit, in kbps. The value ranges from 8 to 261,120. *burst-threshold*: Indicates a burst limit, in kbps. The value ranges from 8 to 261,120. The burst limit must be larger than or equal to the average rate limit.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	A rate limit policy rule 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 a security ACL associated with a filtering policy. *acl-id*: Indicates the ID of a security ACL associated with a filtering policy.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	A filtering policy rule 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 a rate limit policy to be used. *filter-name*: Indicates the name of a filtering policy to be used.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	The rate limit policy rule and filtering policy rule can be used in a user policy rule only after they are configured.

Verification

You can check the configuration effect of a policy rule as follows:

- After a rate limit policy rule is configured and a user goes online after authentication, check the rate limit policy entry corresponding to Wireless Quality of Service (WQoS).

- After a filtering policy rule is configured and a user goes online after authentication, check the ACL entry applied to the user corresponding to an ACL key (ACLK).
- Run the **show running** command to display the user policy configuration.

Configuration Example

Specifying a Rate Limit Policy for an Authenticated User Through a User Policy Rule

Configuration Steps	• Enable web-based authentication on WLAN 1 and configure a user policy name on a server. • Configure a user policy rule and associate it with a specified rate limit policy.

Switch A	`AC(config)# rate-policy user-rate`
	`AC(config-rate-policy)#upstream average-rate 10 burst-rate 10`
	`AC(config-rate-policy)#downstream average-rate 10 burst-rate 10`
	`AC(config)# ip access-list extended user_2000`
	`AC(config)# filter-policy user-filter`
	`AC(config-filter-policy)#filter-acl user_2000`
	`AC(config)# service-policy user-policy`
	`AC(config-service-policy)# rate-policy user-rate apply`
	`AC(config-service-policy)# filter-policy user-filter apply`

Verification	• After a user passes authentication, display uplink and downlink rates of the user.

1.5 Monitoring

Clearing

Command	Description
clear scc event diag [**ap-mac** *mac-address*]	Clears the AP event trajectory information recorded by the SCC.

Displaying

Command	Description
show nac-author-user [**interface** *interface-name*]	Displays information about IPv4 user entries on a specified interface.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug scc event	Debugs the SCC running process.
debug scc user [**mac** | **author** | **mac**]	Debugs SCC user entries.

debug scc acl-show summary	Debugs the ACL summary of all services stored in the SCC.
debug scc acl-show all	Debugs all ACLs stored in the SCC.
debug scc event diag [**ap-mac** *mac-address*] [**type** *type-id*]	Displays event tracks stored in the SCC.
debug scc dump msg-rate [**type** *type-id*]	Displays the rate of messages received by the SCC.
debug scc jemalloc	Displays SCC memory statistics.

Configuring the Number of Logs or Messages to Be Recorded

Command	Description
scc event diag { **log-num** *log-num-count* | **msg-num** *msg-num-count* }	Configures the maximum number of logs and messages that can be recorded by the SSC.

1 Configuring GSN

1.1 Overview

Global Security Network (GSN) is a security policy platform that provides security policy management such as access control and network security. The GSN platform involves the security switch and server. The RG Security Policy Management Platform (RG-SMP) server acts as the security policy server for GSN.

GSN accepts policies assigned by the SMP server, enforces the policies on devices, and determines whether to allow specific data packets to pass through the security device. The security policies are as follows:

- Binding: Binds the IP address and MAC address of an authenticated user on a device.
- Isolation or blocking: Allows or prevents specific data by configuring an Access Control List (ACL).

GSN is used with the SMP server, 802.1X authentication, and web-based authentication.

1.2 Applications

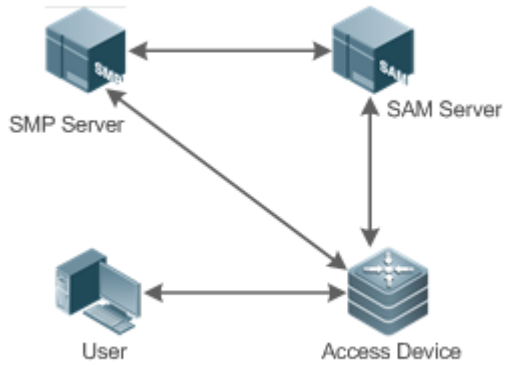
Application	Description
GSN Security Protection for Authenticated Users	After a user passes 802.1X authentication, the SMP server assigns security policies (such as ARP guard and device integrity) to maintain the user's network security.

1.2.1 GSN Security Protection for Authenticated Users

Scenario

After a user passes 802.1X authentication, the SMP server learns the IP-MAC binding of this user from the Security Account Manager (SAM) server and then assigns security policies to the access device.

Figure 19-1



Remarks	Process description: 1. The user passes 802.1X authentication. 2. The SAM server reports user information to the SMP server.

	3. After successful authentication, the access device determines whether to adopt the address binding policy for the user based on the configuration. 4. The user exchanges packets with the SMP server in real time, and the access device converts the packet format and forwards the packets. 5. The SMP server assigns security policies to the access device based on information reported by the user. 6. The SMP server periodically or manually synchronizes policies with the access device. If the SMP server finds that the policies maintained on itself are different from those on the access switch, it deletes all policies on the access device, and then installs all its policies onto the access device. 7. During steps 3, 5, and 6, the access device synchronizes and installs the policies based on policies of GSN.

Deployment

- Enable 802.1X authentication on the access device and deploy the SAM server.
- Deploy the SMP server and add the access device to receive security policies assigned.
- Enable GSN and address binding on the access device.

1.3 Features

Basic Concepts

Ruijie Security Solution

Ruijie security solution is composed of the following entities:

- RG-SMP platform
- RG Security Agent
- RG Restore System
- RG security switch

RG-SMP Platform

Based on the configured policies, the RG-SMP platform determines whether to allow data packets specified in a certain range to pass through the RG security switch. To install policies is to configure policies on a device, and to uninstall policies is to remove policies from a device.

RG Security Agent

RG Security Agent is a type of software running on each device connected to an enterprise network. It collects device information, identifies users' network behaviors, monitors network communication and security status of the devices, and sends collected information to the RG-SMP platform so that the administrator can make security policies accordingly. RG Security Agent automatically downloads new security policies from the RG-SMP platform and enforces specified security policies locally.

RG Restore System

RG Restore System handles abnormal behaviors as follows:

For the users that do not meet requirements of enterprise security policies, the administrator presets policies on the RG-SMP platform to shield most network access permissions of the non-authorized users and retain only one security channel. The security

channel can only connect to enterprise security policy upgrade servers, including the Windows patch upgrade server, antivirus upgrade library server for antivirus software, or other upgrade servers.

When detecting that security policies of a device do not meet the security levels defined by the RG-SMP platform, RG Security Agent immediately uploads its security logs to the RG-SMP platform. The RG-SMP platform selects one policy from the preset policy set based on the alarm logs sent by RG Security Agent, and sends this policy to all RG security switches. After accepting the latest policy configuration, RG security switches immediately apply the configuration so that the user reporting the alarm can access only the specified upgrade server based on restoration operations specified by the SMP server and automatically install patches.

When the user completes all restoration operations specified by the SMP server, RG Security Agent checks security of the RG-SMP platform again. If the user meets requirements of all security policy sets, RG Security Agent notifies the RG-SMP platform to cancel the access limitation on this user and configure the user as a common user.

RG Security Switch

As a component of Ruijie security solution, the RG security switch receives policies from the RG-SMP platform, installs policies, and controls users based on the installed policies.

1.4 Configuration

Configuration	Description and Command	
Configuring GSN Basic Functions	(Mandatory) It is used to enable GSN on an access device and communication with the SMP server.	
	security gsn enable	Globally enables GSN. GSN is disabled by default.
	security { [**v1** | **v2c**] **community** *community* | **v3 user** *username* }	Configures the name of the security authentication mechanism used for communication with the SMP server.
	smp-server host *ip-address*	Configures the IP address of the SMP server.
	(Optional) It is used to configure the minimum interval for transmitting security events.	
	security event interval *interval*	Configures the minimum interval for transmitting security events. The value range is from 1 to 65,535 seconds. The default value is 5 seconds.
Enabling WLAN-based Address Binding	(Optional) It is used to enable address binding on a WLAN.	
	gsn address-bind	Enables WLAN-based address binding. This policy is disabled by default.

1.4.1 Configuring GSN Basic Functions

Configuration Effect

- Globally enable GSN on devices.
- Enable devices to communicate with the SMP server.

Notes

- You can configure SNMPv1, SNMPv2, or SNMPv3 as the name of the security authentication mechanism for communication with the SMP server.
- **security v1 community** and **security community** are both used to configure SNMPv1 to facilitate user configuration. If SNMPv3 is selected, you must configure SNMPv3 users under the **snmp-server** command. For details about configuration commands, see *Configuring SNMP*.
- The number of entries supported by GSN cannot be exceeded.

Configuration Steps

Globally Enabling GSN

- Mandatory.
- Unless otherwise specified, enable GSN on each device that requires the security solution.

Enabling Communication with the SMP Server

- Mandatory.
- Unless otherwise specified, enable this function on each device that requires the security solution to communicate with the SMP server.

Configuring the IP Address of the SMP Server

- Mandatory.
- Unless otherwise specified, configure the IP address of the SMP server on each device that requires the security solution to communicate with the SMP server.

Configuring the Minimum Interval for Transmitting Security Events

- To prevent unauthorized users from frequently sending security events to attack the RG security switch and the SMP server by sending bogus security events, you can configure the minimum interval for transmitting security events to restrict users from reporting security events.
- To change the default minimum interval for transmitting security events, run the **security event interval** *interval* command. The default interval is 5 seconds.

Related Commands

Globally Enabling GSN

Command	**security gsn enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Communication with the SMP Server

Command	**security** { [**v1** | **v2c**] **community** *community* | **v3 user** *username* }

Parameter Description	**community** *community*: Specifies the name of the security authentication mechanism for communication with the SMP server. **user** *username*: Indicates the name of an SNMPv3 user.
Command Mode	Global configuration mode
Usage Guide	**security v1 community** and **security community** are both used to configure SNMPv1 to facilitate user configuration. If SNMPv3 is selected, you must configure SNMPv3 users under the **snmp-server** command. For details about configuration commands, see *Configuring SNMP*.

Configuring the IP Address of the SMP Server

Command	**smp-server host** *ip-address*
Parameter Description	*ip-address*: Specifies the IP address of the SMP server.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Minimum Interval for Transmitting Security Events

Command	**security event interval** *interval*
Parameter Description	**interval** *interval*: Specifies the minimum interval for transmitting security events, in seconds. The value ranges from 1 to 65,535. The default value is 5s.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Enabling GSN and Communication with the SMP Server

Configuration Steps	● Globally enable GSN on the device. ● Configure the name of the security authentication mechanism for devices to communicate with the SMP server. ● Configure the IP address of the SMP server.

	`Hostname# configure terminal`
	`Hostname(config)# security gsn enable`
	`Hostname(config)# security v1 community test-name`
	`Hostname(config)# smp-server host 192.168.30.9`
	`Hostname(config)# exit`

Verification	Run the following **show** commands: ● Run the **show smp-server** command to display the IP address of the SMP server. ● Run the **show security event interval** command to display the minimum interval for transmitting security events.
	`Hostname# show smp-server`

	SMP-Server IP:192.168.30.9 Hostname# show security event interval Event sending interval(Seconds):5

Common Errors

- Routes to the SMP server are unreachable.

1.4.2 Enabling WLAN-based Address Binding

Configuration Effect

- Enable address binding on a WLAN.

Notes

This function takes effect only when GSN is globally enabled and the WLAN security mode is set to Wi-Fi Protected Access (WPA) or WPA2.

You need to disable 802.1X-based IP address authorization before enabling GSN. GSN and 802.1X-based IP address authorization cannot be enabled simultaneously. Otherwise, security policies will be affected.

Configuration Steps

Enabling WLAN-based Address Binding

- To enable address binding based on a WLAN, run the **gsn address-bind** command.

Related Commands

Enabling WLAN-based Address Binding

Command	**gsn address-bind**
Parameter Description	N/A
Command Mode	WLAN security configuration mode
Usage Guide	N/A

Configuration Example

Enabling WLAN-based Address Binding

Configuration Steps	● Create a WLAN. ● Enter the WLAN security configuration mode. ● Enable WLAN-based address binding.
	Hostname# configure terminal Hostname(config)# wlansec 100 Hostname(config-wlansec)# gsn address-bind Hostname(config)# exit

1.5 Monitoring

Displaying

Command	Description
show smp-server	Displays the IP address of the SMP server.
show security event interval	Displays the minimum interval for transmitting security events.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug gsn { **all** | **error** | **event** | **packet** | **server** | **detail** }	Debugs GSN.

Configuring WLAN QoS

1. Configuring WLAN QoS
2. Configuring WMM
3. Configuring Web App

1 Configuring WLAN QoS

1.1 Overview

Wireless LAN Quality of Service (WLAN QoS), also known as WQoS, is a technology for controlling wireless bandwidth. It includes rate limiting, fair scheduling, and Intranet proxy prevention.

Rate limiting is employed to limit traffic of access points (APs), WLAN, or stations (STAs), thus preventing the traffic from exceeding a specified range. It is useful in scenarios where some STAs consume excessive bandwidth, leaving others with inadequate resources.

Fair scheduling, which evenly allocates time resources, addresses issues where some nodes monopolize air interfaces for extended periods, especially low-rate nodes. This mechanism is beneficial for optimizing all types of wireless networks.

In some cases, an authorized STA connected to a wireless network may be utilized as a proxy server by unauthorized STAs, allowing them to connect without proper authorization. Intranet proxy prevention is designed to counter this behavior, ensuring that unauthorized proxy servers are excluded from the intranet environment. This feature is crucial in scenarios where unauthorized access through proxy servers needs to be mitigated.

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 Control in a Fit AP Architecture	A Fit AP architecture is deployed with at least one access controller (AC) and one AP.

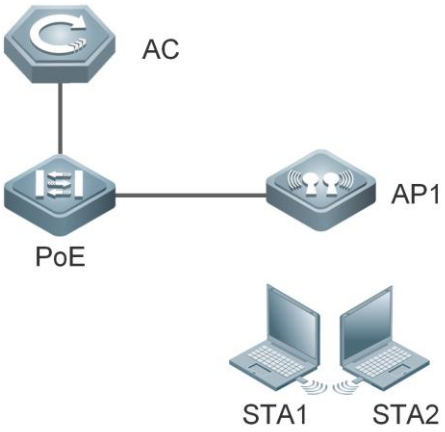
1.2.1 Bandwidth Control in a Fit AP Architecture

Scenario

On a wireless network, an AC is deployed to implement rate limiting on APs, WLANs, and STAs, and fair scheduling and intranet proxy prevention on APs.

As shown in Figure 1-1, the AC implements rate limiting on the AP, WLAN, and STAs, and fair scheduling and intranet proxy prevention on the AP.

Figure 1-1



Remarks	AC: wireless access controller PoE: gateway (switch)for AP1

Deployment

- Enable WQoS on the AC.

1.3 Features

Basic Concepts

Rate Limiting

In order to optimize the utilization of limited network resources and efficiently cater to a larger user base, the access device must support rate limiting. When traffic rates comply with the committed rates, packets are allowed to pass through; otherwise, they are discarded.

Traffic is evaluated based on the following parameters:

- Average data rate: It is the average flow rate that is allowed, also known as the committed information rate (CIR).
- Burst data rate: It is the maximum acceptable rate of each burst data, referred to as the committed burst size (CBS). The configured CBS must be greater than the maximum packet length, which equates to the highest data transmission rate within a 10-millisecond interval. The CBS, measured in kbps, is calculated as the maximum traffic within a period divided by 10 milliseconds.

Bypassing Rate Limiting for the Downlink Packets with the Differentiated Services Code Point (DSCP) Value in the Specified Range

To bypass rate limiting on the downlink traffic of key applications, you can mark the downlink packets of key applications with the specified DSCP value using an application-based QoS policy, thereby prioritizing forwarding of critical application traffic.

Fair Scheduling

Fair scheduling ensures that STAs within the same AP's frequency band equitably share wireless network resources provided by the AP. This function effectively prevents low-speed STAs from compromising the overall throughput of the wireless network, resulting in a smoother network experience for all connected STAs. Additionally, the fair scheduling feature intelligently monitors traffic changes for each STA and dynamically adjusts the proportion of wireless bandwidth

allocated to maintain optimal performance. Starting from software version 10.4(1T19)p1 and later, you can configure different priorities for STAs in fair scheduling, allowing specific users to enjoy preferential access to the wireless bandwidth.

Intranet Proxy Prevention

Software versions later than 10.4(1T19)p1 incorporate a mechanism specifically designed to detect STAs acting as proxy servers for other STAs within a wireless intranet. This enables accurate monitoring of the number of such STAs and their associated network traffic.

Dynamic Rate Limiting

Dynamic rate limiting is achieved based on the channel utilization, ensuring that the channel utilization remains within a proper range.

Overview

Feature	Description
Rate Limiting	Limit the rates of an AP, a WLAN, or a STA to ensure that the rate does not exceed the limit.
Bypassing Rate Limiting for the Downlink Packets with the DSCP Value in the Specified Range	Enables the downlink packets with the DSCP value in the specified range to bypass STA rate limiting.
Fair Scheduling	Allow STAs associated with an AP in the same frequency band to share wireless network resources provided by the AP, thus equitably sharing the bandwidth of the wireless network.
Intranet Proxy Prevention	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.
Dynamic Rate Limiting	Dynamically adjust STA rate limit based on channel utilization.
Uplink Congestion Control	When the delay of key services reaches the threshold and the packet transmission duration of heavy-traffic TCP background services in the uplink reaches the threshold, dynamic adjustment is performed to reduce the volume of the uplink data sent by STAs, ensuring user experience of key services.

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 the limit.

Working Principle

Rate limiting is enforced using a token bucket mechanism, which operates as follows:

- The token bucket maintains a record of the allowable number of bytes that can pass within a specific time period.
- During each interval, the permitted number of data bytes is determined based on the configured CIR and CBS, thereby adjusting the token bucket's capacity.
- Upon the arrival of a packet at the device, its byte count is compared against the token bucket size. If the packet size is smaller than the token bucket capacity, the packet is permitted to pass, and the token bucket size is

reduced. If the packet size exceeds the token bucket capacity, it can be handled in two ways: traffic shaping or traffic policing. Traffic shaping buffers the packet and continues transmission once the token bucket issues a permit notification. Conversely, traffic policing directly discards the packet. The traffic shaping algorithm ensures smoother and less volatile traffic, while the traffic policing algorithm leads to more variable traffic patterns.

- On an AP, traffic shaping is used to implement rate limiting for the AP, a STA, or a WLAN. On an AC, traffic monitoring is used to implement rate limiting for a WLAN.

1.3.2 Bypassing Rate Limiting for the Downlink Packets with the DSCP Value in the Specified Range

This function enables the downlink traffic with the DSCP value in the specified range to bypass STA rate limiting when the traffic exceeds the threshold.

Working Principle

The locally or centrally forwarded packets are marked with the specified DSCP value through the DSCP-based QoS policy on the AP. The downlink packets can also be marked with the DSCP value on the wired devices. If the DSCP value of the downlink packets is within the specified DSCP range, these downlink packets will bypass STA rate limiting.

1.3.3 Fair Scheduling

Fair scheduling, which evenly allocates time resources, addresses issues where some nodes monopolize air interfaces for extended periods, especially low-rate nodes.

Working Principle

Due to the unique characteristics of wireless networks, STAs (including APs) within the same network share air interface resources, which can become a bottleneck for STA performance. This stands as one of the key distinctions between wired and wireless networks. Traditional packet scheduling typically follows a first in, first out (FIFO) approach. On a wireless network, each STA seeking to transmit data strives to seize air interface resources whenever possible. Transmission of numerous low-rate packets can lead to prolonged occupation of the air interfaces. Consequently, persistent queue occupancy results in packet loss and degrades overall network performance.

In real-world wireless scenarios, STAs often vary in type and performance. As a result, some STAs consistently struggle to obtain resources and experience significantly delayed responses. Even worse, these STAs may fail to access the network altogether, severely impacting user experience.

Addressing these issues necessitates ensuring that every STA can fairly obtain resources on the air interfaces. This means that each STA requiring data transmission should be able to occupy the air interfaces for a fair duration. Achieving fair scheduling of wireless links involves several steps: predicting the traffic of each STA based on STA-specific information (such as negotiated rates and aggregation types), converting the traffic into the number of packets that can be transmitted by each STA, adjusting the allowed packet count to allocate bandwidth to each STA over the air interfaces, and implementing traffic shaping. Through fair scheduling, each STA occupies the air interfaces for an equitable duration, effectively averting poor performance of certain STAs and thereby enhancing user experience.

1.3.4 Intranet Proxy Prevention

When an authorized STA that is connected to a wireless network, it can be used as a proxy server by other STAs, which may allow unauthorized STAs to connect to the network without permission. To address this issue, intranet proxy prevention measures can be implemented.

Working Principle

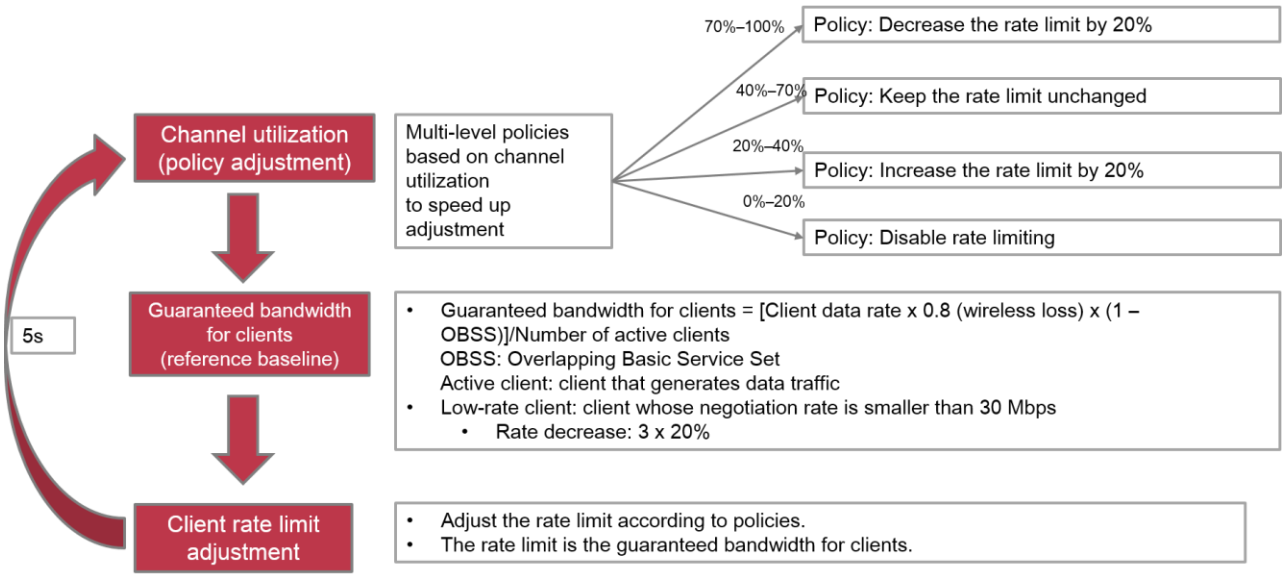
Internet proxy prevention is mainly used to determine whether a packet from a STA meets requirements of a proxy server. If not, the STA is contained. The AP supports the TTL detection policy: Detects whether the TTL in an IP packet sent by a STA to the AP is within the proper range. If the TTL is out of the range, the STA is used as a proxy server.

1.3.5 Dynamic Rate Limiting

Dynamic rate limiting, as compared to traditional rate limiting, only requires the configuration of a switch, with no need for specifying bandwidth limits for individual STAs. In a multi-STA scenario, traditional rate limiting struggles to limit rates when they are high, while air interface resources remain underutilized during idle times when rates are low. Dynamic rate limiting, on the other hand, enables stricter rate limiting to be applied to STAs when multiple users preempt air interfaces and loose rate limiting to be applied to STAs when the air interfaces are less busy. This ensures that air interface resources are appropriately allocated while maintaining a positive network experience for users.

Working Principle

Figure 1-2



The AP adopts a dynamic rate limiting policy based on channel utilization, which includes four levels:

- 70%–100%: The rate limit is decreased by 20%.
- 40%–70%: The rate limit stays unchanged.
- 20%–40%: The rate limit is increased by 20%.
- 0%–20%: Rate limiting is disabled.

The channel and client information is collected periodically to determine the guaranteed bandwidth for each client, as well as identify low-speed clients. The rate limit values are adjusted using the rate limiting algorithm.

After you specify the key clients for dynamic rate limiting, they are allocated with higher guaranteed bandwidth.

After you enable application guarantee for dynamic rate limiting, the critical application group is allocated with higher guaranteed bandwidth. When the air interface is congested, the rate of the suppression application group is limited first.

1.3.6 Uplink Congestion Control

After AP uplink congestion control is enabled, if the delay of key services reaches the threshold and the packet transmission duration of heavy-traffic TCP background services in the uplink reaches the threshold within a unit time (1s), the receiver window (RWND) in the TCP ACK packets will be dynamically adjusted. This process takes about 5s to 10s. After the adjustment is completed, the volume of the uplink data sent by STA is reduced to ensure user experience of key services.

Working Principle

The channel utilization (CU) is used to determine whether a channel is congested. It is used to measure the transmit (Tx/downlink) CU and receive (Rx/uplink) CU values of a local AP, as well as the CU values (uplink and downlink) of co-channel neighboring APs. If a CU value exceeds the threshold, it is considered that congestion is caused by greedy traffic.

Uplink congestion control is implemented based on the TCP backpressure technology. When an AP detects that uplink congestion is caused by greedy services, the AP sends a TCP ACK packet to the STA and reduces the RWND. The STA determines the volume of data to be transmitted based on the congestion window (CWND), buffer, and RWND.

1.4 Configuration

Configuration	Description and Command	
Configuring Rate Limiting	⚠ (Mandatory) It is used to enable rate limiting.	
	ap-based	Configures AP-based rate limiting on an AC.
	netuser	Configures STA-based rate limiting on an AC.
	wlan-based	Configures WLAN-based rate limiting on an AC.
Enabling the Downlink Packets with the Specified DSCP Value in the Specified Range to Bypass STA Rate Limiting	⚠ (Optional) Enables the downlink packets with the specified DSCP value in the specified range to bypass STA rate limiting.	
	wqos skip-rate-limit dscp	Configures the DSCP range of downlink packets which bypass STA rate limiting.
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	⚠ (Mandatory) It is used to configure an intranet proxy prevention policy and enable	

Configuration	Description and Command	
Prevention	intranet proxy prevention detection.	
	illegal-sta-check ip ttl	Enables intranet proxy prevention with the TTL detection policy.
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 the associated rate threshold for low-speed STAs.
	smart-rate-control config rate-limit-step	Configures the rate limiting factor.
	smart-rate-control config sampling	Configures timer parameters.
	smart-rate-control config threshold channel-using	Configures channel utilization thresholds.
	smart-rate-control config threshold link-rate-divisor	Configuring the STA association rate factor.
	smart-rate-control config threshold rate-guard	Configures the threshold for guaranteed bandwidth.
	smart-rate-control config threshold rate-limit	Configures the rate limiting scope.
	smart-rate-control config wlan-loss	Configures wireless loss.
	smart-rate-control config user mac	Configures the MAC address of the key client for dynamic rate limiting.
	smart-rate-control config user weight	Configures the guaranteed bandwidth weights of the key clients and of the ordinary clients respectively.
	smart-rate-control config application guarantee	Configures application guarantee for dynamic rate limiting.
	smart-rate-control config application weight	Configures the guaranteed bandwidth weights of the critical application group, of the ordinary application group, and of the suppression application group respectively.
Configuring Uplink Congestion Control	(Optional) It is used to configure uplink congestion control.	
	congestion-control tcp enable	Enables uplink congestion control.
	congestion-control tcp threshold cu [up | down]	Configures the channel utilization threshold for uplink congestion control.
	congestion-control tcp threshold delay	Configures the delay threshold for uplink congestion control.
	congestion-control tcp threshold upstream	Configures the threshold of uplink traffic volume for uplink congestion control.
	congestion-control tcp window-optimize hold-time	Configures the window optimization duration for uplink congestion control.
	congestion-control tcp dscp	Configures the DSCP threshold for

Configuration	Description and Command	
		background traffic in uplink congestion control.

1.4.1 Configuring Rate Limiting

Configuration Effect

- Only the committed resource is allocated to a flow based on the network situation, which prevents network congestion caused by burst traffic.

Notes

- Rate limiting provided by the **wlan-based per-ap-limit** command configured on an AC is equivalent to that of the **wlan-qos wlan-based total-user-limit** command configured on all connected APs.
- The following types of rate limiting are available on STAs: **wlan-based per-user-limit**, **wlan-based per-ap-limit intelligent**, **ap-based per-user-limit**, **ap-based total-limit intelligent**, and **netuser**. However, only one type of rate limiting is available at a time. The following types of rate limiting are 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**.
- Rate limiting, including **wlan-based total-limit**, **wlan-based per-ap-limit**, **ap-based total-limit**, and STA-based rate limiting, can take effect on different objects simultaneously without considering priorities.

Configuration Steps

↘ Configuring AP-based Rate Limiting

- Mandatory.
- Configure rate limiting per single user on an AC in AP configuration mode.

Command	**wlan-qos ap-based** { **per-user-limit** | **total-user-limit** [**intelligent**] } { **down-streams** | **up-streams** } *average-data-rate* **burst-data-rate** *burst-data-rate*
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 for downlink traffic on the AP. **up-streams**: Indicates that rate limiting is implemented for uplink traffic on the AP. *average-data-rate*: Indicates the CIR. The unit is 8 kbps. The value range is from 8 to 261120. *burst-data-rate*: Indicatesthe CBS. The unit is 8 kbps. The value range is from 8 to 261120.
Defaults	By default, rate limiting is not configured. If **total-user-limit** is configured, intelligent rate limiting is disabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

- In AP configuration mode on the AC, configure rate limiting for the AP.

Command	**ap-based total-user-limit** { **down-streams** | **up-streams** } **intelligent**

Parameter Description	**total-user-limit**: Indicates that rate limiting is applied to the AP. **intelligent**: Indicates whether to enable or disable intelligent rate limiting for total users. **down-streams**: Sets the rate limit for downlink traffic on an AP. **up-streams**: Sets the rate limit for uplink traffic on an AP.
Defaults	It is disabled by default.
Command Mode	AP configuration mode
Usage Guide	N/A

Configuring STA-based Rate Limiting

- Mandatory.
- On an AC, run the **wlan-qos netuser** command in AC configuration mode to configure STA-based rate limiting.

Command	**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 for uplink traffic on a STA. **outbound**: Indicates that rate limiting is implemented for downlink traffic on a STA. *average-data-rate*: Indicates the CIR. The unit is 8 kbps. The value range is from 8 to 261120. *burst-data-rate*: Indicates the CBS. The unit is 8 kbps. The value range is from 8 to 261120.
Defaults	By default, rate limiting is not configured.
Command Mode	AC configuration mode
Usage Guide	N/A

Configuring WLAN-based Rate Limiting

- Mandatory.
- On an AC, run the **wlan-based** command in WLAN configuration mode to configure WLAN-based rate limiting.

Command	**wlan-based** { **per-user-limit** | **total-user-limit** | **per-ap-limit** } { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Indicates that rate limiting is implemented on every STA on a WLAN. **total-user-limit**: Indicates that rate limiting is implemented on all STAs on a WLAN. **intelligent**: Indicates whether rate limiting is implemented on all STAs on a WLAN intelligently. **per-ap-limit**: Indicates that AP-based rate limiting is implemented. **down-streams**: Indicates that rate limiting is implemented for downlink traffic on a WLAN. **up-streams**: Indicates that rate limiting is implemented for uplink traffic on a WLAN. *average-data-rate*: Indicates the CIR. The unit is 8 kbps. The value range is from 8 to 261120. *burst-data-rate*: Indicates the CBS. The unit is 8 kbps. The value range is from 8 to 261120.
Defaults	By default, rate limiting is not configured.
Command Mode	WLAN configuration mode
Usage Guide	N/A

- Configure per-AP intelligent rate limiting for a WLAN.

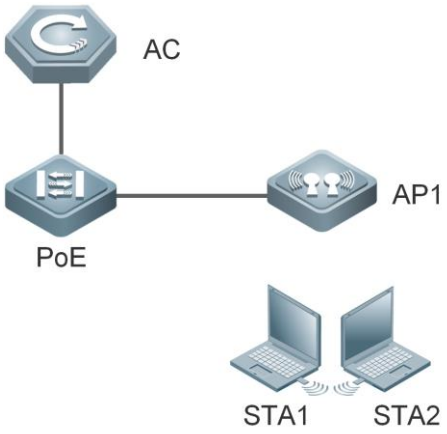
Command	**wlan-based per-ap-limit** { **down-streams** | **up-streams** } **intelligent**
Parameter Description	**down-streams**: Sets rate limiting parameters for downlink traffic on a WLAN. **up-streams**: Sets the rate limiting parameters for uplink traffic on a WLAN. **intelligent**: Indicates whether to enable or disable intelligent rate limiting for total users.
Defaults	No rate limiting is configured by default.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

- Run the **show dot11 ratelimit ap** command to display AP-based rate limiting information.
- Run the **show dot11 ratelimit user** command to display STA-based rate limiting information.
- Run the **show dot11 ratelimit wlan** command to display WLAN-based rate limiting information.

Configuration Example

Configuring AP-based Rate Limiting

Scenario **Figure 1-2**	
Configuration Steps	● In AP configuration mode, configure AP-based rate limiting for downlink traffic.

AC	`Hostname#configure terminal`
	`Hostname(config)# ap-config ap1`
	`Hostname(config-ap)#ap-based per-user-limit down-streams average-data-rate 100000 burst-data-rate 120000`
	`Hostname(config-ap)# exit`

Verification	● Run the **show dot11 ratelimit ap** command to display the configuration.

AC	`AC_20_3F#show dot11 ratelimitap`
	`AP name :test, ratelimit info(unit :8kbps):`
	`Per-user-limit:`
	`  Upstream  : average rate - 0 , burst rate - 0`
	`  Downstream : average rate - 100000, burst rate - 120000`
	`Total-user-limit:`
	`  Upstream  : average rate - 0 , burst rate - 0`

	Downstream : average rate - 0 , burst rate - 0

1.4.2 Enabling the Downlink Packets with the Specified DSCP Value in the Specified Range to Bypass STA Rate Limiting

Configuration Effect

The downlink packets with the DSCP value within the specified range bypass STA rate limiting.

Notes

- Configure this function in the AP configuration mode or all-AP configuration mode on the AC.
- The DSCP range of the packet which bypasses rate limiting includes start and end values.
- The DSCP end value cannot be smaller than the start value, or the configuration fails.
- When the DSCP policy is configured in both all-AP configuration mode and AP configuration mode, the configuration in the AP configuration mode takes precedence.

Configuration Steps

↘ Enabling the Downlink Packets with the Specified DSCP Value in the Specified Range to Bypass STA Rate Limiting

- Optional.
- Run the **wqos skip-rate-limit dscp** command on the AC.

Command	**wqos skip-rate-limit dscp** *dscp-start dscp-end*
Parameter Description	*dscp-start*: Configures the start value of the DSCP range with which the packets bypass STA rate limiting. The value ranges from 0 to 63. *dscp-end*: Configures the end value of the DSCP range with which the packets bypass STA rate limiting. The value ranges from 0 to 63.
Default	This function is disabled by default.
Command Mode	AP configuration mode and all-AP configuration mode on the AC
Usage Guide	The DSCP end value must be equal to or greater than the DSCP start value.

Verification

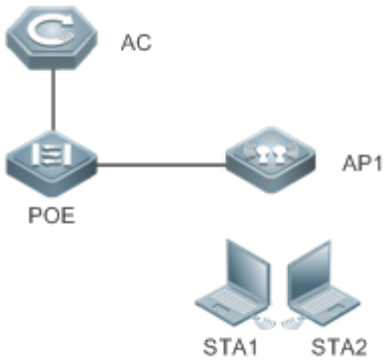
- Run the **show running-config** command to display the DSCP range in the all-AP configuration mode.
- Run the **show ap-config running** command to display the DSCP range in the AP configuration mode.

Configuration Example

↘ Enabling the Downlink Packets with the Specified DSCP Value to Bypass STA Rate Limiting

Network Scenario

Figure 1-74



Configuration Steps

Enable the downlink packets with the DSCP value in the range from 56 to 63 to bypass STA rate limiting.

```
Hostname# ap-config all
Hostname(config-ap)# wqos skip-rate-limit dscp 56 63
```

Verification

Run the **show running-config** command to display the DSCP range of the packet which bypasses STA rate limiting.

```
Hostname# show running-config | include skip-rate-limit
 wqos skip-rate-limit dscp 56 63
```

Common Errors

N/A

1.4.3 Configuring Fair Scheduling

Configuration Effect

- The fair scheduling function prevents low-speed STAs from compromising the overall throughput of the wireless network, resulting in a smoother network experience for all connected STAs

Notes

- In Fit AP mode, configure fair scheduling only on an AC.

Configuration Steps

↘ Enabling Fair Scheduling

- Mandatory.
- On an AC, run the **fair-schedule** command in AP configuration mode to enable fair scheduling.
- Fair scheduling evenly allocates time resources to STAs.

Command	**fair-schedule**
Parameter Description	N/A
Defaults	By default, fair scheduling is enabled.

Command Mode	AP 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 an AC, run the **sta-fair** command in AC configuration mode to configure the fair scheduling priority.

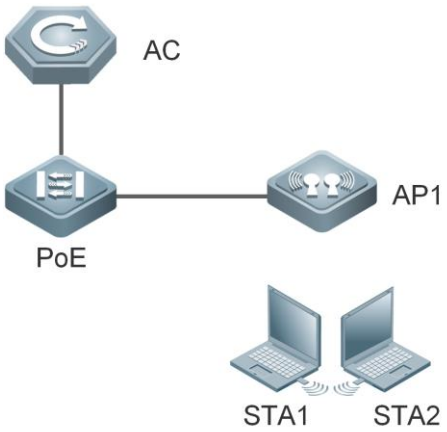
Command	**sta-fair** *mac-address* **priority** *priority*
Parameter Description	*mac-address*: Indicates the MAC address of a STA. *priority*: Indicates the priority. The value range is from 1 to 6.
Defaults	By default, the priority is 1 for all STAs. A greater value indicates a higher priority, and a higher priority indicates longer time allocated to a STA.
Command Mode	AC configuration mode
Usage Guide	Whether this parameter is supported and the value range of this parameter depend on the product version.

Verification

- Run the **show ap-config run** command to display the configuration.

Configuration Example

Enabling Fair Scheduling and Configuring the Priority

Scenario **Figure 1-3**	
Configuration Steps	● In AP configuration mode, enable fair scheduling. ● In AC configuration mode, configure the fair scheduling priority of a STA.

AC	`Hostname#configure terminal`
	`Hostname(config)# ap-config ap1`
	`Hostname(config-ap)#fair-schedule`
	`Hostname(config-ap)# exit`
	`Hostname(config)#ac-controller`
	`Hostname(config-ac)#sta-fair 1111.1111.1111 priority 6`
	`Hostname(config-ac)# end`

Verification	● Run the **show ap-config running** and **show running-config** commands to display the

	configuration.

AC	`Hostname# show ap-config running`
	`!`
	`ap-configap1`
	`!`
	`Hostname# show running-config`
	`!`
	`ac-controller`
	`sta-fair 1111.1111.1111 priority 6`
	`!`

1.4.4 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.
- 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.

↘ Enabling Intranet Proxy Prevention and Using the TTL Detection Policy

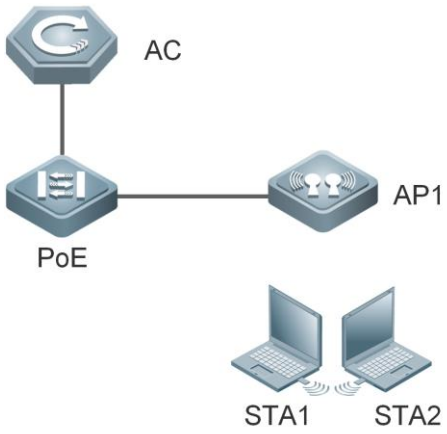
Command	**illegal-sta-check ip ttl**
Parameter Description	N/A
Defaults	By default, intranet proxy prevention is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

↘ Enabling Intranet Proxy Prevention

Scenario **Figure 1-4**	
Configuration Steps	● Enable intranet proxy prevention in AP configuration mode.

AC	`Hostname#configure terminal`
	`Hostname(config)# ap-config ap1`
	`Hostname(config-ap)# illegal-sta-check ip ttl`
	`Hostname(config-ap)# end`

Verification	● Run the **showap-config running** command to display the configuration.

AC	`Hostname# show ap-config running ap1`
	`!`
	`ap-configap1`
	` illegal-sta-check ip ttl`
	`!`

Common Errors

N/A

1.4.5 Configuring Dynamic Rate Limiting

Configuration Effect

- Dynamic rate limiting adjusts STA rate limits based on channel utilization, keeping air interface utilization below 70%.

Notes

- In a scenario where the APs supporting dynamic rate limiting and APs not supporting dynamic rate limiting are deployed, the APs supporting dynamic rate limiting will be suppressed.

Configuration Steps

↘ Enabling Dynamic Rate Limiting Function

- Optional.
- On the AC, run the **smart-rate-control enable** command in AP configuration mode.

Command	**smart-rate-control enable**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Configuring Dynamic Rate Limiting Parameters

- Configure the associated rate threshold for low-speed STAs.

Command	**smart-rate-control config low-rate-sta** *rate-num*
Parameter Description	*rate-num*: Indicates the threshold for the associated rate of a low-speed STA. The value range is from 1 to 500000, in kbps.
Defaults	The default value is 30000, which means the associated rate threshold is 30 Mbps.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	When the associated rate of a STA is lower than the threshold for low-speed STAs, the STA is considered as a low-speed STA. When the rate limiting factor is adjusted by using the **smart-rate-control config rate-limit-step** command, the adjustment result for low-speed STAs is different from that for non-low-speed STAs. 1. When you increase 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 one third of the configured rate limiting factor, that is, 1/3 multiplied by *increase-percent*. 2. When you reduce the rate limiting factor, for non-low-speed STAs, the percentage reduction is as configured. For low-speed STAs, the actual reduction factor is three times the configured factor, that is, 3 multiplied by *reduce-percent*.

- 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 value for increasing the rate limiting factor. The value range is from 1 to 100. *reduce-percent*: Indicates the value for reducing the rate limiting factor. The value range is from 1 to 100.
Defaults	By default, the value for increasing the rate limiting factor is 20 and the value for reducing the rate limiting factor is 20.
Command Mode	AP configuration mode or all-AP 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 range is from 1000 to 10000. *times-num*: Configures the data sampling count before rate adjustment is triggered. The value range

	is from 1 to 100.
Defaults	By default, the sampling period is 1000 ms and the data sampling count is 5.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	The timer configuration takes effect in the next scheduling period, with a waiting time of 0 to **period** multiplied by **times**.

- Configure the channel utilization threshold.

Command	**smart-rate-control config threshold channel-using** { **busy** *busy-num* | **free** *free-num* }
Parameter Description	*busy-num*: Configures the threshold percentage for busy channel utilization. The value range is from 1 to 100. *free-num*: Configures the threshold percentage for free channel utilization. The value range is from 1 to 100.
Defaults	By default, the thresholds for busy channel utilization and free channel utilization are 70 and 40 respectively.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	Ensure that the thresholds for busy channel utilization and free channel utilization are in descending order.

- Configuring the STA association rate factor.

Command	**smart-rate-control config threshold link-rate-divisor** *divisor*
Parameter Description	*divisor*: Indicates the STA association rate factor. The value range is from 16 to 256.
Defaults	64
Command Mode	AP configuration mode or all-AP configuration mode on the AC Global configuration mode on the AP
Usage Guide	After dynamic rate limiting is enabled, if the bandwidth for key users in a multi-user scenario is not effectively guaranteed, increase the STA association rate factor to compromise the minimum guaranteed bandwidth of non-key users, thereby enhancing the bandwidth for key users. This improves network experience of key users in a multi-user scenario. The minimum guaranteed bandwidth for a STA is calculated as follows: (uplink negotiation rate + downlink negotiation rate) x 0.5/*divisor.*

- Configure the threshold for guaranteed bandwidth.

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 range is from 8 to 261120.
Defaults	By default, the threshold is not configured.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	1. After the threshold is configured, 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 – Wireless loss))/Number of STAs

- 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, in the unit of 8 kbps. The value range is from 8 to 261120. *min-num*: Configures the minimum rate limit, in the unit of 8 kbps. The value range is from 8 to 261120.
Defaults	By default, the maximum rate limit is 25000 and the minimum rate limit is 8.
Command Mode	AP configuration mode and all-AP configuration mode
Usage Guide	1. If the rate limit is greater than the maximum value, the maximum rate limit is canceled. 2. The rate limit cannot be smaller than the minimum value.

- 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 range is from 1 to 100.
Defaults	The wireless loss is 20% by default.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

- Configure the MAC address of the key client for dynamic rate limiting.

Command	**smart-rate-control config user mac** *H.H.H*
Parameter Description	*H.H.H*: Configures the MAC address of the client whose bandwidth is to be guaranteed.
Defaults	No MAC address of the key client is configured by default.
Command Mode	AP configuration mode and all-AP configuration mode on the AC and global configuration mode on the AP
Usage Guide	N/A

- Configure the guaranteed bandwidth weights of key clients and of ordinary clients for dynamic rate limiting respectively.

Command	**smart-rate-control config user weight key** *key-user-weight* **normal** *normal-user-weight*
Parameter Description	*key-user-weight*: Indicates the weight of key clients. The value ranges from 1 to 100 and the default value is 100. *normal-user-weight*: Indicates the weight of ordinary clients. The value ranges from 1 to 100 and the default value is 50.
Defaults	The default weights of key clients and of ordinary clients are 100 and 50 respectively.
Command Mode	AP configuration mode and all-AP configuration mode on the AC and global configuration mode on the AP
Usage Guide	The weight of key clients cannot be smaller than that of ordinary clients. The actual data rate is calculated based on the negotiated rate of the client. When the negotiated rate is relatively low, the actual data rate of key clients may be lower than that of ordinary clients though the weight of the key clients is greater.

- Configure application guarantee for dynamic rate limiting.

Command	**smart-rate-control config application guarantee enable**
Parameter Description	N/A
Defaults	The application guarantee for dynamic rate limiting is disabled by default.
Command Mode	AP configuration mode and all-AP configuration mode on the AC and global configuration mode on the AP
Usage Guide	When you enable application guarantee for dynamic rate limiting, add the critical applications into the critical application group by running the **identify-application key** command. It is optional to add the suppression applications into the suppression application group by running the **identify-application inhibitive** command.

- Configure the guaranteed bandwidth weights of the critical application group, of the ordinary application group, and of the suppression application group respectively.

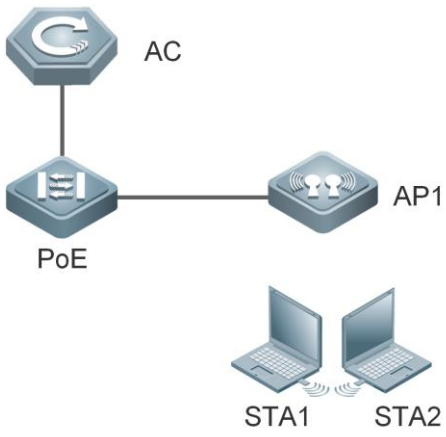
Command	**smart-rate-control config application weight key** *key-group-weight* **normal** *normal-group-weight* **inhibitive** *inhibitive-group-weight*
Parameter Description	*key-group-weight*: Indicates the weight of the critical application group. The value ranges from 1 to 100 and the default value is 100. *normal-group-weight*: Indicates the weight of the ordinary application group. The value ranges from 1 to 100 and the default value is 50. *inhibitive-group-weight*: Indicates the weight of the suppression application group. The value ranges from 1 to 100 and the default value is 50.
Defaults	The default weights of the critical application group, of the ordinary application group, and of the suppression application group are 100, 50, and 50 respectively.
Command Mode	AP configuration mode and all-AP configuration mode on the AC and global configuration mode on the AP
Usage Guide	N/A

Verification

- Run the **show running-config** command to check whether dynamic rate limiting is enabled and check its parameters. By default, this information is not displayed.

Configuration Example

Configuring Dynamic Rate Limiting

Scenario Figure 1-7	

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 to 80%. 6. Set the STA association rate factor to 256. 7. Configure the guaranteed bandwidth as 100, which is equivalent to 800 kbps (100 x 8 kbps). 8. Set the minimum rate limiting to 20, which is equivalent to 160 kbps (20 x 8 kbps). 9. Set the wireless loss to **50%**. 10. Configure **STA 0a08.27c4.a8b2** as the key client for dynamic rate limiting. 11. Set the guaranteed bandwidth weights of the key clients and of the ordinary clients to **75** and **50** respectively. 12. Enable application guarantee for dynamic rate limiting. 13. Set the guaranteed bandwidth weights of the critical application group, of the ordinary application group, and of the suppression application group to **75**, **50**, and **25** respectively.

	`Hostname#configure terminal`
	`Hostname(config)#ap-config ap1`
	`Hostname(config-ap)#smart-rate-control enable`
	`Hostname(config-ap)#smart-rate-control config low-rate-sta 1024`
	`Hostname(config-ap)#smart-rate-control config rate-limit-step increase 20`
	`Hostname(config-ap)#smart-rate-control config sampling period 2000`
	`Hostname(config-ap)#smart-rate-control config threshold channel-using 80`
	`Hostname(config-ap)#smart-rate-control config threshold link-rate-divisor 256`
	`Hostname(config-ap)#smart-rate-control config threshold rate-guard 100`
	`Hostname(config-ap)#smart-rate-control config threshold rate-limit 20`
	`Hostname(config-ap)#smart-rate-control config wlan-loss 50`
	`Hostname(config-ap)# smart-rate-control config user mac 0a08.27c4.a8b2`
	`Hostname(config-ap)# smart-rate-control config user weight key 75 normal 50`
	`Hostname(config-ap)# smart-rate-control config application guarantee enable`
	`Hostname(config-ap)# smart-rate-control config application weight key 75 normal 50 inhibitive 25`

Verification	● Run the **show ap-config** ap1 command to check whether dynamic rate limiting is enabled.

	`Hostname# show ap-config ap1`
	`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 link-rate-divisor 256`

	smart-rate-control config threshold rate-guard 100 smart-rate-control config threshold rate-limit 20 smart-rate-control config wlan-loss 50 mart-rate-control config user mac 0a08.27c4.a8b2 smart-rate-control config user weight key 75 normal 50 smart-rate-control config application guarantee enable smart-rate-control config application weight key 75 normal 50 inhibitive 25

Common Errors

- N/A

1.4.6 Configuring Uplink Congestion Control

Configuration Effect

The uplink congestion control function can be configured to limit traffic by adjusting the TCP sliding window.

Notes

N/A

Configuration Steps

↘ Enabling Uplink Congestion Control

- Optional.
- On the AC, run the **congestion-control tcp enable** command to enable uplink congestion control in AP configuration mode.

Command	**congestion-control tcp enable**
Parameter Description	N/A
Defaults	Uplink congestion control is disabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

↘ Configuring Uplink Congestion Control Parameters

- Configure the channel utilization threshold.

Command	**congestion-control tcp threshold cu** [**up** | **down**] *cu*
Parameter Description	**up**: Configures the uplink channel utilization. **down**: Configures the downlink channel utilization. Currently, downlink channel utilization control is not supported. The configuration cannot take effect. Supported configuration depends on the specifications of the released version. *cu*: Configures the channel utilization threshold. The value range is from 1 to 100, in percentage.
Defaults	The channel utilization threshold is 70%.

Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	When the channel utilization of the TCP flow reaches the threshold, it is considered that there is an uplink congestion.

- Configure the delay threshold.

Command	**congestion-control tcp threshold delay** *num*
Parameter Description	*num*: Indicates the delay threshold, in μs. The value range is from 1000 to 100000.
Defaults	The delay threshold is 10000 μs.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

- Configure the threshold of uplink traffic volume.

Command	**congestion-control tcp threshold upstream** *num*
Parameter Description	*num:* Indicates the threshold of uplink traffic volume, in pps. The value range is from 100 to 100000.
Defaults	The threshold of uplink traffic volume is 1000 pps.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

- Configure the window optimization duration.

Command	**congestion-control tcp window-optimize hold-time** time
Parameter Description	*time*: Configures the window optimization duration, in seconds. The value range is from 1 to 100.
Defaults	The window optimization duration is 5s.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

- Configure the DSCP threshold.

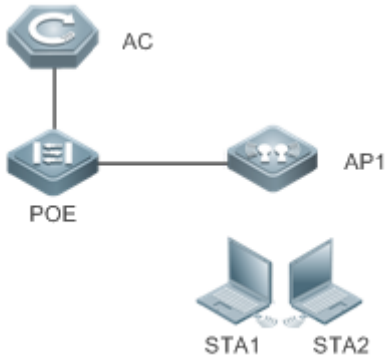
Command	**congestion-control tcp dscp** *num*
Parameter Description	*num*: Configures the DSCP threshold. The value range is from 1 to 63.
Defaults	The DSCP threshold is 10.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	N/A

Verification

- Run **show running-config** command to check whether uplink congestion control is enabled and whether its parameters are configured.

Configuration Examples

Configuring Uplink Congestion Control

Scenario **Figure 1-71**	
Configuration Steps	1. Enable uplink congestion control. 2. Set the window optimization duration to 8s 3. Set the DSCP threshold to 50. 4. Set the uplink CU threshold to 10%. 5. Set the delay threshold to 20 μs. 6. Set the threshold of uplink traffic volume to 30 pps.

	`Hostname(config)#congestion-control tcp enable`
	`Hostname(config)#congestion-control tcp window-optimize hold-time 8`
	`Hostname(config)#congestion-control tcp dscp 50`
	`Hostname(config)#congestion-control tcp threshold cu up 10`
	`Hostname(config)#congestion-control tcp threshold delay 20`
	`Hostname(config)#congestion-control tcp threshold upstream 30`

Verification	Run the **show running-config** command to display the uplink congestion control configurations on the AP.

	`Hostname(config)#show running-config`
	
	`Building configuration...`
	`Current configuration: 2871 bytes`
	
	`congestion-control tcp enable`
	`congestion-control tcp threshold cu up 10`
	`congestion-control tcp threshold delay 20`
	`congestion-control tcp threshold upstream 30`
	`congestion-control tcp dscp 50`

	`congestion-control tcp window-optimize hold-time 8`

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show dot11 ratelimit {**wlan** | **ap** | **user** }	Displays WQoS rate limiting information.

1 Configuring WMM

1.1 Overview

Wi-Fi Multimedia (WMM) is a wireless Quality of Service (QoS) protocol, which is a subset of the 802.11e protocol. WMM is utilized to prioritize high-priority packets, ensuring that voice and video applications receive preferential treatment on a wireless network.

This document consists of two parts:

- WMM service: The WMM service is used to differentiate capabilities of access channels with different priorities, ensuring that channel resources are allocated based on data flow priorities. You can adjust Enhanced Distributed Channel Access (EDCA) parameters for a client or an AP based on requirements, so the AC with a higher priority can start the backoff process earlier than other ACs and preferentially access a channel.
- QoS packet priority mapping: Wireless-to-wired QoS mapping and wired-to-wireless QoS mapping help to implement end-to-end QoS on 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
- RFC 5416: Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE802.11

1.2 Applications

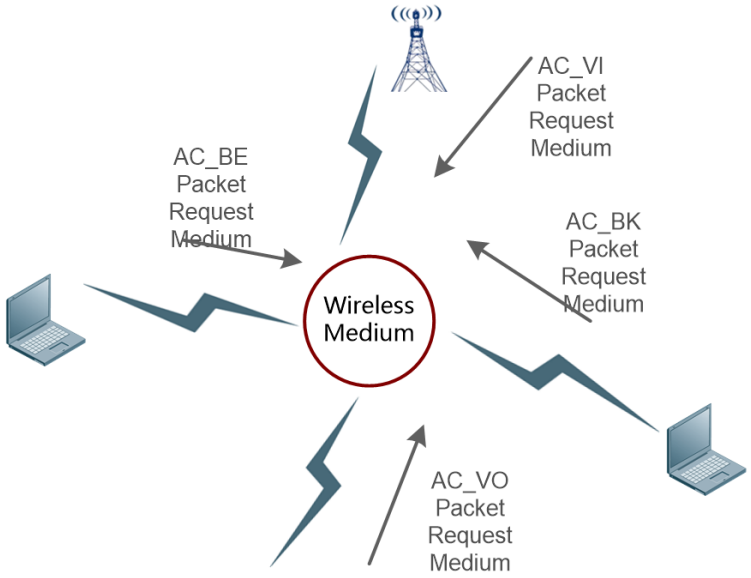
Application	Description
WMM Service	Competition process of channels with different priorities
Wireless-to-Wired Priority Mapping	Wireless-to-wired QoS packet priority mapping process
Wired-to-Wireless Priority Mapping	Wired-to-wireless QoS packet priority mapping process

1.2.1 WMM Service

Scenario

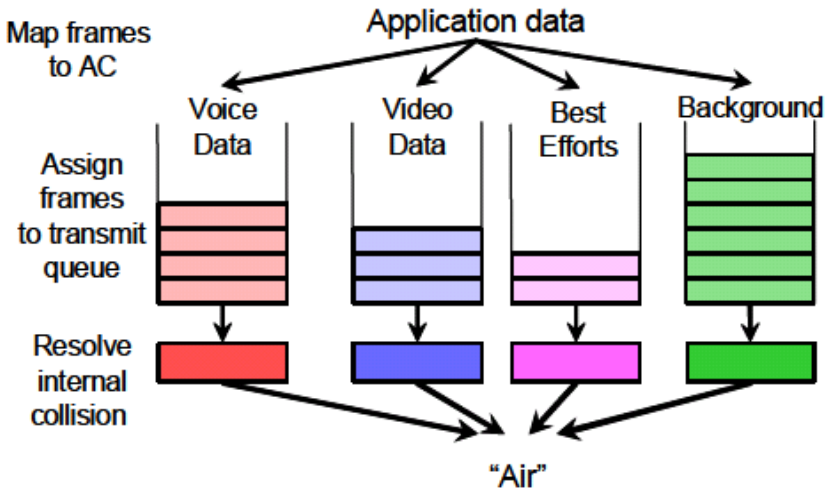
The medium for wireless communication is radio. In a specified frequency band, channels are shared during wireless network communication. In the same RF environment, uplink and downlink traffic of different sites conflicts. Therefore, it is essential to address the issue of how communication participants compete for shared channels to ensure wireless QoS. As shown in Figure 1-1, there are packets of four different priorities in the same wireless network environment (packets in descending order of priority are as follows: AC_VO > AC_VI > AC_BE > AC_BK). When multiple supplicants request access to the medium to send packets and compete for channels, a competition and coordination mechanism is employed to determine which supplicant's packet can access the medium. The higher the packet's priority is, the more likely it is to gain access to the channel.

Figure 1-1 Channel Competition



On a wireless network, the impact of packet loss and signal interference on packet integrity during transmission is significant due to the unique nature of the medium. To ensure packet delivery, retransmission of various wireless transmission parameters becomes necessary. However, it is impractical to apply optimal parameters to all packets. To cater to services with stringent reliability and timeliness requirements, packet classification becomes essential. In essence, different network services are offered based on diverse requirements, prioritizing the processing of critical data packets with high timeliness needs while assigning lower processing priority to common packets without such demands. For a network to support a variety of services, it must not only deliver a single service with top-quality QoS but also accommodate different services with varying QoS levels. As a result, the QoS of a wireless Access Point (AP) hinges on the ability to classify and identify packets to distinguish between different data flows and provide services of distinct quality.

Figure 1-2 Wireless QoS Multi-priority Queue



Deployment

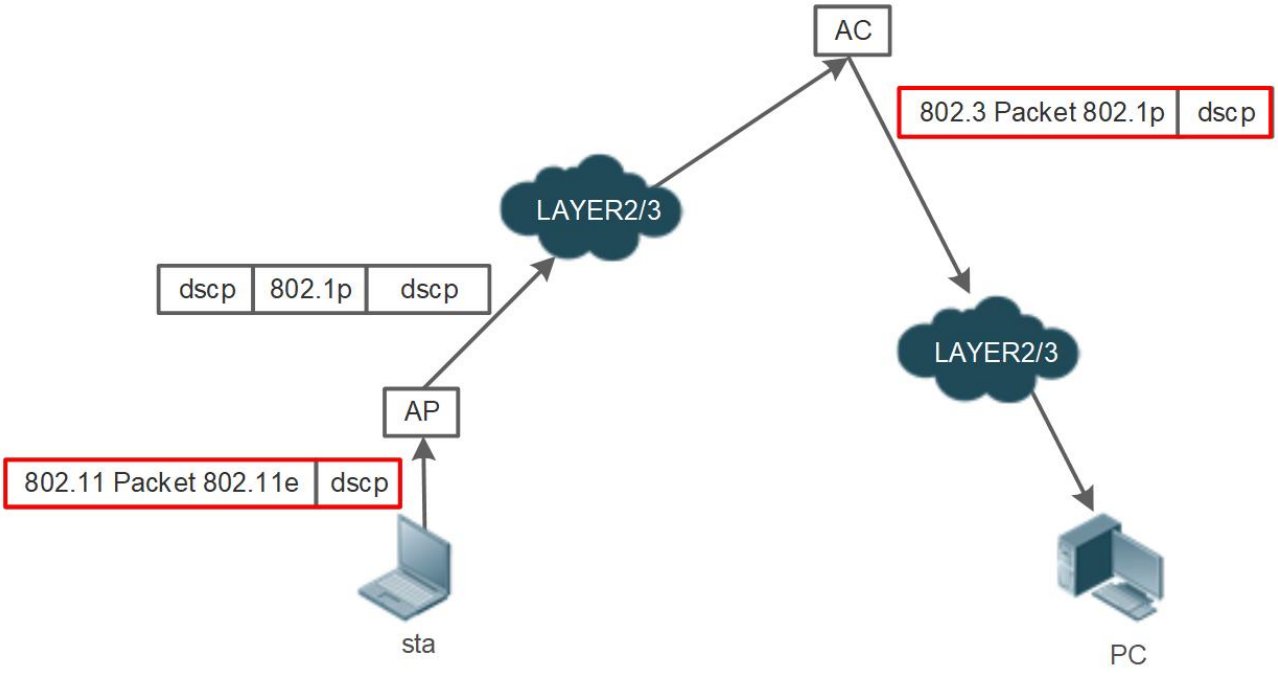
Key configuration on the device:

- Enable WMM.
- Set EDCA competition parameters. Typically, default values are used.

1.2.2 Wireless-to-Wired Priority Mapping

Scenario

Figure 1-3 Wireless-to-Wired Packet Priority Mapping



STA-to-PC priority mapping process:

- A STA sends an 802.11 packet carrying 802.11e and DSCP information to the AP.
- The AP sets the internal priority of the packet based on the trust mode of the wireless interface (configured on the ESS of the AC based on the BSSID). If the trusted packet carries an 802.11e priority, the AP converts the packet with the 802.11e priority into a wired packet with the 802.1p or DSCP priority and the CAPWAP packet with the 802.1p or DSCP priority. If the DSCP priority is trusted, the preceding configuration is performed based on the DSCP priority of the incoming wireless packet. By default, the DSCP priority is trusted, and the wireless end conforms to 802.11e.
- When passing Layer 2/3 network, the CAPWAP packet is processed according to the wired QoS method.
- After receiving the CAPWAP packet, the AC decapsulates the packet and then forwards the decapsulated wired packet to the Layer 2/3 network.
- When passing Layer 2/3 network, the wired packet is processed according to the wired QoS method.

Deployment

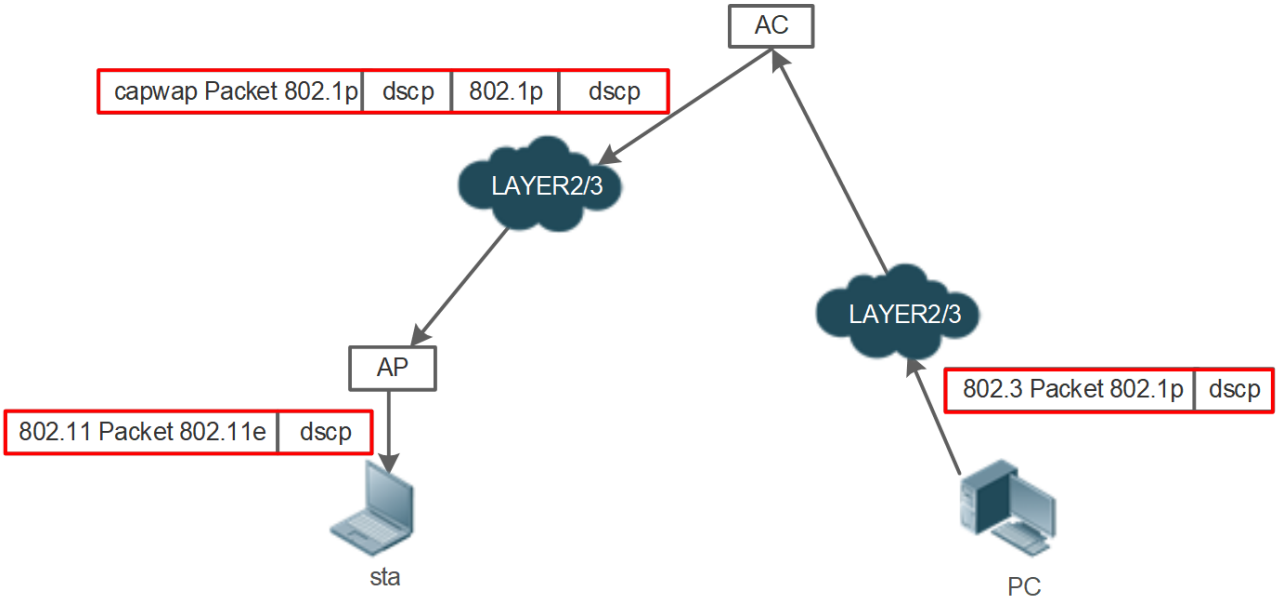
Key configuration on the device:

- Enable WMM.
- Set the wireless-to-wired priority mapping table. Typically, default values are used.

1.2.3 Wired-to-Wireless Priority Mapping

Scenario

Figure 1-4 Wired-to-Wireless Packet Priority Mapping



PC-to-STA QoS mapping process:

- The AC receives an 802.3Mac packet from the PC.
- Set the internal COS priority of the packet based on the trust mode of the physical interface. If the trusted packet has the 802.1p priority and carries a tag, set the internal CoS value of the packet based on the 802.1p priority. Otherwise, set the default priority of the packet based on the default priority of the interface. If the DSCP priority is trusted, the preceding configuration is performed based on the DSCP priority of the incoming wireless packet. By default, the DSCP priority is trusted, and the wireless end conforms to 802.11e.
- The AC encapsulates the 802.3 packet into a CAPWAP packet.
- After receiving the CAPWAP packet, the AP decapsulates the packet and performs QoS priority mapping for the wired-to-wireless packet based on the trusted priority. If the DSCP priority is trusted, the AP configures the 802.11e or DSCP priority of the wireless packet based on the DSCP priority of the 802.3 packet. If the 802.1p priority is trusted, the AP performs the configuration based on the COS value of the 802.3 packet.
- Based on the 802.11e priority of the wireless packet, the AP participates in the competition for wireless channels and sends the wireless packet to the STA.

Deployment

Key configuration on the device:

- Enable WMM.
- Set the wired-to-wireless priority mapping table. Typically, default values are used.

1.3 Features

Basic Concepts

Access Class

According to the WMM standard, access data flows are categorized into four priorities, each representing a class. AC_BK (background), AC_BE (best-effort), AC_VI (video data), and AC_VO (voice data) are in descending order of priority.

EDCA Competitive Mechanism

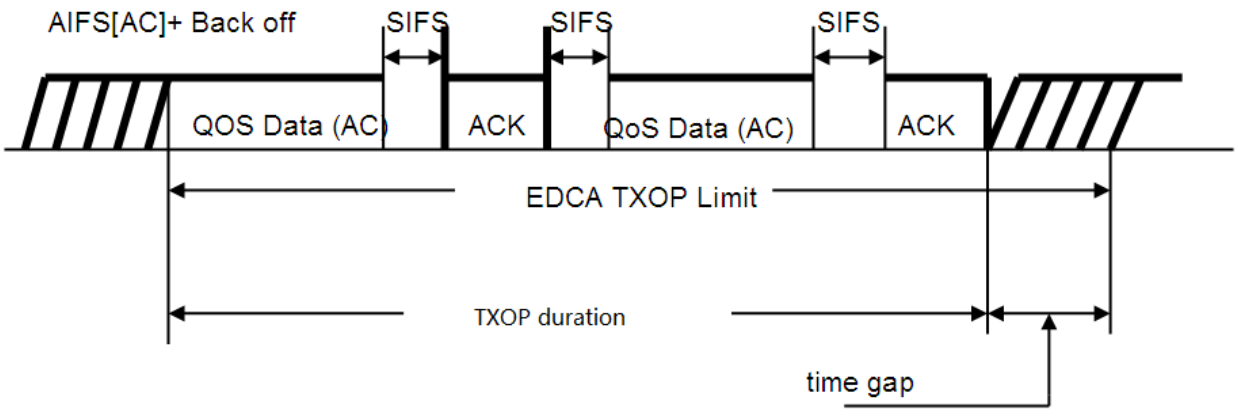
The EDCA competitive mechanism is the core of IEEE 802.11e. It differentiates access capabilities of AC channels with different priorities, ensuring that air interface resources are allocated based on data flow priorities. EDCA retains distributed channel competition between an AP and a STA, and introduces internal competition of four internal priority classes of the QoS AP (QAP) or QoS STA (QSTA). In this way, EDCA introduces the channel competition mechanism that differentiates 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 the Arbitration Inter Frame Spacing Number (AIFSN), Transmission Opportunity (TXOP) limit, CWmin, and CWmax.

EDCA Parameters

The EDCA competition parameters are listed as follows:

- AIFSN: In the 802.11 protocol, the Distributed Inter-frame Spacing (DIFS) has 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 higher probability of preempting channels.
- Exponent form of CWmin (ECWmin) and Exponent form of CWmax (ECWmax) determine the average backoff time. Larger ECWmin and ECWmax mean a longer backoff time.
- Transmission Opportunity (TXOP): It refers to the 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 fragmented.

Figure 1-5 TXOP Successive Frame Transmission



ACK Policy

Two ACK policies are available:

- 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 device not to return an ACK packet for the flow of a certain priority, saving the channel resource. During wireless packet interaction, an ACK packet can be not used. The No ACK policy helps to improve the transmission efficiency. However, it may cause packet loss.

According to the IEEE 802.11 standard, no ACK is returned for multicast or broadcast frames.

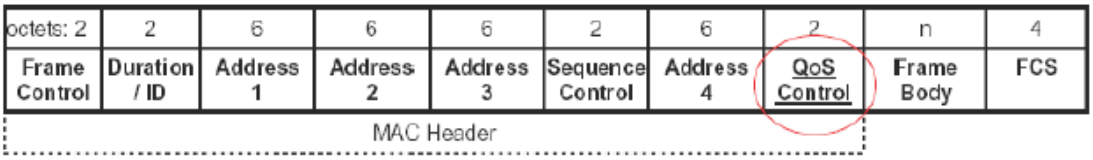
AC Queue Depth

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.

802.11e Priority

802.11e extends the MAC header of 802.11, with the QoS Control field added, as shown in Figure 1-6.

Figure 1-6 802.11e MAC Header



The QoS Control field has 2 bytes. Among them, the first three bits are the TID field, indicating the data form identification code. TID values 0 to 7 represent QoS priorities, indicating user priorities (UP); TID values 8-15 are used for parameter-based QoS, indicating the data flow ID (TSID).

WMM maps the user priority to the corresponding access category (AC). The following table lists the mapping between the 802.11e priority and AC.

Priority	User Priority	Access Category
Lowest ↓ **Highest**	1	Background
	2	Background
	0	Best-effort
	3	Best-effort
	4	Video
	5	Video
	6	Voice
	7	Voice

Priority Mapping Table

After a packet enters a device, the device determines the packet trust mode of the interface, that is, determines which priority in the received packet is valid. In addition, the device determines the work mode (Fat AP or Fit AP) of the AP. Then the device selects a mapping table based on the preset information to perform priority mapping.

Overview

Feature	Description

Feature	Description
WMM Service	Configures the 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 the WMM service, including EDCA competition parameters, AC queue depth, and ACK policy.

Working Principle

WMM provides network services of different quality based on requirements. That is, it provides high-quality services for key data packets having high timeliness requirement and processes them preferentially, and assigns a low processing priority to common packets not having high timeliness requirement. According to the WMM standard, access data flows have four priorities, each representing a class. EDCA differentiates access capabilities of AC channels with different priorities, ensuring that air interface resources are allocated based on data flow priorities.

Enabling WMM

When the WMM service is enabled, the four-level priority queue is used for receiving and mapping. When the WMM service is disabled, the default priority queue is used for receiving and mapping.

EDCA Competitive Mechanism, AC Queue Depth, and NO ACK Policy

- EDCA competitive mechanism

EDCA parameters differentiate channel access capabilities of different priorities. Each AC has its own EDCA channel competition parameters. You can adjust EDCA parameters on a client or an AP based on requirements, so that the AC with a higher priority can start the backoff process earlier than other ACs and preferentially access the channel. Channel competition should be completed automatically by the hardware. The hardware will participate in channel competition after parameters such as the CWmin, CWmax, AIFSN, TXOP of each hardware queue are configured in the software.

You can choose to configure EDCA parameters on a client or an AP based on application requirements. The EDCA client mainly affects WMM competition parameters of a STA, and the EDCA radio mainly affects WMM competition parameters of an AP.

The QSTA configuration is managed and pushed by the QAP in a centralized manner. Channel competition parameters of the QAP and QSTA are independent. In most situations, the channel competition parameters of QAP can be slightly increased to ensure the competent channel control capability for the QAP. The QAP will notify EDCA parameter settings of the QAP through the EDCA Parameter Set IE of the beacon or Probe Response frame, and push the negotiated EDCA configuration to the QSTA through EDCA Parameter Set IE of the (Re)Association Response frame.

- 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.

- NO ACK policy

The NO ACK policy should be supported by both the recipient and sender. When the NO ACK policy is not supported for a queue, the NO ACK policy should be set in the DMA descriptor of each frame sent.

The NO ACK policy is used as an alternative for receiving confirmation (during wireless packet exchange) by using ACK packets in the environment with high communication quality and little interference. It helps to effectively improve the transmission efficiency. However, if the ACK packet for confirmation is not used and the communication quality is poor, the sender will not retransmit the packets even if the recipient has not received the packets, resulting in a higher 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 priority mappings. Then a mapping table is selected based on the preset information to perform priority mapping, implementing end-to-end QoS for the entire network.

Packet Priority Mapping

On an IP network, IPv4 packets can carry the 802.1p priority, ToS priority, and Differentiated Services Codepoint (DSCP) priority.

For the preceding QoS priority types of wired packets, the device only needs to support 802.1p and DSCP priorities because the leftmost six bits in the ToS field correspond to the DSCP field. In addition to the preceding three priority types, the 802.11e priority is also available for wireless packets.

The device determines the packet trust mode or tag policy of an interface, that is, determines which priority in the received packet is valid. In addition, the device determines the work mode (centralized or local forwarding) of an AP. Then the device selects a mapping table based on the preset information to perform priority mapping.

1.4 Configuration

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-auto enable	Configures dynamic EDCA parameter adjustment.
	wmm edca-client	Configures EDCA parameters for the client.
	wmm edca-radio	Configures EDCA parameters for the AP.
Configuring 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 WLAN.
	(Optional) It is used to configure the 802.11p QoS mapping policy mechanism (mapping command for interworking versions).	

Configuration	Description and Command	
	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 the 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 the DSCP priority.

1.4.1 Configuring the WMM Service

Configuration Effect

- Configure EDCA competition parameters for the client.
- Configure 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.
- After dynamic EDCA parameter adjustment is enabled, the AP will dynamically adjust EDCA parameters. Custom configuration of EDCA parameters is not allowed.

Configuration Steps

↘ Enabling the WMM Service

- Mandatory.
- Run the **wmm enable radio** *radio-id* command in AP configuration mode to enable WMM for the Fit AP.
- When the WMM service is enabled, the four-level priority queue is used for receiving and mapping. When the WMM service is disabled, the default priority queue is used for receiving and mapping.

Command	**wmm enable radio** *radio-id*
Parameter Description	**radio** *radio-id*: Indicates that radio of the enabled/disabled WMM service is selected. The value range is from 1 to 48. This command is supported only on ACs.
Defaults	WMM is enabled by default
Command Mode	AP configuration mode for Fit APs

Usage Guide	When the WMM service is disabled, the default priority queue is used for receiving and mapping.

Configuring Dynamic EDCA Parameter Adjustment

- Optional.
- Run the **wmm edca-auto enable radio** *radio-id* command to enable dynamic EDCA parameter adjustment in AP configuration mode.
- After dynamic EDCA parameter adjustment is enabled, the AP can dynamically adjust EDCA parameters based on the number of active users. If dynamic EDCA parameter adjustment is disabled, the AP uses the static EDCA parameters.

Command	**wmm edca-auto enable radio** *radio-id*
Parameter Description	**radio** *radio-id*: Specifies the radio on which dynamic EDCA parameter adjustment is configured. The value range is from 1 to 96. This parameter is supported only on the AC.
Defaults	Dynamic EDCA parameter adjustment is disabled.
Command Mode	AP configuration mode or all-AP configuration mode
Usage Guide	1. Dynamic EDCA parameter adjustment takes effect only when the WMM service is enabled. 2. If static EDCA parameters are configured and dynamic EDCA parameter adjustment is enabled, the dynamic EDCA policy is used preferentially. 3. If dynamic EDCA parameter adjustment is disabled, the AP uses the static EDCA parameters. 4. Dynamic EDCA parameter adjustment is enabled by default. When dynamic EDCA parameter adjustment is disabled, EDCA parameters cannot be manually configured. To customize EDCA parameters, disable dynamic EDCA parameter adjustment.

Configuring EDCA Parameters for the Client

- Optional.
- By default, EDCA parameters on the client 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 EDCA parameters on the client and AC queue depth are set, packets are processed based on the settings. Otherwise, packets are processed based on 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*] } **radio** *radio-id*
Parameter Description	**back-ground**: Sets the background queue. **best-effort**: Sets the BE queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **aifsn** *aifsn-value*: Sets the AIFSN. The value range is from 1 to 15. **cwmin** *cwmin-value*: Sets the CWmin value. The value range is from 0 to 1515. **cwmax** *cwmax-value*: Sets the CWmax value. The value range is from 0 to 1515.

	txop *txop-value*: Sets the TXOP value. The value range is from 0 to 255, in the unit of 32 μs. **length** *queue-length*: Sets the AC queue length. The value range is from 1 to 255. The default is 255. **radio** *radio-id*: Sets the ID of the radio of EDCA parameters on the client. The value range is from 1 to 96. This command is supported only on ACs. Whether this parameter is supported and the value range of this parameter depend on the product version. **no**: Restores default settings.
Command Mode	AP 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. When dynamic EDCA parameter adjustment is enabled, EDCA parameters cannot be configured for a client.

Configuring 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 non-default settings of EDCA parameters on the AP and NO ACK policy are used, packets are processed based on the settings. Otherwise, packets are processed based on the default settings.
- A smaller AIFS of a high-priority AC means earlier backoff. Smaller CWmin and CWmax values mean a shorter backoff period. TXOP limit allows an AC to transmit multi-frame packets on it continuously within the SIFS interval after the AC preempts 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** } **radio** *radio-id*
Parameter Description	**back-ground**: Sets the background queue. **best-effort**: Sets the BE queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **aifsn** *aifsn-value*: Sets the AIFSN. The value range is from 1 to 15. **cwmin** *cwmin-value*: Sets the CWmin value. The value range is from 0 to 1515. **cwmax** *cwmax-value*: Sets the CWmax value. The value range is from 0 to 1515. **txop** *txop-value*: Sets the txop value. The value range is from 0 to 255, in the unit of 32 μs. **noack**: Indicates that the **no ack** policy is enabled. The **no ack** policy is disabled by default. **radio** *radio-id*: Sets the ID of the radio of EDCA parameters on the client. The value range is from 1 to

	96. This command is supported only on ACs. Whether this parameter is supported and the value range of this parameter depend on the actual product version. **no**: Restores default settings.
Command Mode	AP 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. When dynamic EDCA parameter adjustment is enabled, EDCA parameters cannot be configured.

Verification

- You can run the **show run** or **show ap-config run** command on the Fit AP 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 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. ● Enable dynamic EDCA parameter adjustment on Radio 1 of AP002.

	`Hostname # configure terminal`
	`Hostname(config)# ap-config AP001`
	`Hostname(config-ap)# wmm enable radio 1`
	`Hostname(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1`
	`Hostname(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1`

Verification	Run the **show run** or **show ap-config run** command on the Fit AP to display 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

- If no radio exists, an error message is displayed.
- 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 QoS Packet Priority Mapping

Configuration Effect

- Configure packet priority mapping for the WLAN.
- Configure 802.11p mapping policy mechanism.
- Configure DSCP mapping policy mechanism.

Notes

- Packet priority mapping takes effect after the WMM service is enabled.

Configuration Steps

By default, the mapping from DSCP priorities to 802.11e priorities 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 priorities to DSCP priorities 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 WLAN must be configured on all APs.

After the priority mapping and the value corresponding to the mapping table are set, packets are processed based on the settings. Otherwise, packets are processed based on the default settings.

Command	**wlan-qos map-table** { **dot11e-inner-dscp** | **dot11e-tunnel-dscp** | **dscp-dot11e** } **import** *import-tag-value* **export** *export-tag-value*

Parameter Description	**dot11e-inner-dscp**: Sets priority mapping from 802.11e priorities to internal DSCP priorities. **dot11e-tunnel-dscp**: Sets priority mapping from 802.11e priorities to CAPWAP DSCP priorities. **dscp-dot11e**: Sets priority mapping from DSCP priorities to 802.11e priorities. **import** *import-tag-value*: Sets the priority of the incoming original packet. **export** *export-tag-value*: Sets the priority of the outgoing packet. **no**: Restores default settings.
Command Mode	WLAN configuration mode
Usage Guide	This command is for non-interworking versions. The parameter configuration takes effect only when the WMM service is enabled.

Enabling the 802.11p Mapping Policy Mechanism

- Optional.
- Unless otherwise specified, the DSCP mapping policy mechanism must 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 radio** *radio-id*
Parameter Description	**radio** *radio-id*: Indicates the ID of the radio of the enabled/disabled 802.11p mapping policy mechanism. The value range is from 1 to 96. This command is supported only on ACs. Whether this parameter is supported and the value range of this parameter depend on the product version. **no**: Restores default settings.
Command Mode	AP configuration mode for fit APs
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled.

Applying the 802.11p QoS Mapping Policy Mechanism for the AP

- Optional configuration.
- Unless otherwise specified, the 802.11p mapping policy mechanism application shall be performed on all APs.

Determine how to obtain the 802.1Q priority based on the 802.11p mapping policy mechanism applied by the AP.

Command	**wmm dot1p policy 1q** [*1q-policy-value*] **radio** *radio-id*
Parameter Description	**1q** *1q-policy-value*: Applies the 802.11p mapping policy mechanism. The value is 0 or 1. The default value is 0. **radio** *radio-id*: Applies the radio of the 802.11p mapping policy mechanism. The value range is from 1 to 96. This command is supported only on ACs. Whether this parameter is supported and the value range of this parameter depend on the product version. **no**: Restores default settings.
Command Mode	AP configuration mode for fit APs

Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. Applying the 802.11p QoS mapping policy mechanism takes effect only when the 802.11p mapping policy mechanism is enabled.

Configuring the 802.1p Priority

- Optional.
- Unless otherwise specified, the 802.1p priority must be configured on all APs.

Command	**wmm dot1p tag** [*tag-value*] { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*
Parameter Description	**tag** *tag-value*: Sets the 802.1p priority. The value range is from 0 to 7. The default values for **best-effort**, **back-ground**, **video**, and **voice** are 0, 2, 4, and 6 respectively. **back-ground**: Sets the background queue. **best-effort**: Sets the BE queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **radio** *radio-id*: Indicates the ID of the radio of the enabled/disabled 802.11p mapping policy mechanism. The value range is from 1 to 96. This command is supported only on ACs. Whether this parameter is supported and the value range of this parameter depend on the product version. **no**: Restores default settings.
Command Mode	AP configuration mode for fit APs
Usage Guide	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, the DSCP mapping policy mechanism must be disabled on all APs.

When the DSCP policy mechanism is enabled, the mapping table related to the DSCP priority is used. When the DSCP policy mechanism is disabled, the default mode is adopted for mapping.

Command	**wmm dscp enable radio** *radio-id*
Parameter Description	**radio** *radio-id*: Indicates that ID of the radio of the enabled/disabled DSCP QoS mapping policy mechanism. The value range is from 1 to 96. This command is supported only on ACs. Whether this parameter is supported and the value range of this parameter depend on the product version. **no**: Restores default settings.
Defaults	The DSCP mapping policy mechanism is disabled by default.
Command Mode	AP configuration mode
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled.

Applying the DSCP Mapping Policy Mechanism for the AP

- Optional.
- Unless otherwise specified, the DSCP mapping policy mechanism must be performed on all APs.

Determine how to obtain the DSCP priority based on the DSCP mapping policy mechanism applied by the AP

Command	**wmm dscp policy outer-tunnel** *outer-tunnel-value* **inner-tunnel** *inner-tunnel-value* **radio** *radio-id*
Parameter Description	**outer-tunnel** *outer-tunnel-value*: Applies the DSCP mapping policy mechanism for the outer tunnel header. The value is 0 or 1. The default value is 0. **Inner-tunnel** *inner-tunnel-value*: Applies the DSCP mapping policy mechanism for the inner tunnel header. The value is 0 or 1. The default value is 0. **radio** *radio-id*: Applies the radio of the DSCP mapping policy mechanism. The value range is from 1 to 96. This command is supported only on ACs. **no**: Restores the default settings.
Command Mode	AP configuration mode for Fit APs
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. Applying the DSCP mapping policy mechanism takes effect only when the DSCP mechanism is enabled.

Configuring the DSCP Priority

- Optional.
- Unless otherwise specified, the DSCP priority must be configured on all APs.

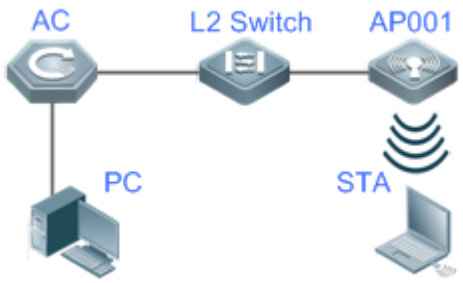
Command	**wmm dscp tag** *tag-value* { **back-ground** | **best-effort** | **video** | **voice** } **radio** *radio-id*
Parameter Description	**tag** *tag-value*: Sets the DSCP priority. The value range is from 0 to 63. The default values for **best-effort**, **back-ground**, **video**, and **voice** are 0, 16, 32, and 48 respectively. **back-ground**: Sets the background queue. **best-effort**: Sets the BE queue. **video**: Sets the video queue. **voice**: Sets the voice queue. **radio** *radio-id*: Indicates the ID of the radio of the enabled/disabled DSCP mapping policy mechanism. The value range is from 1 to 96. This command is supported only on ACs. Whether this parameter is supported and the value range of this parameter depend on the product version. **no**: Restores default settings.
Command Mode	AP configuration mode for fit APs
Usage Guide	The parameter configuration takes effect only when the WMM service is enabled. The DSCP priority takes effect only when the DSCP mechanism is enabled.

Verification

- You can run the **show run** or **show ap-config run** command on the Fit AP to display the mapping configuration. When the default configuration is adopted, no configuration is displayed in the command output.
- Obtain packets to check whether priority mapping is correct.

Configuration Example

Configuring QoS Packet Priority Mapping

Scenario	
	Connect the AC to the Layer 2 switch, and connect AP001 to the AC through the Layer 2 switch. Configure WLAN1 on AP001. Connect STA to AP001 in wireless mode, and connect the PC to the AC in wired mode.
Configuration Steps	Perform the following configuration on the AC: ● Enter the specified WLAN configuration mode. ● Configure packet priority mapping.

	`Hostname# configure terminal`
	`Hostname(config)# wlan-config 1`
	`Hostname(config-wlan)#wlan-qos map-table dot11e-tunnel-dscp import 7 export 50`
	`Hostname(config-wlan)# end`

Verification	Import AC_VO priority traffic from the STA to PC by using IxChariot, obtain packets on the air interface, and display the priority at the wireless end. Then obtain packets from the AC to the PC using a packet obtaining tool to display the priority at the wired end.

Common Errors

- The WMM service is disabled.

1.5 Monitoring

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug wlan-qos-vsp	Debugs WMM VSP.
debug wlan-qos-cli	Debugs WMM CLI.
debug wlan-qos-map	Debugs WMM mapping.

1 Configuring Web App

1.1 Overview

Web App processes and responds to Hypertext Transfer Protocol (HTTP) packets to ensure information exchange outside a device. It can process the mapping relationship for accurate projection.

Web App provides the following function:

- Basic service configuration: Web App can be enabled or disabled, the used port can be configured, and HTTP packets can be received and handled.

Protocols and Standards

- N/A

1.2 Applications

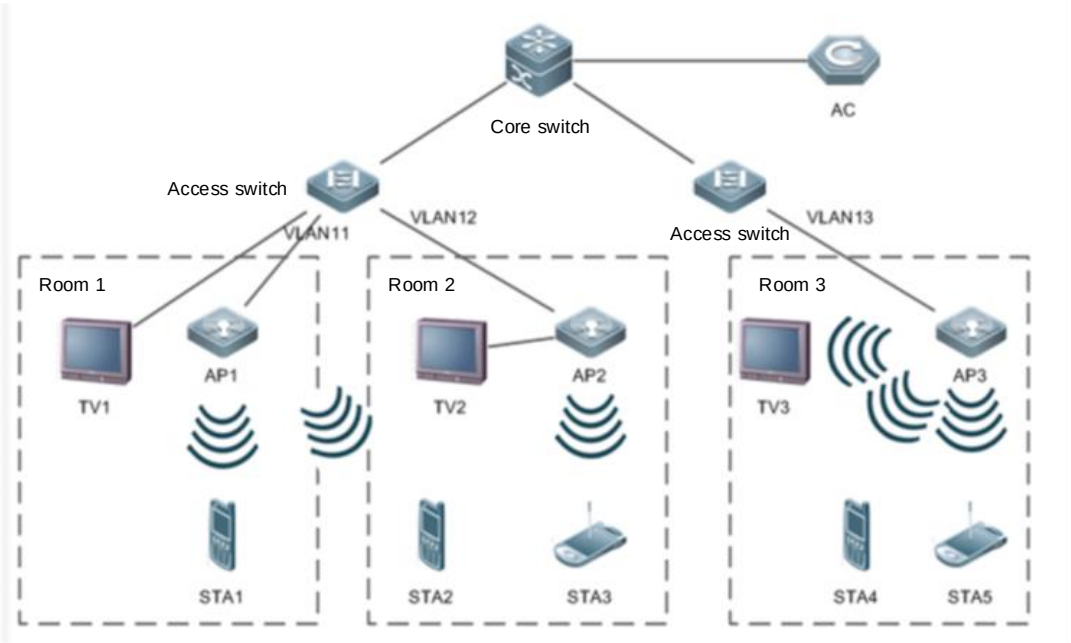
Application	Description
Accurate Projection	The deployed TV and station (STA) that accesses a wireless network are deployed on a Layer 2 or Layer 3 network. The STA scans the QR code or enters the website address to access the projection service page and sends a request packet to Web App to add the mapping relationship. Web App receives and processes the packet and sends the mapping relationship to the Bonjour or Digital Living Network Alliance (DLNA) gateway to add the STA-TV mapping relationship.

1.2.1 Accurate Projection

Scenario

The deployed TV and the STA that accesses a wireless network are on deployed on a Layer 2 or Layer network. The STA scans the QR code or enters the website address to access the projection service page and sends a request packet to Web App to add the mapping relationship. Web App receives and processes the packet and sends the mapping relationship to the Bonjour or DLNA gateway to add the STA-TV mapping relationship. As shown in Figure 1-1, the TV can access the network through a wired port on the switch, a wired port on an access point (AP), or the wireless network of an AP. The STA accesses the network through an AP. The STA and TV may be associated with an AP in the same room or APs in different rooms.

Figure 1-1 Network Topology for Projection



Deployment

- Enable the Web App function in global configuration mode.
- Enable the Bonjour gateway function in global configuration mode and enable Bonjour fixed projection.
- Enable the DLNA gateway function in global configuration mode and set the DLNA working mode to the accurate state.
- Scan the QR code of the TV with the mobile phone to complete mapping. Then you can enjoy the accurate projection service.

1.3 Features

Basic Concepts

Bonjour Gateway

A Bonjour gateway is used to manage clients and servers that support the Bonjour protocol so that the Bonjour protocol can be applied to large-scale networks.

DLNA Gateway

A DLNA gateway is used to manage clients and servers that support the DLNA specifications so that the DLNA projection service can be applied to wireless networks.

Overview

Feature	Description
Configuring Basic Services	Enables or disables the Web App function and configures the port used by the Web App function.

1.3.1 Configuring Basic Services

The basic service configuration includes enabling or disabling the Web App function and configuring the used port.

Working Principle

After the Web App function is enabled, the device can receive and process HTTP packets.

The device supports binding requests of accurate projection. A STA scans the QR code to access the Uniform Resource Locator (URL). The URL contains the IP address and port number of the access controller (AC) to be accessed, access path, and name and media access control (MAC) address of the TV to be bound. Web App will parse the URL, obtain field information to generate binding information on the device, and push the binding result to the STA.

URL format: http://<HOSTNAME>:<PORT>/touping?tvmac=<H.H.H>&tvname=<TV-NAME>

Example: http://172.30.103.252:8080/touping?tvmac=009e.c8cf.2255&tvname=abc

URL field description:

172.30.103.252: Indicates the IP address or domain name of the device. Ensure that the STA can access the address or domain name.

8080: Indicates the port number of the accessed device. The port number is configured by running the **webapp port** command.

009e.c8cf.2255: Indicates the MAC address of the bound TV.

abc: Indicates the name of the bound TV.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Services	⚠ (Mandatory) It is used to enable the Web App function.	
	webapp enable	Enables the Web App function.
	⚠ (Optional)	
	webapp port	Configures the port used by the Web App function.

1.4.1 Configuring Basic Services

Configuration Effect

- After the Web App function is enabled, the device can receive and process HTTP packets.
- Web App modifies the port number and uses the specific port number for packet sending and receiving.

Notes

- N/A

Configuration Steps

↘ **Enabling Web App**

- Mandatory.

Command	**webapp enable**
Parameter Description	N/A
Defaults	The Web App function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Port Used by the Web App

- Optional.

Command	**webapp port** *port*
Parameter Description	*port*: Indicates the port number. The value range is from 1024 to 65535.
Defaults	8080
Command Mode	Global configuration mode
Usage Guide	Plan application port numbers of the device and on a network to prevent service unavailability due to port number conflicts. Run the **show tcp port** and **show ip udp** commands on the device to display the port usage. The port can be configured only when the Web App service is disabled.

Verification

- Run the **show running-config** or **show webapp status** command to display the Web App configuration.

Configuration Example

Enabling Web App

Configuration Steps	• Enter the global configuration mode. • Enable the Web App function.

	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#webapp enable`

Verification	• Check whether the Web App function is enabled.
	`Hostname#show run | in webapp`
	`webapp enable`

Configuring the Port Used by the Web App

Configuration Steps	• Enter the global configuration mode. • Set the port used by Web App to 8192.

	`Hostname#configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#webapp port 8192`

Verification	Check whether the port is configured successfully.
	`Hostname#show run | in webapp`
	`webapp enable`
	`webapp port 8192`

Common Errors

N/A

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show webapp status	Displays the Web App status information.

Debugging

N/A

Configuring WLAN Distributed System

1. Configuring WDS
2. Configuring Leveled AC Configuration Synchronization

1 Configuring WDS

1.1 Overview

The Wireless Distribution System (WDS) connects multiple access points (APs) in wireless bridging or relay mode to interconnect distributed networks and extend wireless signals.

The WDS can work in either of the two following modes:

- Root bridge mode: Wired interfaces connect to wired networks, and wireless interfaces are used as wireless bridges to connect to those in non-root-bridge mode.
- Non-root-bridge mode: Wired interfaces connect to wired networks, and wireless interfaces are used as wireless bridges to connect to those in root bridge mode.

1.2 Applications

Application	Description
Static WDS Bridging	Two separate networks are interconnected through WDS bridging.
Mobile WDS Bridging	A mobile network is interconnected to a statically deployed network through WDS bridging.
Automatic Bridging of an AP Partner	Wireless signals are extended through WDS bridging between the AP partner and common APs.

1.2.1 Static WDS Bridging

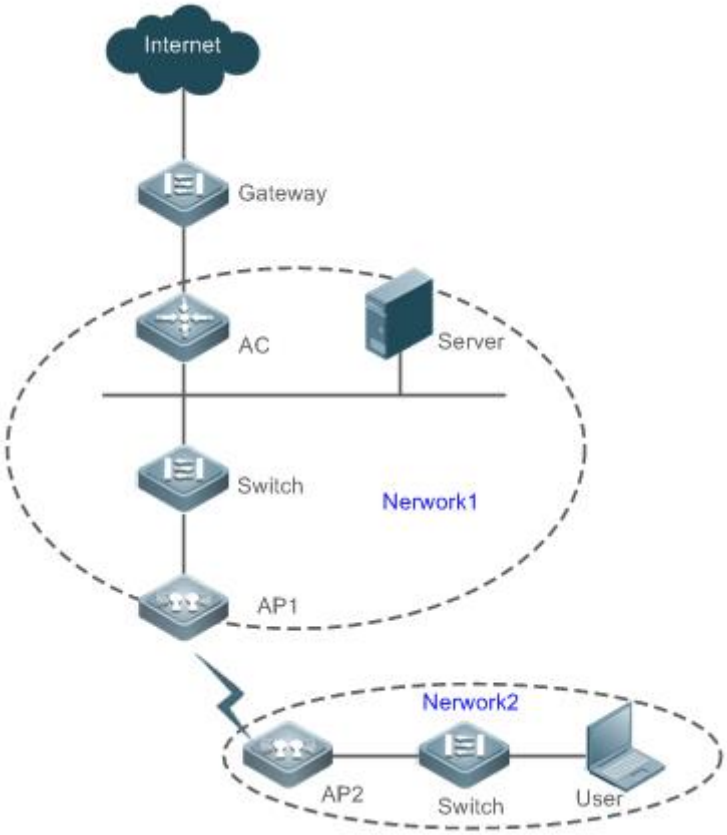
Scenario

Two separate networks are interconnected through bridging.

As shown in Figure 2-1, Network1 and Network2 are interconnected through WDS bridging by AP1 and AP2.

- WDS bridging enables users on Network2 to access the server on Network1.
- WDS bridging also enables users on Network2 to access the Internet.

Figure 2-1



Remarks	AP1 is a root bridge and AP2 is a non-root bridge.

Deployment

- WDS bridging is Layer 2 bridging.
- WDS bridging bridges multiple VLANs transparently.

1.2.2 Mobile WDS Bridging

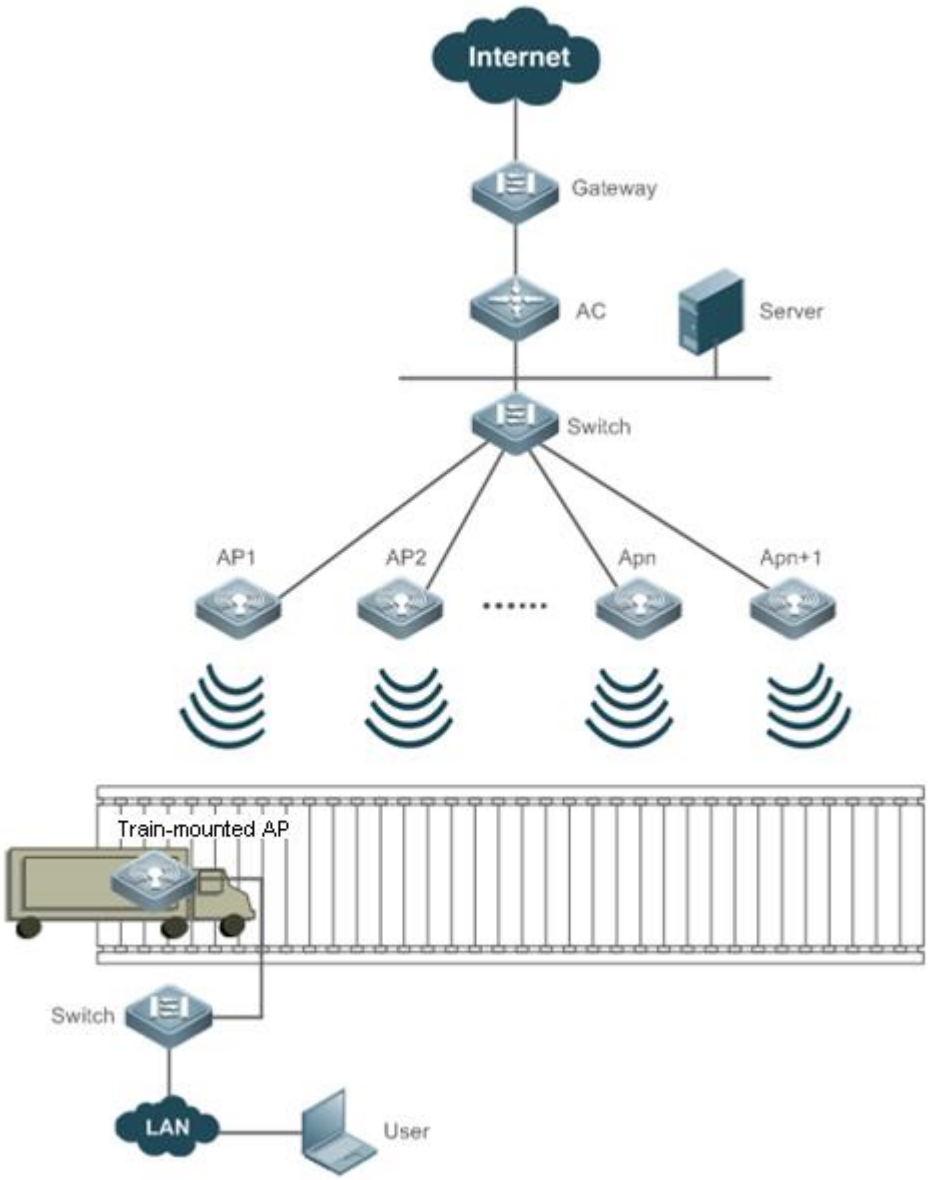
Scenario

A mobile network is interconnected to a static network through WDS bridging.

As shown in Figure 2-2, networks are interconnected through WDS bridging between the train-mounted AP and the APs outside the train (AP1 to AP*n*+1).

- When the train is advancing, users in the train can access the server through bridging.
- When the train is advancing, users in the train can access the Internet through bridging.

Figure 2-2



Remarks	AP1 to AP*n*+1 are root bridges. The train-mounted AP is a non-root bridge.

Deployment

- When the train is advancing, the non-root-bridge of WDS bridging can roam and switch to a root bridge.
- WDS bridging is Layer 2 bridging.
- WDS bridging can be used to transparently data from multiple VLANs.

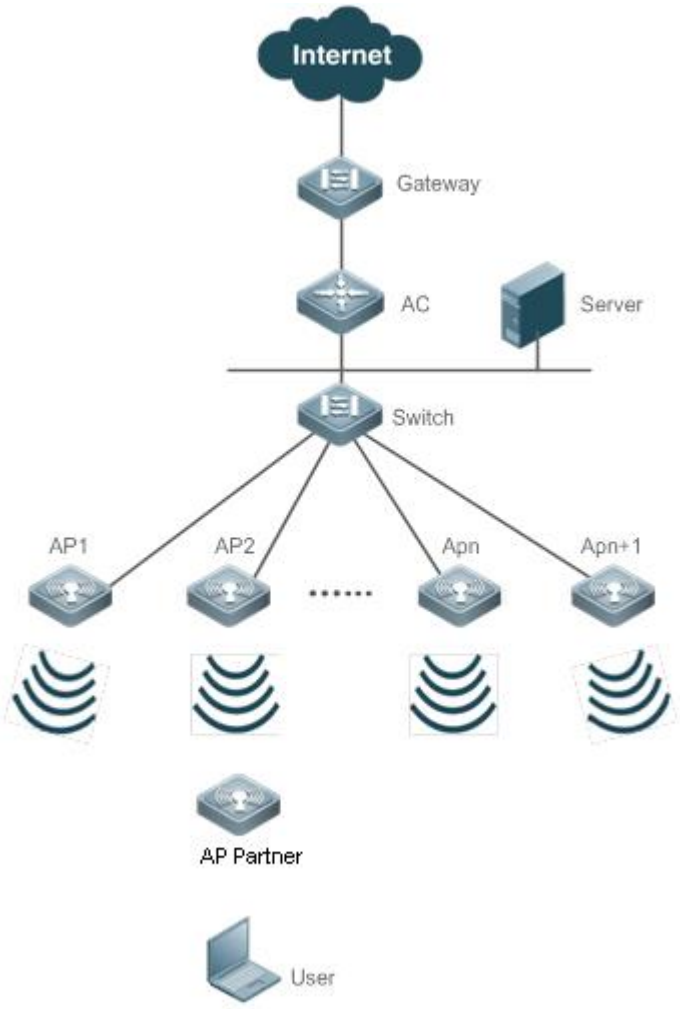
1.2.3 Automatic Bridging of an AP Partner

Scenario

An AP partner is used to extend wireless signals.

As shown in the Figure 2-3, wireless signals are extended through bridging between the AP partner and common APs.

Figure 2-3



Deployment

- The AP partner is used to achieve a large coverage of wireless signals.
- The AP partner uses zero-configuration.
- When automatic bridging is configured, the AP partner automatically connects to the network.

1.3 Features

Basic Concepts

Root Bridge

A root bridge is the root node in WDS bridging. It allows the access of a non-root bridge to establish WDS bridging.

Non-root Bridge

A non-root bridge is a non-root node in WDS bridging. It proactively accesses the root bridge to establish WDS bridging based on user configuration.

Features

Feature	Description
Establishing WDS Bridging	Establishes WDS bridging.
Address Format of MAC Frames in the WDS	Describes the address format of MAC frames exchanged between the root bridge and non-root bridges in WDS.

1.3.1 Establishing WDS Bridging

Establish WDS bridging.

Working Principle

Each AP is a Basic Service Set (BSS). Each has a BSSID (typically the MAC address of an AP). An AP regularly broadcasts Beacon frames that contain the SSID (name of a Wi-Fi network) and BSSID, and STAs listen to the Beacon frames by scanning. If the SSID of a Beacon frame is the same as the network name preset by a STA, the STA connects to the AP to access the network. If the STA listens to Beacon frames from multiple APs, the STA selects one of the APs for access. That is, the STA connects to and associates with the selected AP by identifying the BSSID of the AP.

In the WDS, the root bridge will specify a BSS used for access of non-root bridges to establish bridging. Common STAs are not allowed to access the BSS. When the BSS exists, the root bridge will accept the access request of a non-root bridge. During access, the root bridge will provide a mechanism to determine whether to allow a non-root bridge to connect to a network.

A non-root bridge searches for accessible root bridges based on the configured BSSIDs or SSIDs. A mechanism will be provided to determine whether a root bridge with a specified BSSID or SSID is accessible. The root bridge will be connected if accessible. In this way, WDS bridging is established.

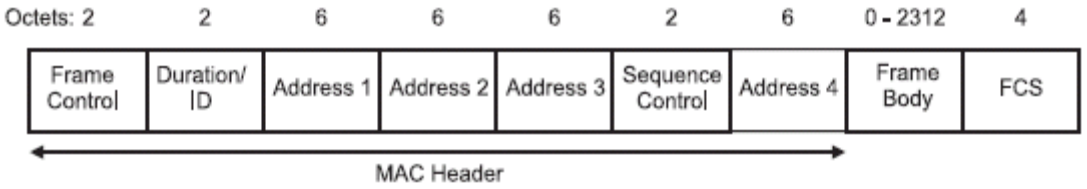
1.3.2 Address Format of MAC Frames in the WDS

This section describes the address format of MAC frames exchanged between a root bridge and a non-root bridge in WDS bridging.

Working Principle

In IEEE 802.11 standards, the format of MAC frames is defined for the wireless technology. The MAC header contains four address fields.

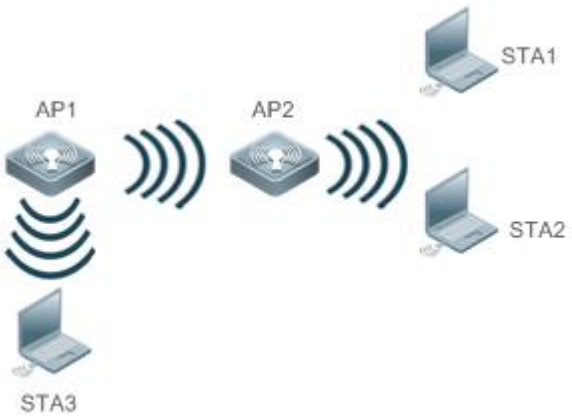
Figure 2-4



Based on transmission modes, 802.11 MAC frames can use the three-address or four-address format. The MAC frames in three-address format are transmitted between APs and STAs; while the MAC frames in four-address format are transmitted between APs.

As shown in Figure 2-5, when STA1 communicates with STA2, STA1 sends a MAC frame with three address fields of AP2, STA1 and STA2 to AP2 (See STA1->AP2 in the table). After receiving the MAC frame, AP2 forwards it to STA2, with three address fields changed into the MAC addresses of STA2, AP2 and STA1 (see AP2->STA2 in the table). When STA1 communicates with STA3, AP2 needs to forward the MAC frame received from STA1 to AP 1. The three-address format is changed to a four-address format, with the MAC addresses of AP2, AP1, STA3, and STA1 filled (see Figure 2-5). After receiving the frame, AP1 forwards it to STA3 and changes the four-address format back to a three-address format.

Figure 2-5



Transmission Mode	Address 1	Address 2	Address 3	Address 4
STA1 -> AP2	RA = AP2	TA = STA1	DA = STA2	N/A
AP2 -> STA2	RA = STA2	TA = AP2	SA = STA1	N/A
AP2 -> AP1	RA = AP1	TA = AP2	DA = STA3	SA = STA1

1.4 Configuration

Configuration	Description and Command	
Configuring WDS Basic Functions	(Mandatory) It is used to establish WDS bridging.	
	station-role root-bridge bridge-wlan	Configures a root bridge.

	station-role non-root-bridge	Configures a non-root bridge.
	parent	Specifies a root bridge for a non-root bridge.
	(Mandatory) If a non-root bridge works in Fit AP mode, it is used for WDS pre-configuration.	
	wds pre-config	Pre-configures a Fit non-root bridge.
	(Mandatory) If the non-root configuration is to be modified on the AC, it is used to submit or delete the ineffective WDS commands.	
	wds config	Submits or clears ineffective configuration of non-root bridges.
	(Optional) It is used to configure WDS parameters or enable the bridge coverage.	
	bridge roam-threshold	Configures roaming thresholds of a non-root bridge.
	bridge with-client	Configures bridge coverage.
	bridge vlan	Creates a bridge VLAN.
	bridge security	Configures bridge encryption on a non-root bridge.
	wds head-chansecurity enable	Sets whether to encrypt the head and tail channels on a non-root bridge.
	wds ctrl eth	Sets whether to control the wired interface on the non-root bridge.
	wds-mode enable	Enables WDS bridge mode.
	autowds	Enables automatic bridging of an AP partner.

1.4.1 Configuring WDS Basic Functions

Configuration Effect

- Configure WDS bridging.

Notes

- In WDS application environments, the Multiple Spanning Tree Protocol (MSTP) function must be enabled to prevent potential network loops.
- The Address Resolution Protocol (ARP) agent must be disabled.
- The WDS configuration commands can be used for establishing bridging only. They must be used with other commands to build a test environment, such as the commands for BBS creation or wireless interface configuration.
- In WDS, Fit APs need to support Control and Provisioning of Wireless Access Points (CAPWAP) through the Bridge-Group Virtual Interface (BVI) by default.

Configuration Steps

Configuring the WDS Mode

- Mandatory.
- Configure the WDS bridge mode on ACs for Fit APs.
- Run the **wds-mode enable** command to configure an AP to work in WDS bridge mode.

Command	**wds-mode {enable | disable}**
Parameter Description	**enable**: Enables the WDS bridge mode. **disable**: Disables the WDS bridge mode.
Defaults	disabled
Command Mode	AP configuration mode on the AC
Usage Guide	On the AC, run the **show ap-config wds-mode summary** command to check whether the corresponding AP has the WDS mode enabled. After this command is configured, the AP will automatically restart.

Configuring a Root Bridge

- Mandatory.
- Configure bridge coverage on ACs for Fit APs.
- Run the **station-role root-bridge bridge-wlan** *wlan-id* command to configure an AP working in WDS bridge mode.
- Specify a WLAN for the bridging BSS. If the WLAN has not been created, WDS bridging cannot work.

Command	**station-role root-bridge bridge-wlan** *wlan-id* [**radio** *radio-id*]
Parameter Description	**bridge-wlan** *wlan-id*: Specifies a WLAN for bridging. **radio** *radio-id*: Specifies the ID of a radio.
Defaults	The root AP mode means the regular AP mode but not the bridging mode.
Command Mode	AP configuration mode on the AC
Usage Guide	N/A

Configuring a Non-Root Bridge

- Mandatory.
- Configure bridge coverage on ACs for Fit APs.
- On a non-root bridge, you must specify a radio to work in non-root bridge mode.
- Run the **station-role non-root-bridge** command to configure an AP working in non-root bridge mode of WDS bridging.
- A non-root bridge starts to establish WDS bridging only after a destination root bridge is specified.

Command	**station-role non-root-bridge** [**radio** *radio-id*]
Parameter Description	**radio** *radio-id*: Specifies the ID of a radio.
Defaults	The root AP mode means the regular AP mode but not the bridging mode.

Command Mode	AP configuration mode on the AC
Usage Guide	The configurable WLAN quantity varies with the product model.

Specifying a Root Bridge for a Non-root Bridge

- Mandatory.
- Configure bridge coverage on ACs for Fit APs.
- Specify the BSSID or SSID to determine the root bridge.
- Specifying the BSSID of a root bridge, which is applicable to a static root bridge.
- Specifying the SSID of a root bridge. The non-root roaming function is enabled to select the root bridge with the best signals for access.
- Run the **parent** { **mac-address** *HHHH.HHHH.HHHH* | **ssid** *ssid* } [**channel** *channel* **chan-width**] command to specify the BSSID or SSID of a root bridge to be accessed by a non-root bridge.

Command	**parent** { **mac-address** *HHHH.HHHH.HHHH*	**ssid** *ssid* } [**radio** *radio-id*]
Parameter Description	**mac-address** *HHHH.HHHH.HHHH*: Specifies the BSSID of a root bridge for static bridging. **ssid** *ssid*: Specifies the SSID of a root bridge for roaming. **radio** *radio-id*: Specifies the ID of a radio.
Defaults	This function is not configured by default.
Command Mode	AP configuration mode
Usage Guide	Non-root bridges start searching root bridges after this command is executed. If WDS bridging is required, this command must be configured on the non-root bridges.

Configuring Roaming Thresholds of a Non-Root Bridge

- Optional.
- Configure bridge coverage on ACs for Fit APs.
- This command is configured to adjust roaming parameters.
- These thresholds are not required unless in special environments where roaming parameters need to be adjusted.
- Professionals are required to provide recommended values after measuring and analyzing the application environments. You are not advised to configure this command without the assistance of professionals; otherwise, the WDS roaming effect and even the use of WDS bridging will be affected.

Command	**bridge roam-threshold** *num1 num2 num3 num4* [*num5 num6 num7*] **radio** *radio-id*
Parameter Description	*num1*: Indicates the roaming start threshold.. The value range is from 0 to 90, and the default value is 40. *num2*: Indicates the scanning start threshold. The value range is from 0 to 30, and the default value is 15. *num3*: Indicates the roaming switch threshold. The value range is from 0 to 30, and the default value is 5. *num4*: Indicates the roaming switch time threshold. The value range is from 0 to 30, and the default value is 5. *num5*: Sets the roaming start upper threshold. The value range is from 0 to 90.

	num6: Sets the roaming switch upper threshold. The value range is from 1 to 30. *num7*: Sets the roaming pre-linking lower threshold. The value range is from 0 to 90. **radio** *radio-id*: Specifies the ID of a radio.
Defaults	This function is enabled by default.
Command Mode	AP configuration mode
Usage Guide	These thresholds are not required unless in special environments where roaming parameters need to be adjusted.

Configuring Bridge Encryption on a Non-Root Bridge

- Optional.
- Configure bridge coverage on ACs for Fit APs.
- This command is configured to adjust encryption parameters.
- This configuration is required only when bridging is required for accessing an encrypted network.
- The encryption parameters must be configured the same as those of the encrypted network to be accessed; otherwise, bridging may fail.

Command	**bridge security radio** *num* { **rsn ciphers aes akm psk key** { **ascii** | **hex** } *key* | **wpa** { **ciphers aes akm psk key** { **ascii** | **hex** } *key* | **mix pwe** { **both** | **hnp** } **passphrase ascii** *key* | **personal pwe** { **both** | **h2e** | **hnp** } **passphrase ascii** *key* } | **wpa3** { **mix pwe** { **both** | **hnp** } **passphrase ascii** *key* | **personal pwe** { **both** | **h2e** | **hnp** } **passphrase ascii** *key* } }
Parameter Description	**radio** *num*: Indicates the number of a configured RF interface. **wpa | rsn**: Configures WPA or RSN authentication. **aes**: Configures AES encryption. **psk**: Configures PSK authentication. **ascii**: Specifies the ASCII format. **hex**: Specifies the hexadecimal format. *key*: When the ASCII format is selected, the value is a string of 8 to 63 ASCII characters. When the hexadecimal format is selected, the value has 64 hexadecimal characters. **mix**: Configures mixed WPA2/WPA3-Personal authentication. **pwe**: Configures the WPA3 SAE encryption mode. **both**: Configures both HnP and H2E for WPA3 SAE authentication. **hnp**: Configures HnP for WPA3 SAE authentication. **passphrase**: Sets a key for authentication **personal**: Configures WPA3-Personal authentication. **h2e**: Configures H2E for WPA3 SAE authentication.
Defaults	No encryption parameter is configured by default.
Command Mode	AP configuration mode
Usage Guide	The encryption parameters must be configured the same as those of the encrypted network to be accessed;

	otherwise, bridging may fail.

Creating or Deleting a Bridge VLAN

- Optional.
- This is configured only on ACs in Fit AP mode.
- If you need to create a VLAN independently on an AP, you must perform this configuration on the AC.

Command	**bridge vlan** *vid*
Parameter Description	*vid*: Indicates the ID of the VLAN to be created
Defaults	This function is not configured by default.
Command Mode	AP configuration mode
Usage Guide	Use this command to create a WDS VLAN in coordination with other VLAN creation commands.

Configuring Bridge Coverage

- Optional.
- In root bridge mode: Configure bridge coverage on ACs for Fit APs. In non-root bridge mode, configure bridge coverage on APs for Fit APs through pre-configuration.
- This command is optional if the bridge coverage function is not required for the WDS. This command is mandatory if the bridge coverage function is required.
- You are not advised to enable the coverage function in bridging mode, because it may affect bridging performance, especially when there are low-speed STAs connecting to the network.

Command	**bridge with-client{ enable** | **disable** } [**radio** *radio-id*]
Parameter Description	**enable**: Enables bridge coverage. **disable**: Disables bridge coverage. **radio** *radio-id*: Specifies the ID of a radio.
Defaults	Bridge coverage is disabled by default.
Command Mode	AP configuration mode
Usage Guide	You are advised to disable bridge coverage.

Configuring Head and Tail Channels in Non-root Bridge Mode

- Optional.
- It can be configured in non-root bridge mode when you need to change AP channels based on head and tail status in metro scenarios.
- After this command is configured, the non-root bridge will switch to the corresponding channel when the status of the non-root bridge mode changes.

Command	**wds head-chan** *num1* **tail-chan** *num2* [**radio** *radio-id*]

Parameter Description	*num1*: Indicates the head channel. *num2*: Indicates the tail channel. **radio** *radio-id*: Indicates the radio ID specified on the AC.
Defaults	This function is disabled by default.
Command Mode	AP configuration mode on the AC
Usage Guide	Only the non-root bridge needs to be configured with this command. For the non-root Fit AP, this command needs to be configured on the AC and committed. Whether this configuration is supported depend on the product version.

Configuring Whether to Control the Wired Interface in Non-root Bridge Mode

- Optional.
- It can be configured in non-root bridge mode when you need to control traffic through wired interfaces in metro scenarios.
- After this command is configured, if the non-root bridge is not connected to the root bridge through bridging, the wired interface will be disconnected to control traffic.

Command	**wds ctrl eth**
Parameter Description	N/A
Defaults	The function is disabled by default.
Command Mode	AP configuration mode on the AC
Usage Guide	Only the non-root bridge needs to be configured with this command. For the non-root Fit AP, this command needs to be configured on the AC. Whether this configuration is supported depend on the product version.

Pre-configuring a Fit Non-root Bridge

- Optional.

Command	**wds pre-config delete radio** *radio-id*
Parameter Description	**delete**: Deletes the pre-configuration. **radio** *radio-id*: Specifies the ID of a radio.
Defaults	N/A
Command Mode	AP configuration mode
Usage Guide	To exit bridging mode, run the **wds pre-config delete** command to delete the non-root configuration created during pre-configuration.

Clearing or Submitting Ineffective WDS Configuration

- Optional.

- Use this command to submit inactive commands.
- Changes in the configuration of non-root bridges on the AC cannot take effect immediately. To issue the changes, you must run the **wds config commit** command.

Command	**wds config**[**clear | commit**] **radio** *radio-id*
Parameter Description	**clear**: Clears ineffective WDS configuration. **commit**: Submits ineffective WDS configuration. Then bridging will be re-established. **radio** *radio-id*: Specifies the ID of a radio.
Defaults	N/A
Command Mode	AP configuration mode on the AC
Usage Guide	Whether this configuration is supported depend on the product version. If the AP is configured to work in non-root bridge mode on the AC or synchronized from the AP to non-root bridge mode, the corresponding radio will enter the WDS edit mode. In this case, most of the WDS commands will not take effect immediately. You can view the configuration using the **show ap-config wds-config** command. After confirming that the configuration is correct, use this command to commit and make it take effect.

Configuring Automatic Bridging on the AC

- Optional.
- It can be configured in AP-all configuration mode, AP group configuration mode, and AP configuration mode in ascending order of priority.
- After this command is configured, the root AP will automatically create the WDS configuration upon receiving requests from an AP partner (non-root bridge).

Command	**autowds**
Parameter Description	N/A
Defaults	This function is not configured by default.
Command Mode	AP configuration mode or AP group configuration mode
Usage Guide	This function does not need to be configured in normal non-root bridge mode, and need to be configured only when an AP partner is to be connected. Whether this configuration is supported depend on the product version.

Verification

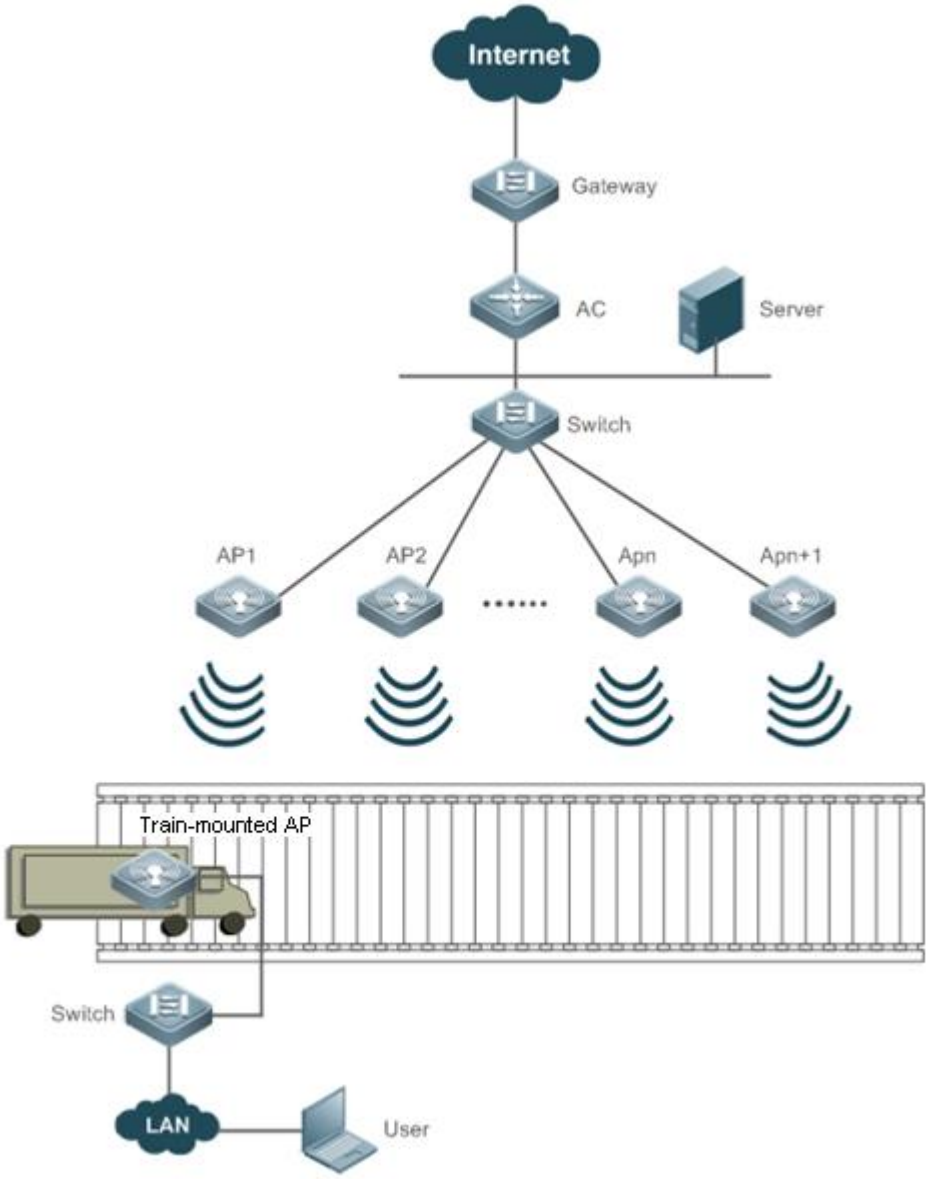
Run the **show running-config**, **show dot11 wds-bridge-info**, or **show wds-mode** command on the AP to display the WDS information.

Run the **show ap-config running**, **show ap-config wds-bridge-info**, **show ap-config wds-config**, or **show ap-config wds-mode summary** command on the AC to display WDS information.

Configuration Example

WDS Roaming Scenario in Fit AP Mode

In this scenario, APs are required to establish a CAPWAP link through the BVI by default.

Scenario **Figure 2-6**	
Configuration Steps	● Configure the WLAN, VLAN, and channels for AP1 to AP*n*+1. Unified channel information is required. ● The preceding configuration is the same as that in common AP application scenarios. ● Configure the root bridge and specify a WLAN used for bridging. ● Configure the non-root bridge. The pre-configuration is used for the non-root bridge. Assume that the bridge WLAN is **ruijie-root** and the channel is 149 with the bandwidth of 40 MB.
ROOT **(AP1 - APn+1)**	`Hostname#configure terminal` `Hostname(config)#ap-config ap1`

	Hostname(config-ap)# station-role root-bridge bridge-wlan 1 radio 2
NONROOT (In-vehicle AP)	Hostname#configure terminal Hostname(config)#interface dot 2/0 Hostname(config-if-Dot11radio 2/0)# station-role non-root-bridge Hostname(config-if-Dot11radio 2/0)# parent ssid ruijie-root Hostname(config-if-Dot11radio 1/0)# wds pre-config create Hostname(config-if-Dot11radio 1/0)# exit Hostname(config)#ap-mode fit
Verification	Run the following command to display WDS bridging information.
In-vehicle AP	Hostname#show dot11 wds-bridge-info 1/0 WDS-MODE: NONROOT-BRIDGE MAC:00d0.f822.3304 WBI 1/0 ROOT 32d0.f822.3303
On the AC	Display WDS bridging information on the interface. Hostname#show ap-config wds-bridge-info summary Ap Name Mac Address Radio Station Role ---------- -------------- ----- ---------------- Ap-001 00d0.f822.3301 2 ROOT-BRIDGE Ap-002 00d0.f822.3304 2 NON-ROOT-BRIDGE Hostname# show ap-config wds-bridge-info Ap-001 radio 2 WDS-MODE: ROOT-BRIDGE BRIDGE-WLAN: Status OK WlanID 1, SSID ruijie_root, BSSID 32d0.f822.3303 WBI 1/0 NONROOT 00d0.f822.3304

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show ap-config wds-mode summary	Displays whether WDS bridge is enabled on an AC.
show ap-config wds-mode summary	Displays the WDS bridge configuration on an AC.
show ap-config wds-bridge-info { **summary** |*ap-name* **radio** *radio-id* }	Displays WDS links on an AC.
show ap-config wds-config [*ap-name*]	Displays the WDS configuration on an AC.

1 Configuring Hierarchical AC Configuration Synchronization

1.1 Overview

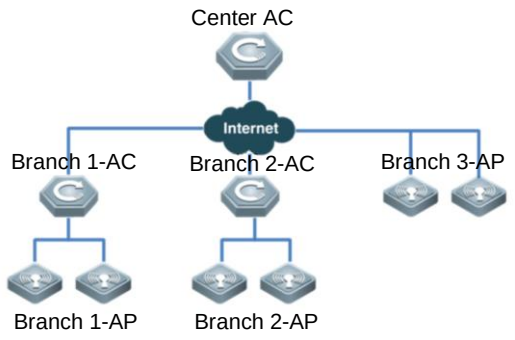
In the hierarchical access controller (AC) scenario, wireless-related configurations on the center AC and branch ACs must be the same. The manual configuration requires a large number of resources and are prone to errors. The hierarchical AC configuration synchronization function ensures configuration synchronization between the center AC and branch ACs in the hierarchical AC scenario. The configuration can be synchronized through the configuration template or configuration commands. In the initial deployment phase of a hierarchical network, the center AC can use the configuration template to deliver the configurations to branch ACs uniformly. If the hierarchical network is deployed, configuration command synchronization can be performed for synchronization of configuration commands of access point (AP) groups associated with branch ACs and in AP configuration mode between the center AC and branch ACs.

Protocols and Standards

N/A

1.2 Applications

1.2.1 Scenario



Deployment

- Configure the AC planned for the headquarters as the center AC in hierarchical AC networking.
- Configure the ACs planned for the branches as the branch ACs in hierarchical AC networking.
- On the center AC and branch ACs, enable the wireless local area network (WLAN) hot standby function.
- On the center AC, add hot standby peers for Branch 1-AC and Branch 2-AC.
- On Branch 1-AC and Branch 2-AC, add the hot standby peer for the center AC.
- On the center AC and branch ACs, add the AP groups to which Branch 1-AP and Branch 2-AP belong to the hot standby instances of the corresponding branches.

- On the center AC, create two different configuration templates named **template1** and **template2**.
- In **template1**, add configuration commands delivered to Branch 1-AC. On Branch 1-AC, request **template1**.
- In **template2**, add configuration commands delivered to Branch 2-AC. On Branch 2-AC, request **template2**.

1.3 Features

Overview

Feature	Description
Configuring Configuration Template Synchronization	Synchronizes configuration commands in configuration templates of the center AC to branch ACs.
Configuring Configuration Command Synchronization	Synchronizes configuration commands of the AP groups associated with branch ACs in AP configuration mode between the center AC and branch ACs.

1.3.1 Configuring Configuration Template Synchronization

In the hierarchical AC scenario, create multiple configuration templates on the center AC. Based on the configuration command maintenance method provided by the configuration templates, create the template content. Then batch synchronize commands in the configuration templates of the center AC to the branch ACs.

Working Principle

A center AC can be configured with multiple configuration templates, and each center AC can map to multiple branch ACs. The methods for determining the configuration templates to be synchronized to the branch ACs are as follows:

1. The center AC applies different configuration templates to different branch ACs.

   After the configuration templates are created, the center AC configures different configuration templates for different branch ACs to batch synchronize configurations to all branch ACs that trigger configuration synchronization.

2. Different branch ACs request different configuration templates from the center AC.

   The center AC creates configuration templates and associates different configuration templates with different branch ACs. Branch ACs request the center AC to deliver configuration templates based on network deployment requirements. In this case, branch ACs can plan the network configuration flexibly.

On a hierarchical network with configuration templates applied, configuration template synchronization can be triggered in two modes:

1. Automatic mode

   The center AC automatically synchronizes configuration templates to branch ACs in the following scenarios:

   (1) Configuration template synchronization is deployed for the first time.

   (2) A connection is established between a branch AC and the center AC for the first time.

2. Manual mode

   After the configuration templates are modified, you can manually synchronize the configuration templates from the center AC to the branch ACs.

When configuration template synchronization is enabled, the execution result varies depending on whether the center AC and branch ACs are associated with configuration templates.

1. If both the center AC and branch ACs are associated with configuration templates, only the configuration templates applied to the center AC are delivered to the branch ACs. Requests for configuration templates from the branch ACs do not take effect.
2. If only the center AC is associated with configuration templates, the center AC synchronizes the associated configuration templates to the branch ACs.
3. If only the branch ACs are associated with configuration templates, the center AC synchronizes the configuration templates requested by the branch ACs to the branch ACs.

1.3.2 Configuring Configuration Command Synchronization

During O&M of a hierarchical wireless network, configurations on the center AC or branch ACs may be changed. If the configuration on the peer AC cannot be changed automatically in a timely manner, it becomes cumbersome to update configuration commands in the configuration templates manually. Configuration command synchronization ensures automatic synchronization of configuration commands changed in the specified configuration mode between the center AC and branch ACs, keeping configuration consistency between them. The configuration command synchronization function can be used when the following configurations are changed:

1. Configurations of AP groups associated in hot standby instance configuration mode on the center AC and branch ACs
2. Configuration commands in AP configuration mode of APs associated with the preceding AP groups

Working Principle

In the hierarchical AC scenario, after configuration command synchronization is enabled and configurations are changed on the center AC or a branch AC, configurations of AP groups in hot standby instances and configurations of APs associated with the AP groups are collected and saved as a changed configuration file on the AC. The process of configuration command synchronization is as follows:

1. When an AC detects that the configuration in the hot standby instance is changed, it sends the changed configuration to the peer AC using a file.
2. After the peer AC receives the changed configuration, it determines whether a baseline file is available.
3. If no baseline file exists, the AC runs all commands in the configuration file to ensure configuration synchronization.
4. If a baseline file exists, it compares the received configuration with the baseline file to identify any differences. It then generates a configuration file to eliminate the differences, and runs the commands in the difference configuration file using a script to ensure configuration synchronization.

1.4 Configuration

Configuration	Description and Command
Configuring Configuration	(Optional) It is used to achieve configuration command synchronization.

Template Synchronization	**cfgmg template**	Configures the center AC to apply configuration templates to a branch AC.
	request cfgmg template	Configures a branch AC to request configuration templates from the center AC.
	sync cfgmg template	Enables the center AC to synchronize commands in the configuration template.
Configuring Configuration Command Synchronization	⚠ (Optional) It is used to maintain commands in a configuration template.	
	config command sync enable	Enables configuration command synchronization.

1.4.1 Configuring Configuration Template Synchronization

Configuration Effect

- With configuration synchronization deployed, configuration template synchronization is automatically triggered when a connection is established between the center AC and a branch AC for the first time. Compare the configuration on the branch AC with that in the configuration template to ensure that commands in the configuration template are synchronized to the branch AC.
- Manually trigger configuration template synchronization on the center AC. Compare the configuration on the branch AC with that in the configuration template to ensure that commands in the configuration template are synchronized to the branch AC.

Notes

- A configuration template needs to be created before being applied.
- When configuration template synchronization is deployed, the center AC synchronizes a configuration template to a branch AC only when a connection is established between the branch AC and center AC for the first time.

↘ Applying a Configuration Template

- Apply a configuration template on the center AC.

Command	**cfgmg template** *temp-name*
Parameter Description	*temp-name*: Indicates the name of the configuration template applied to the specified branch AC on the center AC. The configuration template needs to be created on the center AC in advance. The value is a string of 1 to 31 characters.
Defaults	N/A
Command Mode	Hot standby configuration mode
Usage Guide	1. This command can be configured only on the center AC in the hierarchical AC scenario. A maximum of eight configuration templates can be applied to each hot standby instance. 2. When multiple configuration templates are applied, the sequence for synchronizing commands in these templates depends on the sequence during which the templates are applied. 3. Applied configuration templates are delivered to a branch AC only when the branch AC connects to the center AC for the first time. Subsequent template configuration changes are not proactively synchronized to the branch AC. 4. Applied configuration templates are not forcibly bound to configuration templates of the CFGMG

	module. A non-existent configuration template can be applied. However, no configuration can be synchronized. When configuration templates of the CFGMG module are deleted, applied configuration templates are not deleted.

Verification

- Run the **show this** command in hot standby configuration mode to confirm the configurations.

Requesting a Configuration Template

- Request a configuration template on a branch AC.

Command	**request cfgmg template** *temp-name*
Parameter Description	*temp-name*: Indicates the name of the configuration template requested from the center AC on a branch AC. The configuration template needs to be created on the center AC in advance. The value is a string of 1 to 31 characters.
Defaults	N/A
Command Mode	Hot standby configuration mode
Usage Guide	1. In the hierarchical AC scenario, only branch ACs can request configuration templates from the center AC. 2. A requested configuration template has a lower priority than a configuration template applied to a branch AC by the center AC. If the center AC applies a configuration template to a branch AC, the applied configuration templates are preferred. Otherwise, the configuration template requested by the branch AC takes effect. 3. The requested configuration template is delivered to a branch AC only when the branch AC connects to the center AC for the first time. Subsequent template configuration changes are not proactively synchronized to the branch AC. 4. The requested configuration template is a configuration template of the CFGMG module on the center AC instead of a configuration template of the CFGMG module on the branch AC. 5. The requested configuration template is not forcibly bound to the configuration templates of the CFGMG module on the center AC. A non-existent configuration template can be requested. However, no configuration can be synchronized. When the configuration template of the CFGMG module on the center AC is deleted, the requested configuration template is not deleted.

Verification

- Run the **show this** command in hot standby configuration mode to confirm the configurations.
- When the center AC applies a configuration template, run the **show layerac template name** command to display the branch AC to which the configuration template is applied.
- When a branch AC requests for configuration templates, run the **show layerac template peer** command to display the configuration templates that the branch AC requests from the center AC.

Triggering Configuration Template Synchronization

- Manually trigger configuration template synchronization on the center AC.

Command	**sync cfgmg template**
Parameter Description	N/A
Defaults	N/A
Command Mode	Hot standby configuration mode
Usage Guide	1. When a template configuration is changed or when the template configuration needs to be re-sent in other scenarios, you can use this command to synchronize the template configuration to a branch AC. 2. Before triggering configuration template synchronization, check whether the center AC applies a configuration template in the hot standby instance of a branch AC or the branch AC requests a configuration template. 3. The command is supported only on center ACs.

Verification

- Run the **show running** command on a branch AC to confirm that commands in the template are synchronized.

Configuration Example

Configuring Configuration Template Synchronization

Configuration Steps	Use a typical hierarchical AC case as an example. Create templates **wlan-temp1** and **wlan-temp2** on the center AC and perform WLAN configuration in the templates. On the center AC, apply **wlan-temp1** to Branch AC-1 and **wlan-temp2** to Branch AC-2. Branch AC-1 and Branch AC-2 request configuration templates **wlan-temp1** and **wlan-temp2**. First, configuration template synchronization is automatically triggered. Then the template content is modified, and configuration synchronization is manually triggered. Display the configuration template synchronization results.
	- On the center AC, create configuration templates and import configuration commands to the configuration templates.

	(1) Create the content in the **temp-test1.text** file.
	`wlan-config 10 wlan-test1`
	`tunnel local`
	`wlan-config 20 wlan-test2`
	`tunnel local`
	(2) Create configuration template **wlan-temp1** and import the content in the **temp-test1.text** file to the configuration template.
	`Center AC (config)#cfgmg template wlan-temp1`
	`Center AC (config-temp)#import temp-test1.text`
	(3) Check whether the commands in the **temp-test1.text** file are imported to the configuration template successfully.
	`Center AC (config-temp)#show cfgmg template name wlan-temp1`

```
1: wlan-config 10 wlan-test1
2: tunnel local
3: wlan-config 20 wlan-test2
4: tunnel local
```

(4) Create the content in the **temp-test2.text** file.

```
wlan-config 30 wlan-test3
tunnel local
wlan-config 40 wlan-test4
tunnel local
```

(5) Create configuration template **wlan-temp2** and import the content in the **temp-test2.text** file to the configuration template.

```
Center AC (config)#cfgmg template wlan-temp2
Center AC (config-temp)#import temp-test2.text
```

(6) Check whether the commands in the **temp-test2.text** file are imported to the configuration template successfully.

```
Center AC (config-temp)#show cfgmg template name wlan-temp2
1: wlan-config 30 wlan-test3
2: tunnel local
3: wlan-config 40 wlan-test4
4: tunnel local
```

- On the center AC, apply configuration templates.

(1) On the center AC, apply configuration template **wlan-temp1** to the hot standby instance of Branch AC-1.

```
Center AC (config)#wlan hot-backup 100.100.102.72
Center AC (config-hotbackup)#cfgmg template wlan-temp1
```

(2) On the center AC, apply configuration template **wlan-temp2** to the hot standby instance of Branch AC-2.

```
Center AC (config)#wlan hot-backup 63.254.254.47
Center AC (config-hotbackup)#cfgmg template wlan-temp2
```

- On a branch AC, request configuration templates.

(1) Apply configuration templates **wlan-temp1** and **wlan-temp2** to Branch AC-1.

```
Branch AC-1 (config)#wlan hot-backup 89.2.1.78
Branch AC-1 (config-hotbackup)#request cfgmg template wlan-temp1
Branch AC-1 (config-hotbackup)#request cfgmg template wlan-temp2
```

(2) Check whether Branch AC-1 requests **wlan-temp1** and **wlan-temp2** successfully.

```
Branch AC-1 (config-hotbackup)#show layerac template peer 89.2.1.78
Apply in center:
1. wlan-temp1

Request in branch:
1. wlan-temp1
2. wlan-temp2
```

(3) On Branch AC-2, request configuration templates **wlan-temp1** and **wlan-temp2**.

```
Branch AC-2 (config-hotbackup)#request cfgmg template wlan-temp1
Branch AC-2 (config-hotbackup)#request cfgmg template wlan-temp2
```

(4) Check whether Branch AC-2 requests **wlan-temp1** and **wlan-temp2** successfully.

```
Branch AC-2 (config-hotbackup)#show layerac template peer 89.2.1.78
Apply in center:
1. wlan-temp1

Request in branch:
1. wlan-temp1
2. wlan-temp2
```

- Automatic configuration template synchronization

(1) Establish a hot standby channel between a branch AC and the center AC. If the following syslog is displayed on the branch AC, configuration template synchronization is complete.

```
Branch AC-1#
*Apr 26 17:18:39: %LAYERAC-6-CONFIG_SYNC: The template configuration has been
successfully synchronized from the center ac(89.2.1.78).
```

(2) Run the **show running** command on Branch AC-1 to confirm that commands in the template are synchronized.

```
Branch AC-1#show running | beggning wlan-config
wlan-config 10 wlan-test1
 ssid-code utf-8
 tunnel local
!
wlan-config 20 wlan-test2
 ssid-code utf-8
 tunnel local
!
```

(3) Run the **show layerac template peer** command on Branch AC-1 to display the configuration templates requested by Branch AC-1 and applied by the center AC.

```
Branch AC-1 (config-hotbackup)#show layerac template peer 89.2.1.78
Apply in center:
1. wlan-temp1

Request in branch:
1. wlan-temp1
2. wlan-temp2
```

(4) Run the **show running** command on Branch AC-2 to confirm that commands in the template are synchronized.

```
Branch AC-1#show running | begging wlan-config
wlan-config 30 wlan-test3
 ssid-code utf-8
 tunnel local
```

```
!
wlan-config 40 wlan-test4
 ssid-code utf-8
 tunnel local
!
```

(5) Run the **show layerac template peer** command on Branch AC-2 to display the configuration templates requested by Branch AC-2 and applied by the center AC.

```
Branch AC-2 (config-hotbackup)#show layerac template peer 89.2.1.78
Apply in center:
1. wlan-temp2

Request in branch:
1. wlan-temp1
2. wlan-temp2
```

- Modify commands in a configuration template on the center AC.

(1) Modify commands in the configuration template **wlan-temp1** on the center AC and display the modification result.

```
Center AC (config)#cfgmg template wlan-temp1
Center AC (config-temp)#line 1 wlan-config 11 wlan-test11
Center AC (config-temp)#line 3 wlan-config 22 wlan-test22
Center AC (config-temp)#show this

Building configuration...
!
 line 1 wlan-config 11 wlan-test11
 line 2 tunnel local
 line 3 wlan-config 22 wlan-test22
 line 4 tunnel local
!
end
```

(2) Modify commands in the configuration template **wlan-temp2** on the center AC and display the modification result.

```
Center AC (config)#cfgmg template wlan-temp2
Center AC (config-temp)#line 1 wlan-config 33 wlan-test33
Center AC (config-temp)#line 3 wlan-config 44 wlan-test44
Center AC (config-temp)#show this

Building configuration...
!
 line 1 wlan-config 33 wlan-test33
 line 2 tunnel local
 line 3 wlan-config 44 wlan-test44
 line 4 tunnel local
```

```
!
end
```

- Manual triggering of configuration template synchronization

(1) Run the following commands in hot standby configuration mode of Branch AC-1 on the center AC.

```
Center AC (config)#wlan hot-backup 100.100.102.72
Center AC (config-hotbackup)#sync cfgmg template
```

(2) Run the following commands in hot standby configuration mode of Branch AC-2 on the center AC.

```
Center AC (config)#wlan hot-backup 63.254.254.47
Center AC (config-hotbackup)#sync cfgmg template
```

(3) Run the following command on Branch AC-1 to check whether the commands in the template are synchronized.

```
Branch AC-1#sh run | b wlan-config
wlan-config 10 wlan-test1
 ssid-code utf-8
 tunnel local
!
wlan-config 11 wlan-test11
 ssid-code utf-8
 tunnel local
!
wlan-config 20 wlan-test2
 ssid-code utf-8
 tunnel local
!
wlan-config 22 wlan-test22
 ssid-code utf-8
 tunnel local
```

(4) Run the show running command on Branch AC-2 to check whether the commands in the template are synchronized.

```
Branch AC-2#sh run | b wlan-config
wlan-config 30 wlan-test3
 ssid-code utf-8
 tunnel local
!
wlan-config 33 wlan-test33
 ssid-code utf-8
 tunnel local
!
wlan-config 40 wlan-test4
 ssid-code utf-8
 tunnel local
!
wlan-config 44 wlan-test44
 ssid-code utf-8
```

	tunnel local !

Common Errors

A non-existent template is applied on the center AC or requested by a branch AC. Because the template does not exist, no content is synchronized to the branch AC.

1.4.2 Configuring Configuration Command Synchronization

Configuration Effect

- The configuration of the center AC can be synchronized to a branch AC only when configuration synchronization is enabled on the center AC.
- The configuration on a branch AC can be synchronized to the center AC only when configuration synchronization is enabled on the branch AC.

Notes

N/A

↘ Enabling Configuration Command Synchronization

- Enable configuration command synchronization.

Command	**config command sync enable**
Parameter Description	N/A
Defaults	Configuration command synchronization is enabled by default.
Command Mode	Global configuration mode
Usage Guide	1. When configuration synchronization is disabled on a branch AC, the branch AC cannot synchronize configuration to the center AC. However, the center AC can synchronize configuration to the branch AC. 2. When configuration synchronization is disabled on the center AC, the center AC cannot synchronize configuration to the branch AC. However, the branch AC can synchronize configuration to the center AC. 3. Configuration command synchronization takes effect only in the hierarchical AC scenario. The synchronized commands are configurations of AP groups in the hot standby instance and configurations of APs associated with the AP groups. 4. Synchronization of commands that depend on other commands or files may fail. For example, the **interface-mapping** command depends on the WLAN. Therefore, the WLAN needs to be configured at both ends in advance. The file specified by the **auto-cfg file** *filename* command must be uploaded to the AC in advance. 5. After commands are configured through the NMS software, such as the Simple Network Management Protocol (SNMP) network management platform or smart network controller (SNC), configuration command synchronization is not triggered by default. You need to manually run this command in configuration mode to trigger configuration collection.

Verification

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

Configuration Example

Configuring Configuration Command Synchronization

Configuration Steps	Use a typical hierarchical AC case as an example. Create group **branch1** on the center AC and add **branch1** to the hot standby instance of Branch AC-1. Add configuration to **branch1** and confirm that configuration of **branch1** can be synchronized to Branch AC-1. Add an AP to **branch1** and confirm that configuration of the AP can be synchronized to Branch AC-1. After configuration of **branch1** is synchronized to Branch AC-1, Branch AC-1 deletes or modifies configuration of b**ranch1** and can synchronize the configuration to the center AC.
	● Enable configuration command synchronization on the center AC and a branch AC.

	(1) Enable configuration command synchronization on the center AC.
	`Center AC (config)#config command sync enable`
	`Check whether configuration command synchronization is enabled on the center AC.`
	`Center AC #show run | in config command sync enable`
	`config command sync enable`
	(2) Enable configuration command synchronization on Branch AC-1.
	`Branch AC (config)#config command sync enable`
	(3) Check whether configuration command synchronization is enabled on Branch AC-1.
	`Branch AC-1 #show run | in config command sync enable`
	`config command sync enable`

	● Synchronize configuration commands of the AP groups in the hot standby instance.

	(1) Create **branch1** on the center AC and add commands.
	`Center AC (config)#ap-group branch1`
	`Center AC (config-group)#interface-mapping 10 10 ap-wlan-id 1`
	`Center AC (config-group)#interface-mapping 20 20 ap-wlan-id 2`
	`Center AC (config-group)#sh th`
	
	`Building configuration...`
	`!`
	` interface-mapping 10 10 ap-wlan-id 1`
	` interface-mapping 20 20 ap-wlan-id 2`
	`!`
	`end`
	(2) On the center AC, add branch1 to the hot standby instance of Branch AC-1.
	`Center AC (config)#wlan hot-backup 100.100.102.72`
	`Center AC (config-hotbackup)#context 0`
	`Center AC (config-hotbackup-ctx)#ap-group branch1`
	(3) On the center AC, check whether **branch1** is added to the hot standby instance of Branch AC-1 successfully.
	`Center AC (config-hotbackup-ctx)#show this`

```
Building configuration...
!
  ap-group branch1
  peer-ip 100.100.102.72
!
end

Center AC (config-group)#ap-group branch1
Center AC (config-group)#sh th

Building configuration...
!
end
```

(4) On Branch AC-1, check whether **branch1** is added to the hot standby instance.

```
Branch AC-1#show run | b wlan hot-backup
wlan hot-backup branch
!
wlan hot-backup 89.2.1.78
 local-ip 100.100.102.72
 !
 context 0
  ap-group branch1
  peer-ip 89.2.1.78
 !
 wlan hot-backup enable
!
```

(5) On Branch AC-1, check whether the configuration of **branch1** is synchronized.

```
Branch AC-1#show run | b ap-group branch1
ap-group branch1
 interface-mapping 10 10 ap-wlan-id 1
 interface-mapping 20 20 ap-wlan-id 2
!
```

- Synchronize configuration commands of APs in the hot standby instance.

(1) On the center AC, add AP **sync-test** to **branch1**.

```
Center AC (config)#ap-config sync-test
You are going to config AP(sync-test), which is online now.
Center AC (config-ap)#ap-group branch1
Center AC (config-ap)#show ap-config run sync-test

Building configuration...
Current configuration: 426 bytes

!
```

```
ap-config sync-test
 ap-mac 8005.880a.b557
 ap-group branch1
 ript enable
 power local 50 radio 1
 power local 50 radio 2
 power local 50 radio 3
 channel 11 radio 1
 channel 64 radio 2
 channel 149 radio 3
 chan-width 20 radio 1
 chan-width 40 radio 2
 chan-width 20 radio 3
!
End
```

(2) On **b**ranch AC-1, check whether configuration of AP **sync-test** is synchronized.

```
Branch AC-1 #show ap-config run sync-test

Building configuration...
Current configuration: 359 bytes

!
ap-config sync-test
 ap-mac 8005.880a.b557
 ap-group branch1
 ript enable
 power local 50 radio 1
 power local 50 radio 2
 power local 50 radio 3
 channel 11 radio 1
 channel 64 radio 2
 channel 149 radio 3
 chan-width 20 radio 1
 chan-width 40 radio 2
 chan-width 20 radio 3
!
end
```

- Modify the configuration of the AP group on the branch AC and check whether the configuration on the center AC is also modified.

(1) On Branch AC-1, modify the configuration of the AP group.

```
Branch AC-1 (config)#ap-group branch1
Branch AC-1 (config-group)#no interface-mapping 20 20
Branch AC-1 (config-group)#interface-mapping 22 22
Branch AC-1 (config-group)#show this
```

```
Building configuration...
!
 interface-mapping 10 10 ap-wlan-id 1
 interface-mapping 22 22 ap-wlan-id 2
!
end
```

(2) On the center AC, check that the configuration modified on Branch AC-1 is synchronized.

```
Center AC (config)#ap-group branch1
Center AC (config-group)#show this

Building configuration...
!
 interface-mapping 10 10 ap-wlan-id 1
 interface-mapping 22 22 ap-wlan-id 2
!
end
```

Common Errors

The command or file that a command depends on is not pre-configured on the center AC and branch AC. As a result, configuration synchronization fails.

After commands are configured through the NMS software, such as the SNMP network management platform or SNC, configuration command synchronization is not manually triggered. As a result, the configuration commands cannot be synchronized.

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show layerac config-sync summary	Displays the template synchronization status.
show layerac template name	Displays application and request of the specified configuration template in branch ACs.
show layerac cli record	Displays template commands run by the LAYERAC module in the CLI.
show layerac template peer	Displays templates applied to and requested by the specified branch AC.

Debugging

N/A

Configuring WLAN Optimization and Maintenance

1. Configuring WLOG
2. Configuring WLAN Optimization
3. Configuring WIS
4. Configuring STA-TRACE
5. Configuring Broadcast Forwarding Control
6. Configuring Metric Monitoring

1 Configuring WLOG

1.1 Overview

WLAN Log (WLOG) enables the access controller (AC) to store and view the wireless network and station (STA) status in the past period of time. By collecting and storing information about the wireless network, access points (APs), and STAs in the past 24 hours and then displaying such information through CLI commands, WLOG allows users to analyze the wireless network status and troubleshoot problems.

WLOG can be used to collect and store information, but does not support automatic information analysis and diagnosis.

WLOG information can be installed on an AC or AP. Except that STA spatial information is stored on the AP, all other information is stored on the AC.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Fit AP Networking	The Fit AP networking includes at least one AC and one AP.

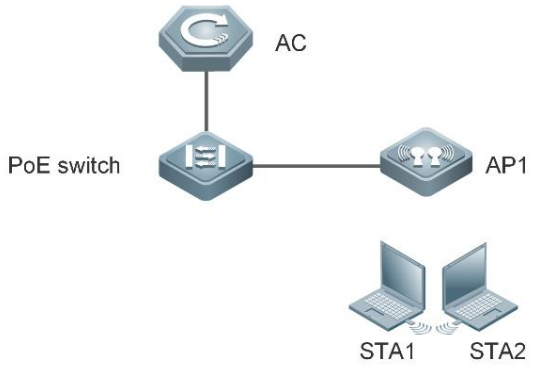
1.2.1 Fit AP Networking

Scenario

Deploy an AC on a wireless network to query information on the network, and AP and STAs associated with the AC.

Figure 1-1 shows the networking topology for viewing information on the network, AP and STAs associated with the AC.

Figure 1-1



Deployment

- Enable the WLOG feature on an AC.

1.3 Features

Basic Concepts

Two Modes of Information Collection on the AC

- Periodic collection

The summary of the entire network, AP, and STA is collected and stored once or at an interval of 1 hour. The AP and STA summary covers all the information about online APs and STAs.

- Reception advertisement collection

When an AP behavior occurs, the WLOG module is informed to collect and store information about the behavior.

When a STA behavior occurs, the WLOG module is informed to collect and store information about the behavior.

Information collection on the AP covers only periodic collection of spatial information on all online STAs.

Summary of the Entire Network

- Continuous operation time of the AC
- Number of online APs
- Number of pre-configured and offline APs
- Versions of online APs (number of APs of each version)
- Information on each WLAN (SSID) includes:
- Number of online STAs which have passed web-based authentication
- Number of online STAs which have passed 802.1X authentication
- Number of online authentication-free STAs

Summary of the AP

- AP's name
- AP's MAC address
- AP's IP address
- AP's uptime
- Status of each wired interface of the AP
- Input/output rate (bits/sec) in the last 5 minutes
- Statistics on received or sent unicast, broadcast, multicast, and error frames
- Summary of each radio
- Working channel
- Transmit power (dBm, absolute value)
- Number of associated online STAs
- Number of online STAs which have passed web-based authentication
- Number of online STAs which have passed 802.1X authentication

- Intensity of the co-channel interference signal
- Number of received error frames
- Packet retransmission count

Summary of the STA

- IP address
- Signal strength
- Access rate
- Associated AP, radio, and SSID

STA's Spatial Information

- The STA's spatial information includes statistics on data frames and management frames of the STA, and statistics on each type of the rate:
- Number of data frames successfully transmitted (from the AP to the STA)/total traffic
- Number of unresponsive data frames/total traffic
- Number of management frames/total traffic
- Statistics of each type of frames with the 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

- Statistics of each type of frames with the 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 there is a high proportion of frames for which no ACK frame is transmitted, and whether many management frames are transmitted and received, so as to further analyze and locate the network problems caused by low-speed STAs, management frame attacks, and poor conditions. The STA's spatial information varies in real time, and is collected every five minutes. The information is saved only on the AP due to a large data volume.

AP Behavior Type

The AP behavior type includes login, logout, and CAPWAP connection failures.

STA Behavior Type

The STA behavior type includes association, de-association, roaming, and login and logout through web-based authentication or 802.1X authentication.

Overview

Feature	Description
Enabling the WLOG Feature	Enables the WLOG feature to automatically collect AC, AP, and STA information.

Feature	Description
Synchronizing STA Login or Logout Information to the erver	Synchronizes STA login or logout information to the Elog server.
Configuring the AP Detection Function	An AP detects information about STAs and hotspots nearby.
Synchronizing Information Detected by an AP to the	An AC synchronizes STA information and hotspot information detected by an AP to the Elog server.
Generating Detected STA Information in Syslog Format	Generates STA information detected by the AP in syslog format for output.
Interconnecting with the BCR	Sends information about STAs to the BCR device.

1.3.1 Enabling the WLOG Feature

After the WLOG feature is enabled, the AC or AP automatically collects AC, AP, and STA information and records the information into memory. This helps a network administrator 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 AC or AP automatically collects AC, AP, and STA information and records the information into memory, and receives login or logout advertisement of the AP and STA and records into memory for query.

1.3.2 Synchronizing STA Login or Logout Information to the Elog Server

After the WLOG function is enabled and the URL of the Elog server is configured, the AC sends STA login or logout information to the Elog server.

Working Principle

After the WLOG function is enabled and the AC receives the STA login or logout notification, the AC sends STA information in a specific format to the Elog server.

1.3.3 Configuring the AP Detection Function

The AP detection function is used to detect STAs and hotspots around an AP. The AP detection function can be configured to detect either or both of STAs and hotspots.

Working Principle

After an AC delivers the command of enabling the AP detection function, the AP periodically reports the detected information to the AC for reprocessing.

1.3.4 Synchronizing Information Detected by an AP to the Elog Server

An AC reports information detected by an AP to the Elog server.

Working Principle

An AC reports information detected by an AP in a specific format to the Elog server.

1.3.5 Generating Detected STA Information in Syslog Format

An AC generates detected STA information in syslog.

Working Principle

Generate STAs information detected by an AP in a specified syslog format for output.

1.3.6 Interconnecting with the BCR Server

After the WLOG function is enabled, configure the URL and type of the BCR server. When a STA goes online or offline, relevant information about the STA will be sent to the BCR server.

Working Principle

On the AC enabled with WLOG, when a STA goes online or offline, relevant information about the STA will be sent to the BCR server, and STA login or logout log will be generated on the local device.

1.4 Configuration

Configuration	Description and Command	
Enabling the WLOG Feature	(Mandatory) It is used to enable the WLOG feature.	
	wlan diag enable	Enables the WLOG feature.
Synchronizing STA Login or Logout Information to the	(Optional) It is used to synchronize STA login or logout information to the Elog server.	
	web-server enable api-path assoc-sta url *url*	Configures the address of the Elog server.
Configure the AP Detection Function	(Optional) It is used to enable the detection function of an AP.	
	ap-probe ap enable	Enables the hotspot information detection function of an AP.
	ap-probe sta enable	Enables the STA information detection function of an AP.
	ap-probe cache-time	Configures the time for caching detection information (aging) for an AP.
	ap-probe upload-time	Configures the interval for periodically reporting detection information for an AP.
	ap-probe limit	Configures the number of non-repeated detection information records that can be received within aging period for the AP.
Synchronizing Information Detected by an AP to the	(Optional) It is used to synchronize information detected by an AP to the Elog server.	
	web-server enable api-path probe-ap url *url*	Configures the Elog address to which the hotspot information detected by an AP is synchronized.

Configuration	Description and Command	
	web-server enable api-path probe-sta url *url*	Configures the Elog address to which the STA information detected by an AP is synchronized.
Generating Detected STA Information in Syslog	(Optional) It is used to generate detected STAs in syslog format.	
	web-server enable api-path probe-sta syslog	Generates detected STAs in syslog format.
Interconnecting with the BCR Device	(Optional) It is used to interconnect with the BCR device.	
	web-server enable api-path auth-sta url ***url***	Configures the URL to interconnect with the BCR server.
	web-server enable api-path auth-sta type ***type***	Configures the authentication type to interconnect with the BCR server.

1.4.1 Enabling the WLOG Feature

Configuration Effect

- After the WLOG feature is enabled, the AC or AP automatically records the AC, AP, and STA information.

Notes

- Enabling the WLOG will result in memory pre-allocation. If the memory is insufficient, 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.
- Enable the WLOG feature in global configuration mode of the AC.
- After the WLOG feature is enabled, information is collected and recorded into the memory periodically.

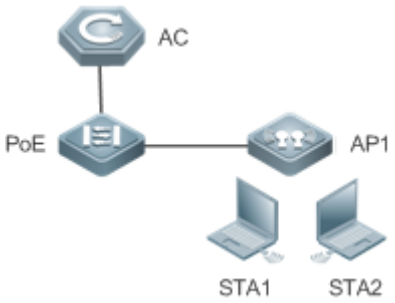
Command	**wlan diag enable**
Parameter Description	N/A
Defaults	By default, the WLOG feature is disabled on the AC and AP.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show wlan diag network** command to check whether the entire network information can be viewed on the AC.
- Run the **show wlan diag sta** command to check whether the STA information can be viewed on the AC.

Configuration Example

Enabling the WLOG Feature

Scenario **Figure 8-2**	
Configuration Steps	● Enable the WLOG feature in global configuration mode.
AC	`Hostname# configure terminal` `Hostname(config)# wlan diag enable`
Verification	● Use the **show wlan diag network** command to display the summary of the entire network.

AC	`Hostname# show wlan diag network`
	`Time: 2017-05-05 14:57:07`
	`AC uptime: 10 h`
	`Online AP: 1`
	`Offline AP:0`
	`Online AP Version:`
	`PID HwVer SwVer AP Number`
	`--- ---`
	`--- ---`
	`AP520 1.00 AP_RGOS 11.1(5)B9P2, Release(04162423) 1`
	
	`Wlan information:`
	`WLAN ID SSID Active STA WEB Auth 1X Auth Other`
	
	`--- --- --- --- --- ---`
	`4 wlan-guest 2 2 0 0`
	
	`5 wlan-802.1x 6 0 6 0`

1.4.2 Synchronizing STA Login or Logout Information to the Elog Server

Whether this function is supported depends on the actual product version.

Configuration Effect

- After the WLOG function is enabled and the URL of the Elog server is configured, the AC sends the STA login or logout information to the Elog server.

Notes

- This function is triggered by the STA login or logout action. Before the function is enabled, the STA login or logout information is not sent to the Elog server.

Configuration Steps

Configuring the URL of the Elog Server

- The complete address of the Elog server needs to be configured.

Command	**web-server enable api-path assoc-sta url** *url*
Parameter Description	*url*: indicates the URL of the Elog server.
Defaults	By default, the URL of the Elog server is not configured, that is, the AC does not interwork with the Elog server.
Command Mode	Global configuration mode
Usage Guide	To ensure smooth data transmission, the WLOG function needs to be enabled. In local forwarding scenarios, if the AC does not obtain the STA's IP address (which can be queried by running the **show ac-config client** command) after the STA goes online, run the **ip dhcp snooping** command in global configuration mode to ensure that the AC can obtain the STA's IP address. Up to eight Elog servers are supported. Whether this configuration is supported depends on the actual product version.

Verification

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

Configuration Example

Configuring the URL of the Elog Server

Configuration Steps	● In global configuration mode, configure two URLs of Elog servers.

AC	`Hostname# configure terminal`
	`Hostname(config)#web-server enable api-path assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta`
	`Hostname(config)# web-server enable api-path assoc-sta url http://172.18.155.15:8080/elog/service/dc/updateSta`

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

AC	`Hostname# show running-config`
	`!`
	`web-server enable api-path assoc-sta url http://172.18.155.14:8080/elog/service/dc/updateSta`

	http://172.18.155.14:8080/elog/service/dc/updateSta web-server enable api-path assoc-sta url http://172.18.155.15:8080/elog/service/dc/updateSta !

Common Errors

- Only an IP address but not a complete URL is specified in *url*.

Common Errors

- N/A

1.4.3 Configure the AP Detection Function

Whether this function is supported depends on the actual product version.

Configuration Effect

After an AC delivers the command of enabling the AP detection function, the AP periodically reports detected STA information and hotspot information to the AC.

Configuration Steps

Enabling the Hotspot Information Detection 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 or all-AP configuration mode
Usage Guide	N/A

Enabling the STA Information Detection 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 or 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 on the AP.

Command	**ap-probe cache-time** *time*
Parameter Description	*time*: Indicates the cache time (aging time). The value range is from 0 to 3600, in seconds.
Defaults	The default value is 120s.
Command Mode	AP configuration mode, AP group configuration mode, or 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 duplicate information being reported to the AC. A high packet sending frequency may cause the high CPU load of the AP and potentially impact wireless services. It is recommended that this configuration be performed only during debugging, and you are not advised to set the cache time to 0 seconds in normal situations.

Configuring the Interval for Periodically Reporting Detected Information for an AP

- Optional. Configure the interval for periodically reporting detected information for an AP.

Command	**ap-probe upload-time** *time*
Parameter Description	*time*: Indicates the interval for periodically reporting detected information. The value range is from 1 to 300, in seconds.
Defaults	The default value is 5s.
Command Mode	AP configuration mode or 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-repeated 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 range is from 1 to 65535. The actual number of records that can be cached on an AP depends on the AP's memory.
Defaults	The default value is 100.
Command Mode	AP configuration mode or 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 is used. Cached information occupies memory resources, so do not set it to a large number.

Verification

- Run the **show running-config** command to display the detection configuration in all-AP configuration mode.
- Run the **show ap-config running** command to display the configuration in AP configuration mode.

Configuration Example

Enabling the Detection Function of AP 1

Configuration Steps	● Enable the hotspot and STA detection function in AP configuration mode. Set the cache time to 60s, report interval to 6s, and the number of non-repeated detected information that can be cached to 200.

AC	`Hostname# configure terminal`
	`Hostname(config)#ap-config AP1`
	`You are going to config AP(AP1), which is online now.`
	`Hostname(config-ap)#ap-probe ap enable`
	`Hostname(config-ap)#ap-probe sta enable`
	`Hostname(config-ap)#ap-probe cache-time 60`
	`Hostname(config-ap)#ap-probe upload-time 6`
	`Hostname(config-ap)#ap-probe limit 200`
	`Hostname(config-ap)#`

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

AC	`Hostname# show ap-config running`
	`!`
	`ap-config AP1`
	` ap-mac 1234.1234.5656`
	` ap-probe sta enable`
	` ap-probe ap enable`
	` ap-probe upload-time 6`
	` ap-probe cache-time 60`
	` ap-probe limit 200`
	`!`

1.4.4 Synchronizing Information Detected by an AP to the Elog Server

Whether this function is supported depends on the actual product version.

Configuration Effect

- After the hotspot information detection function of an AP is enabled and the URL of the Elog server to which the detected hotspot information is synchronized is configured, the AC sends the detected hotspot information reported by the AP to the Elog server.
- After the STA information detection function of an AP is enabled and the URL of the Elog server to which the detected STA information is synchronized is configured, the AC sends the detected STA information reported by the AP to the Elog server.

Configuration Steps

Configuring the URL of the Elog Server to Which Hotspot Information Detected by an AP Is Synchronized

- The complete address of the Elog server needs to be configured.

Command	**web-server enable api-path probe-ap url** *url*
Parameter Description	*url*: Indicates the complete address of the Elog server for storing detected hotspot information.

Defaults	By default, The Elog server's URL is not configured, that is, an AC is not connected to the Elog server.
Command Mode	Global configuration mode
Usage Guide	A maximum of eight Elog servers can be configured.

Configuring the URL of the Elog Server to Which STA Information Detected by an AP Is Synchronized

- The complete address of the Elog server needs to be configured.

Command	**web-server enable api-path probe-sta url** *url*
Parameter Description	*url*: Indicates the complete address of the Elog server for storing detected STA information.
Defaults	By default, The Elog server's URL is not configured, that is, an AC is not connected to the Elog server.
Command Mode	Global configuration mode
Usage Guide	A maximum of eight Elog servers can be configured.

Verification

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

Configuration Example

Configuring the URL of the Elog Server to Which Information Detected by an AP Is Synchronized

Configuration Steps	• In global configuration mode, set the URL of the first Elog server for storing detected hotspot information to http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid and the URL of the second Elog server to http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSsid. • In global configuration mode, set the URL of the first Elog server for storing detected STA information to http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta and the URL of the second Elog server to http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSta.

AC	`Hostname# configure terminal`
	`Hostname(config)# web-server enable api-path probe-ap url http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid`
	`Hostname(config)# web-server enable api-path probe-ap url http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSsid`
	`Hostname(config)# web-server enable api-path probe-sta url http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta`
	`Hostname(config)# web-server enable api-path probe-sta url http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSta`

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

AC	`Hostname# show running-config`
	`!`
	`web-server enable api-path probe-ap url http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSsid`

	http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSsid web-server enable api-path probe-sta url http://172.21.155.131:8080/elog/service/dc/updateAcCapturedSta http://172.21.155.132:8080/elog/service/dc/updateAcCapturedSta!

1.4.5 Generating Detected STA Information in Syslog Format

Whether this function is supported depends on the actual product version.

Configuration Effect

After this function is enabled, information about detected STAs will be generated in syslog format.

Notes

This command cannot be used with the **web-server enable api-path probe-sta url** *url* command.

Configuration Steps

Generating Detected STA Information in Syslog Format

Command	**web-server enable api-path probe-sta syslog**
Parameter Description	N/A
Defaults	This function is disabled by default.
Command Mode	Global configuration mode
Usage Guide	This command cannot be used with the **web-server enable api-path probe-sta url** *url* command.

Verification

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

Configuration Example

Generating Detected STA Information in Syslog Format

Configuration Steps	● Enable the device to generate information about detected STAs in global configuration mode.
AC	Hostname# configure terminal Hostname(config)# web-server enable api-path probe-sta syslog
Verification	● Run the **show running-config** command to display the configuration.
AC	Hostname# show running-config ! web-server enable api-path probe-sta syslog !

1.4.6 Interconnecting with the BCR Server

Configuration Effect

- When the AC is enabled with WLOG and configured with the URL and type of the BCR server for interconnection, the AC sends STA login or logout information to the BCR server.

Notes

N/A

Configuration Steps

↘ Configuring the URL for the BCR Server Where STA Login or Logout Information Will Be Sent

- To configure the URL, enter the http:// prefix and the part of the web address following it, such as proline/Msg. You only need to enter information preceding the question mark (?).

Command	**web-server enable api-path auth-sta url** *url*
Parameter Description	*url*: Indicates the prefix of the BCR server address.
Defaults	The URL is not configured by default. That is, the AC does not interconnect with the BCR server by default.
Command Mode	Global configuration mode
Usage Guide	In global configuration mode, first enable WLOG, and then configure the URL of the BCR server for interconnection (enter the http:// prefix and the part of the web address following it, such as proline/Msg). You only need to enter information preceding the question mark (?).

↘ Configuring the Authentication Type for the BCR Server Where STA Login or Logout Information Will Be Sent

- The type value depends on the corresponding input authentication type value.

Command	**web-server enable api-path auth-sta type** *type*
Parameter Description	*type*: Indicates the authentication type.
Defaults	The default type is 1020004.
Command Mode	Global configuration mode
Usage Guide	In global configuration mode, first enable WLOG, and then u configure the authentication type for interconnection with the BCR server.

Verification

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

Configuration Example

↘ Configuring the URL for the BCR Server Where STA Login or Logout Information Will Be Sent

Configuration	● For example, in global configuration mode, configure the URL of the BCR server as

Steps	http://10.18.78.149:19900/pronline/Msg.
AC	`Hostname# configure terminal` `Hostname(config)#web-server enable api-path auth-sta url http://10.18.78.149:19900/pronline/Msg`
Verification	● Run the **show running-config** command to display the configuration.
AC	`Hostname# show running-config` `web-server enable api-path auth-sta url http://10.18.78.149:19900/pronline/Msg`

Configuring the Authentication Type Value for the BCR Server Where STA Login or Logout Information Will Be Sent

Configuration Steps	● For example, in global configuration mode, configure the authentication type of the BCR server as 1020002.
AC	`Hostname# configure terminal` `Hostname(config)#web-server enable api-path auth-sta type 1020002`
Verification	● Run the **show running-config** command to display the configuration.
AC	`Hostname# show running-config` `web-server enable api-path auth-sta type 1020002`

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show wlan diag network Whether this configuration is supported depends on the actual product version.	Displays the general information on the whole network
show wlan diag ap [**ap-mac** *ap-mac*] [**number** *number*]	Displays the AP information on the AC
show wlan diag sta [**sta-mac** *sta-mac*] [**ip-range** *ip-prefix*] [**action** *action* [**result** *result*]] [**number** *number*]	Displays the STA information on the AC
show wlan diag sta [**sta-mac** *sta-mac*] [**number** *number*]	Displays STA information on the AP.

1 Configuring WLAN Optimization

1.1 Overview

Wireless network optimization is to optimize the wireless network and enhance the experience of wireless users by adjusting the WLAN configuration.

WLAN configuration optimization can achieve the following effects:

- Reduce co-channel interference and adjacent-channel interference and enhance signal coverage.
- Increase the channel bandwidth.
- Improve the channel utilization.
- Improve the available channel bandwidth for wireless users.
- Decrease network attacks and multicast packet bandwidth usage.
- Improve the downlink throughput of an access point (AP).
- Reduce weak-signal terminals and overall wireless network performance.
- Reduce the impact of the power-saving network adapter.
- Limit the number of access users.

Different WLAN optimization methods are applicable to different application scenarios.

WLAN Optimization Method	Application Scenario
Channel planning and adjustment	This method is used as required.
Power planning and adjustment	This method is used as required.
Terminating low-rate applications	This method is applicable to the high-density deployment scenario (school and building).
Establishing a pure 802.11n wireless network	This method is used as required.
Adjusting Beacon sending interval	This method is applicable to the high-density deployment scenario where many service set identifiers (SSIDs) are configured for the AP.
Enabling Layer 2 isolation for wireless users in a VLAN	This function is mandatory for the network where Layer 2 mutual access is not required.
Enabling the RTS/CTS protection mechanism	This method is applicable to the network involving indoor coverage.
Enhancing the AP's packet sending priority and suppressing packet sending by a STA	It is recommended that you determine whether to use this method based on actual effects.
Reducing the influence of weak-signal terminals	This method is applicable to the high-density deployment scenario (school and building).
Band selection	This method is applicable to the high-density deployment scenario where an AP supports dual bands.
Power-saving STA processing optimization	This method is applicable to all scenarios.
802.11n A-MPDU aggregation frame sending protection	This method is applicable to all scenarios.

WLAN Optimization Method	Application Scenario
Limiting the number of STAs connected to an AP	This method is applicable to the high-density deployment scenario (school and building) with lots of wireless users.

Protocol Specification

IEEE Std 802.11-2012: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

1.2 Applications

Application	Description
802.11n	Both the AP and STA support the 802.11n network.
Spectrum Navigation for a WLAN Composed of Fit APs	In the Fit AP architecture, spectrum navigation is enabled for the WLAN composed of multiple dual-band APs.

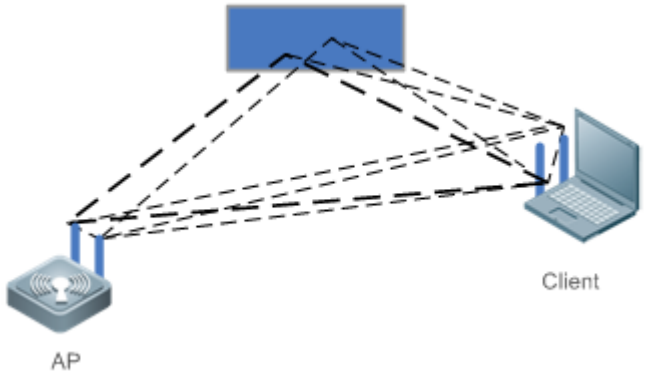
1.2.1 802.11n

Scenario

As a new protocol of the 802.11 protocol suite, 802.11n supports two frequency bands, that is, 2.4 GHz and 5 GHz. 802.11n aims to provide WLAN access users with higher access rate. It improves the communication rate by using the MIMO technology or by increasing the bandwidth and improving the channel utilization.

As shown in Figure 1-1, the client accesses the wired network through the AP; the client and AP communicate with each other in wireless mode; and there are multiple transmission paths between the client and AP.

Figure 1-1



Deployment

Enable the IEEE802.11 protocol on the AP and client to implement access and authentication of the client.

1.2.2 Spectrum Navigation for a WLAN Composed of Fit APs

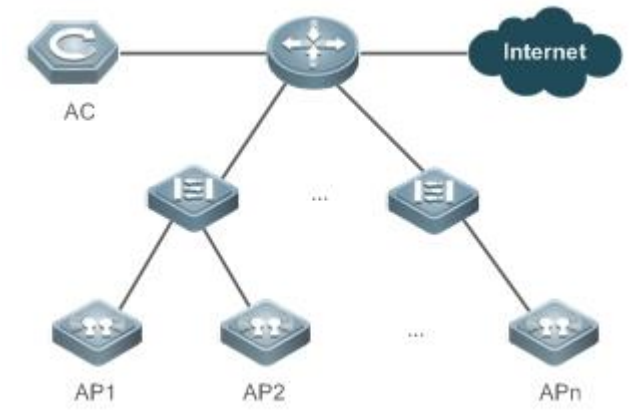
Scenario

In the Fit AP architecture, spectrum navigation is enabled for the WLAN composed of multiple dual-band APs.

In Figure 1-2:

- One access controller (AC) is associated with many dual-band APs. The AC and APs are connected by the Layer 2 switching device and Layer 3 routing device.
- The WLAN is mapped to the two radio frequency (RF) interfaces of all dual-band APs.

Figure 1-2



Deployment

- Manage operating parameters of the spectrum navigation function on the AC.
- Enable the spectrum navigation function on the AP to identify the STA type and guide STA access.

1.3 Features

Basic Concepts

WLAN

A Wireless Local Area Network (WLAN) interconnects computers by using the wireless communication technology to form a network system that supports mutual communication and resource sharing. It uses the wireless mode but not communication cables, making it flexible to build a network and migrate a terminal.

AP

An AP is used for a wireless terminal to access a wired network. It serves as the communication bridge between a wireless terminal and a wired network.

STA

A station (STA) refers to the user who accesses the Internet by using a wireless terminal.

RSSI

The Received Signal Strength Indication (RSSI) is used to indicate the quality of a wireless link.

Overview

Feature	Description

Feature	Description
Terminating Low-Rate Applications	Terminates low-rate applications by configuring the rate set.
Increasing the Beacon Frame Period Appropriately	Increases the Beacon frame period; reduces the frequency of sending Beacon frames; reduces the channel utilization for packet management; increases the available channel bandwidth for wireless users.
Configuring Layer 2 Isolation of Wireless Users in a VLAN	Configures this function for the network not requiring Layer 2 mutual access to decrease network attacks and multicast packet bandwidth usage.
Configuring the Rate Limit for Wireless Users	Makes full use of network resources.
Improving the Anti-Interference Capability	Decreases the RTS threshold appropriately to improve the anti-interference capability when there is co-channel interference.
Improving the Capability of Competing for Channels	Adjusts of EDCA parameters on the STA or AP as needed to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.
Reducing Weak-Signal STAs	Limits the number of wireless access users to control the network coverage of the AP and improve the transmission quality of wireless signals.
Configuring the Maximum Number of STAs Connected to an AP	Limits the STA number on the AP to implement load balancing, avoiding uneven distribution of connected STAs.
Establishing a Pure 802.11n Network	Configures a pure 802.11n network to prohibit access of non-802.11n devices so that all the 802.11n devices to use pure HT header for transmission. This reduces the size of the packet header and increases the available channel bandwidth for wireless users.
Spectrum Navigation	Guides access of the dual-band STA to the 5G frequency band that has stronger access capacity by means of band selection to reduce the pressure of the 2.4G frequency band, thereby improving user experience.
One-Click Network Optimization	Is required to address the following issues on a wireless network that has been running for a period of time: ● The network speed is slow. ● Signal or interference problems exist. ● The authentication page cannot be displayed. ● STAs equipped with 2.4 GHz/5 GHz network adapters are usually associated the network at the 2.4 GHz band. ● A large number of low-rate packets exist. ● Multicast packets are lost or retransmitted.
Intelligent Network Optimization	Performs wireless network optimization intelligently based on real-time network running.
Mcell Configuration	Enables dense deployment optimization.
Roaming Stickiness	Determines whether a STA is associated with the AP with the optimal signal quality based on STA detection information. If the AC detects that a STA associates with an AP with poor signal quality, a notification is reported to the WIS client. Based on collected remote association information, the WIS client performs coverage optimization for APs.

Feature	Description
Remote Association Information Collection	Determines whether a STA is associated with the AP with the optimal signal quality based on STA detection information. If the AC detects that a STA associates with an AP with poor signal quality, a notification is reported to the WIS client. Based on collected remote association information, the WIS client performs coverage optimization for APs.
Automatic Device Information Upload	Configures automatic upload of software and hardware version numbers of the AC and AP.

1.3.1 Terminating Low-Rate Applications

Working Principle

Terminate low-rate applications by configuring the rate set.

1.3.2 Increasing the Beacon Frame Period Appropriately

Working Principle

Increase the Beacon frame period; reduce the frequency of sending Beacon frames; reduce the channel usage for packet management; increase the available channel bandwidth for wireless users.

1.3.3 Configuring Layer 2 Isolation of Wireless Users in a VLAN

Working Principle

Configure this function for the network not requiring Layer 2 mutual access to reduce network attacks and multicast packet bandwidth usage.

1.3.4 Configuring the Rate Limit for Wireless Users

Working Principle

To make full use of network resources, ensure that the device supports the traffic rate limit function. When data traffic accords with the committed rate, data packets are allowed to pass. When data traffic does not accord with the committed rate, data packets are discarded.

1.3.5 Improving the Anti-Interference Capability

Working Principle

To avoid data transmission failures caused by conflicts between channels, the IEEE 802.11 MAC protocol provides a Request to Send/Clear to Send (RTS/CTS) handshake protocol, that is, requests to send/allow sending protocol. The following description assumes that workstation A needs to send data to workstation B. First of all, workstation A sends a RTS request frame. If workstation B allows workstation A to send the request frame, workstation B replies a CTS permission frame. After receiving this permission frame, workstation A begins to sending data. If multiple workstations send RTS requests to the same workstation, only the workstations receiving CTS are allowed to send data. For the workstation not receiving CTS, it is regarded that channel conflict occurs. In this case, this workstation waits for a given period of time and sends an RTS request again.

If RTS/CTS handshake needs to be performed when a workstation sends data each time, excessive RTS frames will occupy much channel bandwidth. You can set the RTS threshold to specify the length of the data frame to be sent. RTS/CTS handshake is not performed when a workstation sends a data frame with a length smaller than the RTS threshold.

1.3.6 Improving the Capability of Competing for Channels

Working Principle

EDCA parameters differentiate access capabilities of channels with different priorities. Each AC has its own EDCA channel competition parameters. You can adjust values of EDCA parameters on the STA or AP as needed to make the AC with a higher priority to start the backoff process earlier than other ACs and preferentially access the channel.

In real-world applications, you can choose to configure EDCA parameters on the STA or AP based on application requirements. Configuring EDCA parameters on the STA and AP affects downlink and uplink data traffic respectively.

1.3.7 Reducing Weak-Signal STAs

Working Principle

STAs search for the AP in proactive or passive scanning mode:

- Proactive scanning: A STA sends a Probe Request for accessing the AP. After confirming the request frame, the AP returns a Probe Response frame.
- Passive scanning: The AP periodically broadcasts Beacon frames. A STA attempts to connect to the AP after listening Beacon frames.

To control the network coverage of the AP and improve the transmission quality of wireless signals, limit the number of STAs. You can control the Beacon frame broadcast coverage of the AP to prevent access of remote STAs. You can also limit the minimum value of the RSSI for STAs. When the RSSI of the request frame sent from a STA is smaller than the minimum value, access of the STA is not allowed.

1.3.8 Configuring the Maximum Number of STAs Connected to an AP

↘ Working Principle

On a WLAN, one AP allows access of multiple wireless users, and an administrator can specify the maximum number of wireless users. The number of STAs connected to the AP can be limited to implement load balancing, avoiding uneven distribution of AP access users.

1.3.9 Establishing a Pure 802.11n Network

↘ Working Principle

Configure a pure 802.11n network to prohibit access of non-802.11n devices; make all the 802.11n devices of the network to use pure HT header for transmission; reduce the size of the packet header; increase the available channel bandwidth for wireless users.

1.3.10 Spectrum Navigation

Working Principle

IEEE802.11 mainly has three communication frequency bands:

- 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.

1.3.11 One-Click Network Optimization

Working Principle

One-click network optimization is required to address the following issues on a wireless network that has been running for a period of time:

- The network speed is slow.
- Signal or interference problems exist.
- The authentication page cannot be displayed.
- STAs equipped with 2.4 GHz/5 GHz network adapters are usually associated the network at the 2.4 GHz band.
- A large number of low-rate packets exist.
- Multicast packets are lost or retransmitted.

1. The network speed is slow.

The possible causes are as follows:

- No rate limit is configured. Some users occupy large bandwidth for downloading or playing videos. As a result, the network speed of other users is slow.
- A rate limit is configured but the rate is high, without achieving the rate limit effect.
- A rate limit is configured but the rate is low, resulting in slow network speed.
- The rate limit solution can be used. Rate limiting is performed for all STAs by WLAN to ensure that the average uplink or downlink rate is 256 kbit/s and the burst traffic rate is 300 kbit/s.

2. Signal or interference problems exist.

For example, the signal is poor, roaming frequently occurs, or intra-frequency or inter-frequency interference occurs. To address this issue, use the RRM function. After the RRM function is enabled, channel or power adjustment is performed for online APs or new APs to ensure signal coverage and channel different from those of neighboring APs. If the poor signal or intra-frequency/inter-frequency interference problem does not exist, disable the RRM function to improve the device performance.

3. The authentication page cannot be displayed.

This is because few sessions are configured. Restore the default number of sessions to ensure that each STA supports 255 sessions and each interface supports 1000 sessions by default.

4. STAs equipped with 2.4 GHz/5 GHz network adapters are usually associated the network at the 2.4 GHz band.

For this problem, band steering can be used. If only few 5 GHz/6 GHz-capable clients exist in the environment, it is recommended that band steering be disabled.

5. A large number of low-rate packets exist.

The low-rate packet forbidding function can be used to forbid packets complying with 802.11b, 802.11g, or 802.11a and with a rate lower than 11 Mbps.

6. Multicast packets are lost or retransmitted.

This is because a high multicast rate is set. To solve this problem, restore the default multicast rate to ensure user experience.

1.3.12 Intelligent Network Optimization

Perform wireless network optimization intelligently.

Working Principle

Perform wireless network optimization intelligently based on real-time network running.

1.3.13 Mcell Configuration

Enable dense deployment optimization.

Working Principle

Enable dense deployment optimization.

1.3.14 Roaming Stickiness

Working Principle

Monitor STAs with low RSSI and poor user experience on the entire wireless network in real time and determine whether more suitable APs exist for STAs to access the network based on STA detection information collected by each AP. If such STAs with sticky roaming exist, the AP sends a deauthentication frame to disassociate with the terminal to ensure that the STA is associated with an AP with better signal quality.

1.3.15 Remote Association Information Collection

Working Principle

Determine whether a STA is associated with the AP with the optimal signal quality based on STA detection information. If the AC detects that a STA associates with an AP with poor signal quality, a notification is reported to the WIS client. Based on collected remote association information, the WIS client performs coverage optimization for APs.

1.3.16 Automatic Device Information Upload

Working Principle

Configure automatic upload of software and hardware version numbers of the AC and AP.

1.4 Configuration

Configuration Item	Configuration Suggestion & Relevant Command	
Configuring the Rate Set	(Optional) It is used to terminate low-rate applications.	
	802.11a network rate	Configures the 802.11a rate set.
	802.11b network rate	Configures the 802.11b rate set.
	802.11g network rate	Configures the 802.11g rate set.
Configuring the Beacon Frame Period	(Optional) It is used to increase the Beacon frame period.	
	beacon period	Configures the Beacon frame period.
Configuring Layer 2 Isolation of Wireless Users in a VLAN	(Optional) It is used to enable Layer 2 isolation of wireless users in a VLAN.	
	user-isolation ssid_ap enable	Configures WLAN-based user isolation for an AP.
	user-isolation ap enable	Configures user isolation for an AP.
	user-isolation ssid_ac enable	Configures WLAN-based user isolation for an AC.
	user-isolation ac enable	Configures user isolation for an AC.
Configuring the Rate Limit for Wireless Users	(Optional) It is used to configure rate limit for wireless users.	
	ap-based	Configures AP-based rate limit.
	netuser	Configures STA-based rate limit.
	wlan-based	Configures WLAN-based rate limit.
Configuring the RTS/CTS Protection Mechanism	(Optional) It is used to configure the RTS/CTS protection mechanism.	
	rts-threshold	Configures the RTS threshold.
Configuring EDCA Parameters	(Optional) It is used to configure EDCA parameters.	
	wmm edca-client	Configures EDCA parameters on the STA.
	wmm edca-radio	Configures EDCA parameters on the AP.
Configuring the Allowed Access Signal Strength	(Optional) It is used to configure the allowed access signal strength.	
	response-rssi	Configures the minimum RSSI for wireless user access.
	coverage-area-control	Configures the management frame transmit power.
Configuring the Maximum Number of STAs Connected to an AP	(Optional) It is used to configure the maximum number of STAs connected to the AP.	
	sta-limit	Configures the maximum number of STAs connected to the AP.
Configuring a Pure 802.11n Network	(Optional) It is used to configure a pure 802.11n network.	
	11asupport	Configures whether to support 802.11a or not.

Configuration Item	Configuration Suggestion & Relevant Command	
	11bsupport	Configures whether to support 802.11b or not.
	11gsupport	Configures whether to support 802.11g or not.
	11nasupport	Configures whether to support 802.11na or not.
	11ngsupport	Configures whether to support 802.11ng or not.
Configuring Spectrum Navigation	⚠ (Mandatory) It is used to enable the spectrum navigation function of the WLAN.	
	band-select enable	Enables the spectrum navigation function.
	⚠ (Optional) It is used to configure the operating parameters of the spectrum navigation function.	
	band-select acceptable-rssi	Configures the lower limit of STA signal strength accepted by spectrum navigation.
	band-select access-denial	Configures the number of times for which dual-band STA access to 2.4G band is denied.
	band-select age-out	Configures the STA information aging time.
	band-select probe-count	Configures the detection period count of suppression STA.
	band-select scan-cycle	Configures the threshold of STA detection scanning period.
Configuring One-Click Network Optimization	⚠ (Optional) It is used to configure network optimization options.	
	wopt choose	Configures network optimization options.
	⚠ (Optional) It is used to configure one-click network optimization.	
	wopt enable	Configures one-click network optimization.
Configuring Intelligent Network Optimization	⚠ (Optional) It is used to configure network optimization options.	
	wis enable	Enables intelligent network optimization.
Configuring Mcell	⚠ (Optional) It is used to configure network optimization options.	
	mcell enable	Enables dense deployment optimization.
Configuring Roaming Stickiness	⚠ (Optional) It is used to configure network optimization options.	
	sticky-steering monitor-only	Enables roaming stickiness monitoring.
	⚠ (Optional) It is used to configure one-click network optimization.	
	sticky-steering enable	Enables roaming stickiness navigation.
Configuring Automatic Device Information Upload	**wis devinfo enable**	Enables the automatic device information upload function.

1.4.1 Configuring the Rate Set

Configuration Effect

Configure the rate set to terminate low-rate applications; prohibit packet transmission at low rate between the STA and AP; improve the channel usage.

Notes

- If you disable a rate, this rate can no longer be used.
- If you disable all rates, wireless users cannot access the WLAN.
- If you disable all 802.11b rates, 802.11b wireless users cannot access the WLAN.

Configuration Steps

Configuring the 802.11a Rate Set

- Mandatory.
- Unless otherwise specified, the configuration is performed in AC configuration mode on the AC.

Command	**802.11a network rate** { **6** | **9** | **12** | **18** | **24** | **36** | **48** | **54** } { **disable** | **mandatory** | **supported** }
Parameter Description	**6**: The rate is 6 Mbps. **9**: The rate is 9 Mbps. **12**: The rate is 12 Mbps. **18**: The rate is 18 Mbps. **24**: The rate is 24 Mbps. **36**: The rate is 36 Mbps. **48**: The rate is 48 Mbps. **54**: The rate is 54 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command Mode	AC configuration mode
Defaults	The rates of 6 Mbps, 12 Mbps, and 24 Mbps are mandatory, and the rates of 9 Mbps, 18 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps are optional.
Usage Guide	N/A

Configuring the 11b Rate Set

- Optional.
- Unless otherwise specified, the configuration is performed in AC configuration mode on the AC.

Command	**802.11b network rate** { **1** | **2** | **5** | **11** } { **disable** | **mandatory** | **supported** }
Parameter Description	**1**: The rate is 1 Mbps. **2**: The rate is 2 Mbps. **5**: The rate is 5.5 Mbps. **11**: The rate is 11 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command	AC configuration mode

Mode	
Defaults	By default, the rates of 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps are mandatory.
Usage Guide	N/A

Configuring the 11g Rate Set

- Optional.
- Unless otherwise specified, the configuration is performed in AC configuration mode on the AC.

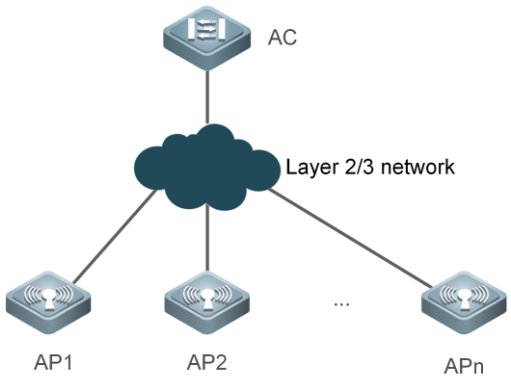
Command	**802.11g network rate** { **1** | **2** | **5** | **6** | **9** | **11** | **12** | **18** | **24** | **36** | **48** | **54** } { **disable** | **mandatory** | **supported** }
Parameter Description	**1**: The rate is 1 Mbps. **2**: The rate is 2 Mbps. **5**: The rate is 5.5 Mbps. **6**: The rate is 6 Mbps. **9**: The rate is 9 Mbps. **11**: The rate is 11 Mbps. **12**: The rate is 12 Mbps. **18**: The rate is 18 Mbps. **24**: The rate is 24 Mbps. **36**: The rate is 36 Mbps. **48**: The rate is 48 Mbps. **54**: The rate is 54 Mbps. **disable**: Disables the rate. **mandatory**: Specifies the mandatory rate. **supported**: Specifies the supported rate.
Command Mode	AC configuration mode
Defaults	The rates of 1 Mbps, 2 Mbps, 5.5 Mbps, and 11 Mbps are mandatory, and the rates of 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps are optional.
Usage Guide	N/A

Verification

- You can run the **show running-config** command to display the configuration of the rate set.

Configuration Examples

Configuring the Rate Set

Scenario **Figure 1-3**	
Configuration Steps	● Disable the 6 Mbps rate for 802.11a users on the AC. ● Disable the 1 Mbps and 2 Mbps rates for the 802.11b users on the AC. ● Disable the 1 Mbps, 2 Mbps, and 5.5 Mbps rates for 802.11g users on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ac-controller`
	`Hostname(config-ac)# 802.11a network rate 6 disabled`
	`Hostname(config-ac)# 802.11b network rate 1 disabled`
	`Hostname(config-ac)# 802.11b network rate 2 disabled`
	`Hostname(config-ac)# 802.11g network rate 1 disabled`
	`Hostname(config-ac)# 802.11g network rate 2 disabled`
	`Hostname(config-ac)# 802.11g network rate 5 disabled`

Verification	After configuring the rate set, you can display the configuration of the rate set. ● You can run the **show running** command to display the configuration of the rate set.

	`Hostname# show running`
	`!`
	`ac-controller`
	` country CN`
	` country US`
	` 802.11g network rate 1 disabled`
	` 802.11g network rate 2 disabled`
	` 802.11g network rate 5 disabled`
	` 802.11g network rate 11 mandatory`
	` 802.11g network rate 6 supported`
	` 802.11g network rate 9 supported`
	` 802.11g network rate 12 supported`
	` 802.11g network rate 18 supported`
	` 802.11g network rate 24 supported`
	` 802.11g network rate 36 supported`
	` 802.11g network rate 48 supported`
	` 802.11g network rate 54 supported`
	` 802.11b network rate 1 disabled`
	` 802.11b network rate 2 disabled`

```
 802.11b network rate 5 mandatory
 802.11b network rate 11 mandatory
 802.11a network rate 6 disabled
 802.11a network rate 9 supported
 802.11a network rate 12 mandatory
 802.11a network rate 18 supported
 802.11a network rate 24 mandatory
 802.11a network rate 36 supported
 802.11a network rate 48 supported
 802.11a network rate 54 supported
!
```

Common Errors

None.

1.4.2 Configuring the Beacon Frame Period

Configuration Effect

Increase the Beacon frame period; reduce the frequency of sending Beacon frames; reduce the channel usage for packet management; increase the available channel bandwidth for wireless users.

Notes

If a long Beacon frame period is used, users may be disconnected from the WLAN or detect the WLAN frequently.

Configuration Steps

↘ Configuring the Beacon Frame Period

- Optional.
- Unless otherwise specified, the configuration is performed in AP configuration mode on the AC.

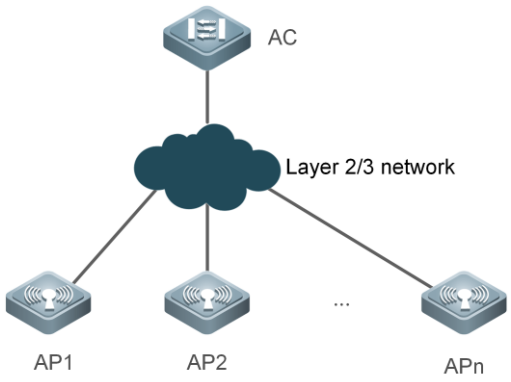
Command	**beacon period** *milliseconds* **radio** *radio-id*
Parameter Description	*milliseconds*: Specifies the Beacon frame period, in milliseconds. The value range is from 20 to 1,000. *radio-id*: Specifies the RF interface index. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	The Beacon frame period is 100 milliseconds.
Usage Guide	The configuration for all APs is not supported.

Verification

You can run the **show ap-config running** command to display the configuration of the Beacon frame period.

Configuration Examples

↘ Configuring the Beacon Frame Period

Scenario **Figure 1-4**	
Configuration Steps	Set the Beacon frame period of radio 1 of AP1 to 300 milliseconds on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# beacon period 300 radio 1`

Verification	● After configuring the Beacon frame period, you can display the configuration of the Beacon frame period. ● You can run the **show ap-config running** command to display the configuration of the Beacon frame period.

	`Hostname# show ap-config running AP1`
	`!`
	`ap-config AP1`
	` no 11acsupport enable radio 1`
	` no 11acsupport enable radio 2`
	` 802.11n mcs support 15 radio 1`
	` 802.11n mcs support 15 radio 2`
	` antenna receive 3 radio 1`
	` antenna receive 3 radio 2`
	` antenna transmit 3 radio 1`
	` antenna transmit 3 radio 2`
	` radio-type 1 802.11b`
	` radio-type 2 802.11a`
	` beacon period 300 radio 1`
	` beacon period 100 radio 2`
	` ap-mac 001a.a9c5.3f49`
	` no enable-radio 1`
	` no enable-radio 2`
	`!`

Common Errors

None.

1.4.3 Configuring Layer 2 Isolation of Wireless Users in a VLAN

Configuration Effect

Configure this function for the network not requiring Layer 2 mutual access to decrease network attacks and multicast packet bandwidth usage.

Notes

None.

Configuration Steps

Configuring WLAN-Based User Isolation for an AP

- Optional. Unless otherwise specified, the configuration is performed in WIDS configuration mode on the AC.

Command	**user-isolation ssid-ap enable**
Parameter Description	N/A
Defaults	WLAN-based user isolation on the AP is disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring User Isolation for an AP

Optional. Unless otherwise specified, the configuration is performed in WIDS configuration mode on the AC.

Command	**user-isolation ap enable**
Parameter Description	*N/A*
Defaults	User isolation on the AP is disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring WLAN-Based User Isolation for an AC

- Optional configuration. By default, WLAN-based user isolation is disabled for the AC.
- Unless otherwise specified, the configuration shall be performed in WIDS configuration mode on the AC device.

Command	**user-isolation ssid-ac enable**
Parameter Description	N/A
Defaults	WLAN-based user isolation on the AC is disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Configuring User Isolation for an AC

Optional. Unless otherwise specified, the configuration is performed in WIDS configuration mode on the AC.

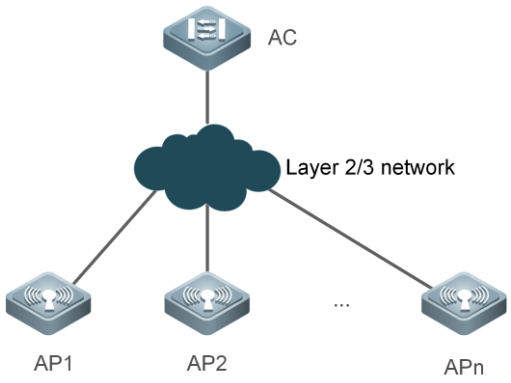
Command	user-isolation ac enable
Parameter Description	*N/A*
Defaults	User isolation on the AC is disabled.
Command Mode	WIDS configuration mode
Usage Guide	N/A

Verification

You can run the **show running-config** command to display the configuration of Layer 2 isolation of wireless users in a VLAN.

Configuration Examples

Configuring Layer 2 Isolation of Wireless Users in a VLAN

Scenario Figure 1-5	
Configuration Steps	● Enable WLAN-based user isolation for an AP on the AC. ● Enable user isolation for an AP on the AC. ● Enable WLAN-based user isolation for an AC on the AC. ● Enable user isolation for an AC on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# wids`
	`Hostname(config-wids)# user-isolation ssid-ap enable`
	`Hostname(config-wids)# user-isolation ap enable`
	`Hostname(config-wids)# user-isolation ssid-ac enable`
	`Hostname(config-wids)# user-isolation ac enable`

Verification	● After configuring Layer 2 isolation of wireless users in a VLAN, you can display the configuration on Layer 2 isolation of wireless users in a VLAN. ● You can run the **show running-config** command to display the configuration on Layer 2 isolation of wireless users in a VLAN.
	`Hostname# show running-config` `!`

	wids user-isolation ap enable user-isolation ac enable user-isolation ssid-ac enable user-isolation ssid-ap enable !

1.4.4 Configuring the Rate Limit for Wireless Users

Configuration Effect

To make full use of network resources, ensure that the device supports the traffic rate limit function. When data traffic accords with the committed rate, data packets are allowed to pass. When data traffic does not accord with the committed rate, data packets are discarded.

Notes

When data traffic does not accord with the committed rate, data packets are discarded.

Configuration Steps

Configuring AP-Based Rate Limit

- Optional.
- Unless otherwise specified, the configuration is performed in AP configuration mode on the AC.

Command	**ap-based { per-user-limit | total-user-limit } { up-streams | down-streams } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Limits the rates of all users on the AP. **total-user-limit**: Limits the rate of the AP. **up-streams**: Limits the rate of uplink traffic. **down-streams**: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the unit of 8 kbps. The value range is from 8 to 261120. *burst-data-rate*: Specifies the burst rate limit, in the unit of 8 kbps. The value range is from 8 to 261120.
Command Mode	AP configuration mode
Defaults	AP-based rate limit is disabled.
Usage Guide	N/A

Configuring STA-Based Rate Limit

Optional. Unless otherwise specified, the configuration is performed in AC configuration mode on the AC.

Command	**netuser** *mac-address* **{ inbound | outbound } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	*mac-address*: Specifies the MAC address of a STA. **inbound**: Limits the rate of uplink traffic.

	outbound: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the unit of 8 kbps. The value range is from 8 to 261120. *burst-data-rate*: Specifies the burst rate limit, in the unit of 8 kbps. The value range is from 8 to 261120.
Command Mode	AC configuration mode
Defaults	STA-based rate limit is disabled.
Usage Guide	N/A

Configuring WLAN-Based Rate Limit

- Optional.
- Unless otherwise specified, the configuration is performed in WLAN configuration mode on the AC.

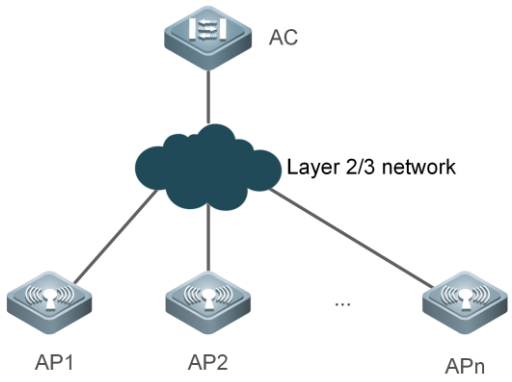
Command	**wlan-based { per-user-limit | total-user-limit | per-ap-limit } { up-streams | down-streams } average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate*
Parameter Description	**per-user-limit**: Limits the rates of all users on the WLAN. **total-user-limit**: Limits the rate of the WLAN. **per-ap-limit**: Limits the rate of the WLAN for each AP separately. **up-streams**: Limits the rate of uplink traffic. **down-streams**: Limits the rate of downlink traffic. *average-data-rate*: Specifies the average rate limit, in the unit of 8 kbps. The value range is from 8 to 261120. *burst-data-rate*: Specifies the burst rate limit, in the unit of 8 kbps. The value range is from 8 to 261120.
Command Mode	WLAN configuration mode
Defaults	WLAN-based rate limit is disabled.
Usage Guide	N/A

Verification

You can run the **show running-config** command to display the configuration of the rate limit for wireless users.

Configuration Examples

Configuring Rate Limit for Wireless Users

Scenario **Figure 1-6**	
Configuration Steps	● Limit the maximum uplink average rate and maximum uplink burst rate of each user on AP1 to 256*8 kbps and 1024*8 kbps respectively on the AC. ● Limit the maximum uplink average rate and maximum uplink burst rate of wireless user 14cf.920b.bfce on the AC to 256* 8 kbps and 1024*8 kbps respectively on the AC. ● Limit the maximum uplink average rate and maximum uplink burst rate of each user in WLAN 12 to 256*8 kbps and 1024*8 kbps respectively on the AC.
	Hostname# configure terminal Hostname(config)# ap-config AP1 Hostname(config-ap)# ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 Hostname(config-ap)# end Hostname#configure terminal Hostname(config)# ac-controller Hostname(config-ac)# netuser 14cf.920b.bfce inbound average-data-rate 256 burst-data-rate 1024 Hostname(config-ap)# end Hostname# configure terminal Hostname(config)# wlan-config 12 Hostname(config-wlan)# wlan-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024
Verification	● After configuring the rate limit for wireless users, you can display the configuration of the rate limit for wireless users. ● You can run the **show running-config** command to display the configuration of the rate limit for wireless users.
	Hostname# show ap-config running AP1 ! ap-config AP1 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024 no 11acsupport enable radio 1 no 11acsupport enable radio 2 802.11n mcs support 15 radio 1

```
 802.11n mcs support 15 radio 2
 antenna receive 3 radio 1
 antenna receive 3 radio 2
 antenna transmit 3 radio 1
 antenna transmit 3 radio 2
 radio-type 1 802.11b
 radio-type 2 802.11a
 beacon period 300 radio 1
 beacon period 100 radio 2
 ap-mac 001a.a9c5.3f49
 no enable-radio 1
 no enable-radio 2
!
Hostname#show running
!
wlan-config 12 wlan_opt
 wlan-based per-user-limit up-streams average-data-rate 256 burst-data-rate
1024
 enable-broad-ssid
!
!
ac-controller
 netuser 14cf.920b.bfce inbound average-data-rate 256 burst-data-rate 1024
 country CN
 country US
 802.11g network rate 1 disabled
 802.11g network rate 2 disabled
 802.11g network rate 5 disabled
 802.11g network rate 11 mandatory
 802.11g network rate 6 supported
 802.11g network rate 9 supported
 802.11g network rate 12 supported
 802.11g network rate 18 supported
 802.11g network rate 24 supported
 802.11g network rate 36 supported
 802.11g network rate 48 supported
 802.11g network rate 54 supported
 802.11b network rate 1 disabled
 802.11b network rate 2 disabled
 802.11b network rate 5 mandatory
 802.11b network rate 11 mandatory
 802.11a network rate 6 disabled
 802.11a network rate 9 supported
 802.11a network rate 12 mandatory
```

	802.11a network rate 18 supported 802.11a network rate 24 mandatory 802.11a network rate 36 supported 802.11a network rate 48 supported 802.11a network rate 54 supported !

Common Errors

None.

1.4.5 Configuring the RTS/CTS Protection Mechanism

Configuration Effect

When co-channel interference exists, a smaller RTS threshold means a higher anti-interference capability. However, more RTS/CTS packets require higher channel usage for packet control, reducing the available channel bandwidth for wireless users. You can set the RTS threshold to specify the length of the data frame to be sent. RTS/CTS handshake is not performed when a workstation sends a data frame with the length smaller than the RTS threshold.

Notes

None.

Configuration Steps

↘ Configuring the RTS Threshold

Optional. Unless otherwise specified, the configuration is performed in AP configuration mode on the AC.

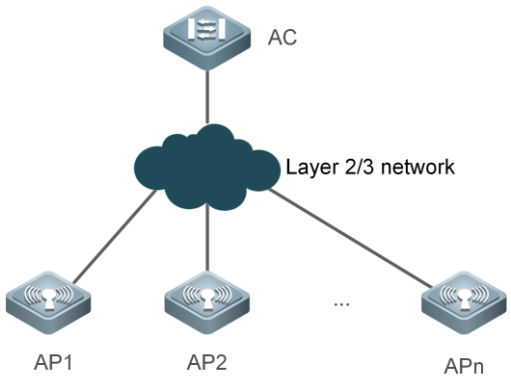
Command	**rts-threshold** *value* **radio** *radio-id*
Parameter Description	*value*: Specifies the RTS threshold, in bytes. The value range is from 257 to 2347. *radio-id*: Specifies the RF interface index. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	The RTS threshold is 2347 bytes.
Usage Guide	N/A

Verification

You can run the **show ap-config running** command to display the configuration of the RTS threshold.

Configuration Examples

↘ Configuring the RTS Threshold

Scenario **Figure 1-7**	
Configuration Steps	Set the RTS threshold of Radio1 on AP1 to 800 bytes on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# rts-threshold 800 radio 1`

Verification	● After configuring the RTS threshold, you can display the configuration of the RTS threshold. ● You can run the **show ap-config running** command to display the configuration of the RTS threshold.

	`Hostname# show ap-config running AP1`
	`!`
	`ap-config AP1`
	` ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024`
	` no 11acsupport enable radio 1`
	` no 11acsupport enable radio 2`
	` 802.11n mcs support 15 radio 1`
	` 802.11n mcs support 15 radio 2`
	` rts-threshold 800 radio 1`
	` antenna receive 3 radio 1`
	` antenna receive 3 radio 2`
	` antenna transmit 3 radio 1`
	` antenna transmit 3 radio 2`
	` radio-type 1 802.11b`
	` radio-type 2 802.11a`
	` beacon period 300 radio 1`
	` beacon period 100 radio 2`
	` ap-mac 001a.a9c5.3f49`
	` no enable-radio 1`
	` no enable-radio 2`
	`!`

Common Errors

None.

1.4.6 Configuring EDCA Parameters

Configuration Effect

In real-world situations, you can choose to configure EDCA parameters on a STA or an AP as needed. EDCA parameters on the STA and AP respectively affect downlink data traffic and uplink data traffic.

Notes

None.

Configuration Steps

Configuring EDCA Parameters on a STA

- Optional.
- Unless otherwise specified, the configuration is performed in AP configuration mode on the AC.

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*] } **radio** [*radio-id*]
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort (BE) queue. **video**: Sets the video queue. **voice**: Sets the voice queue. *aifsn-value*: Sets the AIFSN value. The value range is from 1 to 15. *cwmin-value*: Sets the CWmin value. The value range is from 0 to 15. *cwmax-value*: Sets the CWmax value. The value range is from 0 to 15. *txop-value*: Sets the TXOP value. The value range is from 0 to 255, in the unit of 32 microseconds. *queue-length*: Sets the AC queue length. The value range is from 1 to 255. The default is 255. *radio-id*: Sets the ID of a radio on the STA. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	
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 message indicating a configuration failure is displayed.

AC	AIFSN	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

Configuring the EDCA Parameters on an AP

- Optional.
- Unless otherwise specified, the configuration is performed in AP configuration mode on the AC.

Command	**wmm edca-radio** { **back-ground** | **best-effort** | **video** | **voice** } { **aifsn** [*aifsn-value*] **cwmin**

	[*cwmin-value*] **cwmax** [*cwmax-value*] **txop** [*txop-value*] | **noack** } **radio** [*radio-id*]
Parameter Description	**back-ground**: Sets the back-ground queue. **best-effort**: Sets the best-effort queue. **video**: Sets the video queue. **voice**: Sets the voice queue. *aifsn-value*: Sets the AIFSN value. The value range is from 1 to 15. *cwmin-value*: Sets the CWmin value. The value range is from 0 to 15. *cwmax-value*: Sets the CWmax value. The value range is from 0 to 15. *txop-value*: Sets the TXOP value. The value range is from 0 to 255, in the unit of 32 microseconds. **noack**: Enables the no ack policy. The no ack policy is not enabled by default. *radio-id*: Sets the ID of a radio on the STA. The value range is from 1 to 48.
Command Mode	AP configuration mode
Defaults	
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 message indicating a configuration failure is displayed.

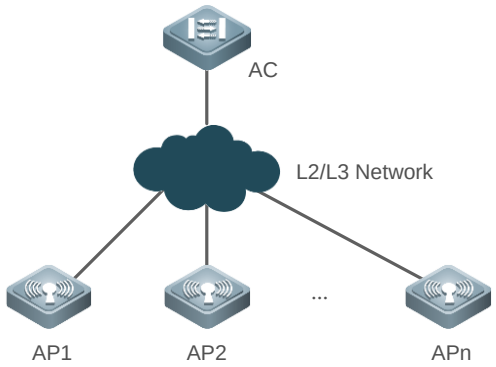
AC	AIFSN	CWmin	CWmax	TXOP
back-ground	7	4	10	0
best-effort	3	4	6	0
video	1	3	4	94
voice	1	2	3	47

Verification

You can run the **show ap-config running** command to display the configuration of EDCA parameters.

Configuration Examples

Configuring EDCA Parameters

Scenario **Figure 1-8**	
Configuration Steps	● Configure EDCA parameters of the STA for Radio1 of AP1 on the AC. ● Configure EDCA parameters of the AP for Radio1 of AP1 on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1`

	`Hostname(config-ap)# wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1`
Verification	● After configuring EDCA parameters, you can display the configuration of EDCA parameters. ● You can run the **show ap-config running** command to display the configuration of EDCA parameters.

	`Hostname# show ap-config running AP1`
	`!`
	`ap-config AP1`
	` wmm edca-client voice aifsn 2 cwmin 2 cwmax 3 txop 50 radio 1`
	` wmm edca-radio voice aifsn 1 cwmin 1 cwmax 3 txop 50 radio 1`
	` no 11acsupport enable radio 1`
	` no 11acsupport enable radio 2`
	` 802.11n mcs support 15 radio 1`
	` 802.11n mcs support 15 radio 2`
	` antenna receive 3 radio 1`
	` antenna receive 3 radio 2`
	` antenna transmit 3 radio 1`
	` antenna transmit 3 radio 2`
	` radio-type 1 802.11b`
	` radio-type 2 802.11a`
	` beacon period 300 radio 1`
	` beacon period 100 radio 2`
	` ap-mac 001a.a9c5.3f49`
	` no enable-radio 1`
	` no enable-radio 2`
	`!`

Common Errors

None.

1.4.7 Configuring the Allowed Access Signal Strength

Configuration Effect

You can control the Beacon frame broadcast coverage of an AP to prevent access of remote wireless users. You can also limit the minimum value of the RSSI for wireless users. When the RSSI of the request frame sent from a wireless user is smaller than the minimum value, access of the wireless user is prohibited.

Notes

- If a large value of the minimum RSSI for wireless user access is used, many wireless users may fail to access the WLAN.
- If a large management frame transmit power is used, many remote wireless users may fail to discover the network.

Configuration Steps

Configuring the Minimum RSSI for Wireless User Access

- Optional.
- Unless otherwise specified, the configuration is performed in AP configuration mode on the AC.

Command	**response-rssi** *rssi* **radio** *radio-id*
Parameter Description	*rssi*: Specifies the minimum RSSI for wireless user access. The value range is from 0 to 100, in dB. *radio-id*: Specifies the ID of a radio to be configured. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	The default RSSI is 0. That is, all users are allowed to access the WLAN regardless of the RSSI.
Usage Guide	N/A

Configuring the Management Frame Transmit Power

- Optional.
- Unless otherwise specified, the configuration is performed in AP configuration mode on the AC.

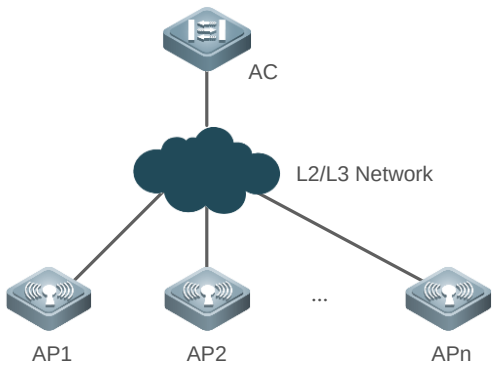
Command	**coverage-area-control** *power* **radio** *radio-id*
Parameter Description	*power*: Specifies the management frame transmit power. The value range is from 0 to 32, in dBm. *radio-id*: Specifies the ID of a radio to be configured. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	The default power is 0. That is, the management frame transmit power is not configured.
Usage Guide	N/A

Verification

You can run the **show ap-config running** command to display the configuration of the allowed access signal strength.

Configuration Examples

Configuring the Allowed Access Signal Strength

Scenario **Figure 1-9**	
Verification	● Set the minimum RSSI for wireless user access of Radio1 on AP1 to 20 dB on the AC. ● Set the management frame transmit power of Radio1 on AP1 to 30 dBm on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# response-rssi 20 radio 1`
	`Hostname(config-ap)# coverage-area-control 30`

Configuration Steps	● After configuring the allowed access signal strength, you can display the configuration of the allowed access signal strength. ● You can run the **show ap-config running** command to display the configuration of the allowed access signal strength.

	`Hostname# show ap-config running AP1`
	`!`
	`ap-config AP1`
	` ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024`
	` no 11acsupport enable radio 1`
	` no 11acsupport enable radio 2`
	` 802.11n mcs support 15 radio 1`
	` 802.11n mcs support 15 radio 2`
	` rts-threshold 800 radio 1`
	` coverage-area-control 30`
	` response-rssi 20 radio 1`
	` antenna receive 3 radio 1`
	` antenna receive 3 radio 2`
	` antenna transmit 3 radio 1`
	` antenna transmit 3 radio 2`
	` radio-type 1 802.11b`
	` radio-type 2 802.11a`
	` beacon period 300 radio 1`
	` beacon period 100 radio 2`
	` ap-mac 001a.a9c5.3f49`
	` no enable-radio 1`
	` no enable-radio 2`
	`!`

Common Errors

None.

1.4.8 Configuring the Maximum Number of STAs Connected to an AP

Configuration Effect

Configure the maximum number of STAs connected to an AP to implement load balancing, avoiding uneven distribution of STAs of an AP.

Notes

None.

Configuration Steps

Configuring the Maximum Number of STAs Connected to an AP

- Optional.
- Unless otherwise specified, the configuration is performed in AP configuration mode on the AC.

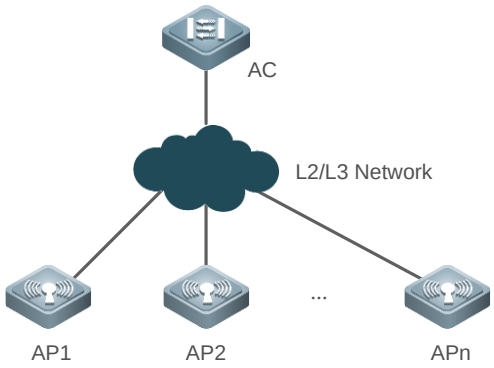
Command	**sta-limit** *client-max-num*
Parameter Description	*client-max-num*: Specifies the maximum number of STAs connected to an AP. The value range is from 1 to 512.
Command Mode	AP configuration mode
Defaults	The default value is 512.
Usage Guide	N/A

Verification

You can run the **show ap-config running** command to display the maximum number of STAs connected to an AP.

Configuration Examples

Configuring the Maximum Number of STAs Connected to an AP

Scenario **Figure 1-10**	
Configuration Steps	● Set the maximum number of STAs connected to AP1 to 12 on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# sta-limit 12`

Verification	● After configuring the maximum number of STAs connected to an AP, you can display the maximum value. ● You can run the **show ap-config running** command to display the maximum number of STAs connected to.
	`Hostname# show ap-config running AP1` `!`

```
ap-config AP1
 ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate
1024
 no 11acsupport enable radio 1
 no 11acsupport enable radio 2
 802.11n mcs support 15 radio 1
 802.11n mcs support 15 radio 2
 rts-threshold 800 radio 1
 coverage-area-control 30
 response-rssi 20 radio 1
 antenna receive 3 radio 1
 antenna receive 3 radio 2
 antenna transmit 3 radio 1
 antenna transmit 3 radio 2
 radio-type 1 802.11b
 radio-type 2 802.11a
 sta-limit 12
 beacon period 300 radio 1
 beacon period 100 radio 2
 ap-mac 001a.a9c5.3f49
 no enable-radio 1
 no enable-radio 2
!
```

Common Errors

None.

1.4.9 Configuring a Pure 802.11n Network

Configuration Effect

Configure a pure 802.1n network to prohibit access of non-802.11n devices; make all the 802.11n devices of the network to use pure HT header for transmission; reduce the size of the packet header; increase the available channel bandwidth for the wireless users.

Notes

Pure 802.11n network does not allow access of non-802.11n devices.

Configuration Steps

↘ Configuring Whether to Support 802.11a or Not

- Optional.
- This configuration takes effect only when the radio of the AP operates at 5 GHz.

Command	**11asupport enable radio** *radio-id*
Parameter	*radio-id*: Specifies the ID of a radio to be configured. The value range is from 1 to 96.

Description	
Command Mode	AP configuration mode
Defaults	802.11a is supported.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 5 GHz. The configuration for all APs is not supported.

Configuring Whether to Support 802.11b or Not

- Optional.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

Command	**11bsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio to be configured. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	802.11b is supported.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. The configuration for all APs is not supported.

Configuring Whether to Support 802.11g or Not

- Optional. By default, access of 11g users at 2.4 GHz is supported.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

Command	**11gsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio to be configured. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	802.11g is supported.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. The configuration for all APs is not supported.

Configuring Whether to Support 802.11na or Not

- Optional.
- This configuration takes effect only when the radio of the AP operates at 5 GHz.

Command	**11nasupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio to be configured. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	802.11n at 5 GHz is supported.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 5 GHz. The configuration for all APs is not supported.

Configuring Whether to Support 802.11ng or Not

- Optional.
- This configuration takes effect only when the radio of the AP operates at 2.4 GHz.

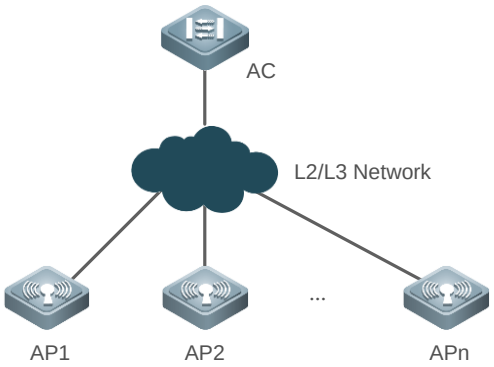
Command	**11ngsupport enable radio** *radio-id*
Parameter Description	*radio-id*: Specifies the ID of a radio to be configured. The value range is from 1 to 96.
Command Mode	AP configuration mode
Defaults	802.11n at 2.4 GHz is supported by default.
Usage Guide	This configuration takes effect only when the radio of the AP operates at 2.4 GHz. The configuration for all APs is not supported.

Verification

You can run the **show ap-config running** command to display the configuration of the pure 802.11n network.

Configuration Examples

Configuring a Pure 802.11n Network

Scenario **Figure 1-11**	 ● Radio1 of AP1 operates at 2.4 GHz. ● Radio2 of AP2 operates at 5.8 GHz.
Configuration Steps	● Configure Radio1 of AP1 as a pure 802.11n network on the AC. ● Configure Radio2 of AP2 as a pure 802.11n network on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# no 11bsupport enable radio 1`
	`Hostname(config-ap)# no 11gsupport enable radio 1`
	`Hostname(config-ap)# 11ngsupport enable radio 1`
	`Hostname(config-ap)# no 11asupport enable radio 2`
	`Hostname(config-ap)# 11nasupport enable radio 2`

Verification	● After configuring a pure 802.11n network, you can display the configuration of the pure 802.11n network.

	• You can run the **show ap-config running** command to display the configuration of the pure 802.11n network.

	`Hostname# show ap-config running AP1`
	`!`
	`ap-config AP1`
	` ap-based per-user-limit up-streams average-data-rate 256 burst-data-rate 1024`
	` no 11asupport enable radio 2`
	` no 11bsupport enable radio 1`
	` no 11gsupport enable radio 1`
	` no 11acsupport enable radio 1`
	` no 11acsupport enable radio 2`
	` 802.11n mcs support 15 radio 1`
	` 802.11n mcs support 15 radio 2`
	` rts-threshold 800 radio 1`
	` coverage-area-control 30`
	` response-rssi 20 radio 1`
	` antenna receive 3 radio 1`
	` antenna receive 3 radio 2`
	` antenna transmit 3 radio 1`
	` antenna transmit 3 radio 2`
	` radio-type 1 802.11b`
	` radio-type 2 802.11a`
	` sta-limit 12`
	` beacon period 300 radio 1`
	` beacon period 100 radio 2`
	` ap-mac 001a.a9c5.3f49`
	` no enable-radio 1`
	` no enable-radio 2`
	`!`

1.4.10 Configuring Spectrum Navigation

Configuration Effect

The spectrum navigation function of the WLAN is enabled, steering the dual-band STA to the 5G frequency band.

Configuration Steps

↘ Enabling the Spectrum Navigation Function of the WLAN

- Mandatory.
- Unless otherwise specified, this configuration is performed on the AC or Fat AP.

Command	**band-select enable**
Parameter Description	N/A

Command Mode	WLAN configuration mode
Defaults	Spectrum navigation is disabled.
Usage Guide	N/A

Configuring the Lower Limit of STA Signal Strength Accepted by Spectrum Navigation

- Optional. This configuration is performed when the spectrum navigation coverage needs to be adjusted.
- Unless otherwise specified, this configuration is performed on the AC.

Command	**band-select acceptable-rssi** *value*
Parameter Description	*value*: Lower limit of STA RSSI accepted by spectrum navigation. The value range is from -100 to -50, in dBm.
Command Mode	Global configuration mode
Defaults	The lower limit of STA RSSI accepted by spectrum navigation is -80 dBm.
Usage Guide	N/A

Configuring the Number of Times for Which the Dual-Band STA's Access to 2.4G Band is Denied

- Optional. This configuration is performed when the dual-band STA's access to 2.4G band needs to be denied. If access of many dual-band STAs lasts for a long time or fails after the configuration, you need to set a lower value or remove the configuration.
- Unless otherwise specified, this configuration is performed on the AC.

Command	**band-select access-denial** *value*
Parameter Description	*value*: Number of times for which the dual-band STA's access to 2.4G band is denied. The value range is from 0 to 10.
Command Mode	Global configuration mode
Defaults	0
Usage Guide	N/A

Configuring the STA Information Aging Time

- Optional. If no dual-band STA switches to a single-band 2.4G STA on a network, you can configure a long aging time. Otherwise, you can configure a short aging time. If you cannot determine whether this type of switching occurs on the network, use the default configuration.
- Unless otherwise specified, this configuration is performed on the AC.

Command	**band-select age-out** { **dual-band** *value* **| suppression** *value* }
Parameter Description	**dual-band** *value*: Aging time of dual-band STA information. The value range is from 20 to 120, in seconds. **suppression** *value*: Aging time of dual-band STA information. The value range is from 10 to 60, in seconds.
Command Mode	Global configuration mode
Defaults	**dual-band** *value:* 60 seconds

	suppression *value:* 20 seconds
Usage Guide	It is recommended that the aging time of dual-band STA information be set to twice to three times the aging time of suppression STA information.

Configuring the Detection Period Count Value of Suppression STA

- Optional. If a single-band 2.4G STA cannot discover the WLAN for a long time, decrease the value.
- Unless otherwise specified, this configuration is performed on the AC.

Command	**band-select probe-count** *value*
Parameter Description	*value*: Detection period count of suppression STA. The value range is from 1 to 10.
Command Mode	Global configuration mode
Defaults	2
Usage Guide	N/A

Configuring the Threshold of STA Detection Scanning Period

- Optional. If a single-band 2.4G STA cannot discover the WLAN for a long time, decrease the value. The default setting is recommended if the network situation is not clear.
- Unless otherwise specified, this configuration is performed on the AC.

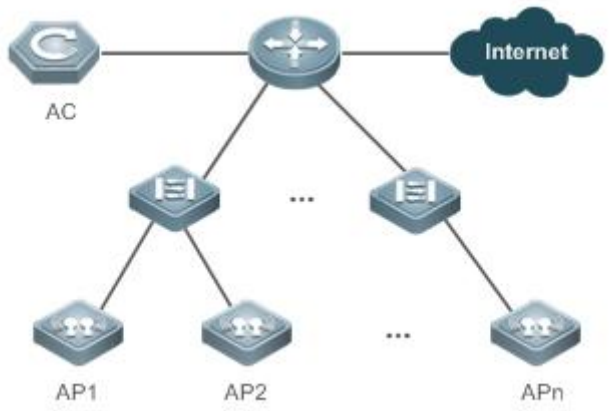
Command	**band-select scan-cycle** *value*
Parameter Description	*value*: Threshold of STA detection scanning period. The value range is from 1 to 1000, in milliseconds.
Command Mode	Global configuration mode
Defaults	200
Usage Guide	N/A

Verification

- Run the **show band-select configuration** command to display the spectrum navigation parameter configuration on the device.
- Run the **show running-config** command to display whether the spectrum navigation function is enabled for the WLAN.
- After the device operates for a period of time, run the **show band-select statistics** command to display the running statistics on the device.
- Obtain packets to check whether spectrum navigation has controlled the active detection process.

Configuration Examples

Configuring WLAN Spectrum Navigation for the Fit AP Architecture

Scenario **Figure 1-12**	 In the typical Fit AP architecture: ● The AC represents a wireless access controller. ● AP1, AP2… and AP*n* are all dual-band APs. ● The AC and APs are connected through the Layer 2 switching device and Layer 3 routing device. ● To configure spectrum navigation WLAN as WLAN 99 with SSID **wlan-bandselect**, map the WLAN to the two RF interfaces to all dual-band APs.
Configuration Steps	● Configure spectrum navigation parameters on the AC (optional). ● Enable the spectrum navigation function of WLAN 99 on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# wlan-config 99`
	`Hostname(config-wlan)# band-select enable`

Verification	Use a dual-band STA to access WLAN **wlan-bandselect**. ● Make the STA access the 5G frequency band. (Navigation may fail, and the STA may access the 2.4G frequency band.) ● Display the running statistics of spectrum navigation on the AC, and verify that the count increases.

AC	`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

- Spectrum navigation parameters are improperly configured.
- The spectrum navigation function is not enabled.

- One of the two RF interfaces of the dual-band AP is disabled.

1.4.11 Configuring One-Click Network Optimization

Configuration Effect

Improve the network performance.

Configuration Steps

Configuring Network Optimization Options

- Optional.
- Enable network optimization on the AC unless otherwise specified.
- Run the **wopt choose** command to configure network optimization options. At least one option is selected.
- Network optimization options can be configured through the network optimization function to improve network performance. You can select network optimization options based on recommended configurations and actual network conditions. The **no** form is not supported to restore the configurations before optimization. Therefore, if the configurations are incorrect, change configurations in corresponding mode.

Command	**wopt choose** { **band-select-disable** | **band-select-enable** | **low-rate-disable** | **multicast-speed** | **rrm-disable** | **rrm-enable** | **session-limit** | **speed-limit** }
Parameter Description	**band-select-disable**: Disables the band steering function. If only few 5 GHz/6 GHz-capable STAs exist in the environment, it is recommended that banding steering be disabled. **band-select-enable**: Enables the band steering function. If a large number of 5 GHz/6 GHz-capable STAs exist in the environment, it is recommended that banding steering be enabled. **low-rate-disable**: Forbids low-rate packets. Packets with a rate lower than 11 Mbps are forbidden. **multicast-speed**: Restores the default multicast rate (24 Mbps). **rrm-disable**: Disables the RRM function. If no intra-frequency or inter-frequency interference exists in the environment, it is recommended that the RRM function be disabled. **rrm-enable**: Enables the RRM function. If intra-frequency or inter-frequency interference exists in the environment, it is recommended that the RRM function be enabled to perform channel or power adjustment. **session-limit**: Restores the default number of sessions. The number of sessions affects the authentication page pushing by iPortal. It is recommended that the default number of sessions be used. The default number of sessions is 255 for each STA and 1000 for each interface. **speed-limit**: Limits the rate. (Rate limiting is performed for all STAs by WLAN. The average uplink and downlink rate is 256 kbit/s and the burst traffic rate is 300 kbit/s.)
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Select network optimization options as required. Restoring to the configurations before network optimization is not supported. Therefore, exercise caution when selecting network optimization options. If incorrect configurations are optimized, change configurations in corresponding configuration mode manually.

Configuring One-Click Network Optimization

- Optional.
- Enable network optimization on the AC unless otherwise specified.
- Run the **wopt enable** command to configure one-click network optimization.
- One-click network optimization can be configured through the network optimization function to improve network performance. The **no** form is not supported to restore the configurations before optimization. Therefore, if the configurations are incorrect, change configurations in corresponding mode.

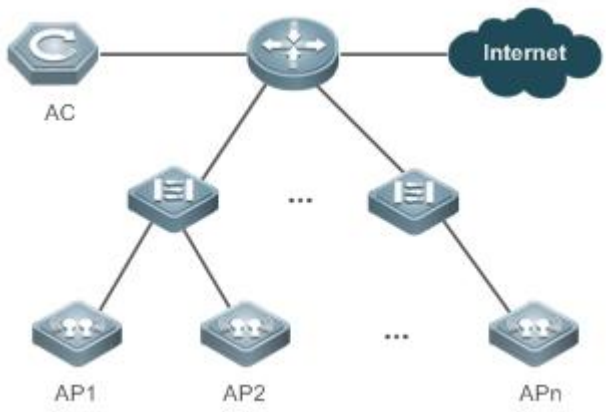
Command	**wopt enable**
Parameter Description	N/A
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	One-click network optimization can be configured if low-rate packets need to be forbidden. Restore default multicast rates for WLANs, restore the default number of sessions, and limit rates for WLANs (average uplink and downlink rate is 256 kbit/s and abrupt rate is 300 kbit/s). Restoring to the configurations before network optimization is not supported. Therefore, exercise caution when configuring one-click network optimization. If incorrect configurations are optimized, change configurations in corresponding configuration mode manually.

Verification

Run the **show wopt** command to display network optimization information.

Configuration Example

Configuring Network Optimization Options in a Fit AP Architecture

Scenario **Figure 1-13**	 In the Fit AP architecture: ● The AC is the wireless network controller. ● AP1, AP2, ….APn are dual-band APs. ● The AC and AP are connected through a Layer 2 switch and a Layer 3 router. ● Many STAs supporting 5 GHz exist. Therefore, it is recommended that the band steering function be enabled, that is, the spectrum navigation function be enabled.

	● Low-rate packets are forbidden.
Configuration Steps	Configure network optimization options on the AC.
AC	`Hostname# configure terminal` `Hostname(config)# wopt choose band-select-enable low-rate-disable`
Verification	● After network optimization options are configured, display network optimization information. ● Run the **show wopt** command to display network optimization information.

AC	`Hostname# show wopt`
	
	`Low rate status:`
	` 802.11b rate:`
	`    1 Mbps: Disable`
	`    2 Mbps: Disable`
	`  5.5 Mbps: Disable`
	`   11 Mbps: Enable`
	` 802.11g rate:`
	`    1 Mbps: Disable`
	`    2 Mbps: Disable`
	`  5.5 Mbps: Disable`
	`    6 Mbps: Disable`
	`    9 Mbps: Disable`
	`   11 Mbps: Enable`
	` 802.11a rate:`
	`    6 Mbps: Disable`
	`    9 Mbps: Disable`
	
	`Multicast rate:`
	`1    24  Mbps`
	`2    24  Mbps`
	`3    24  Mbps`
	`4    24  Mbps`
	`5    24  Mbps`
	`6    24  Mbps`
	`7    24  Mbps`
	`8    24  Mbps`
	`11   24  Mbps`
	`12   24  Mbps`
	`13   24  Mbps`
	`14   24  Mbps`
	`15   24  Mbps`
	`16   24  Mbps`
	`17   24  Mbps`

```
18   24  Mbps
19   24  Mbps
100  24  Mbps
1000 24  Mbps
1048 24  Mbps

Session limit:
 Session limit : 255

wlan 1, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 2, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 3, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 4, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 5, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 6, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 7, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 8, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 11, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.
```

```
wlan 12, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 13, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 14, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 15, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 16, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 17, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 18, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 19, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 100, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 1000, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

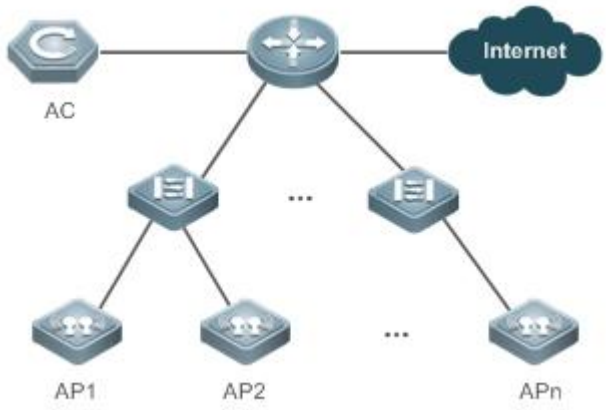
wlan 1048, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.
```

```
RRM status:
RRM 11a status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
RRM 11b status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
 -----> If there are co-channel and adjacent channel interference, suggest
to enable RRM.

Speed limit:
 wlan[1   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[2   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[3   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[4   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[5   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[6   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[7   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[8   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[11  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[12  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[13  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[14  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[15  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[16  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[17  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[18  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[19  ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
```

	wlan[100] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1000] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1048] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]

Configuring One-Click Network Optimization in the Fit AP Architecture

Scenario **Figure 1-14**	 In the Fit AP architecture: ● The AC is the wireless network controller. ● AP1, AP2, ….APn are dual-band APs. ● The AC and AP are connected through a Layer 2 switch and a Layer 3 router. ● One-click network optimization is to be configured.
Configuration Steps	Configure one-click network optimization on the AC.
AC	Hostname# configure terminal Hostname(config)# wopt choose band-select-enable low-rate-disable
Verification	● After one-click network optimization is configured, display the network optimization information. ● Run the **show wopt** command to display network optimization information.
AC	Hostname# show wopt Low rate status: 802.11b rate: 1 Mbps: Disable 2 Mbps: Disable 5.5 Mbps: Disable 11 Mbps: Enable 802.11g rate: 1 Mbps: Disable

```
    2 Mbps: Disable
  5.5 Mbps: Disable
    6 Mbps: Disable
    9 Mbps: Disable
   11 Mbps: Enable
 802.11a rate:
    6 Mbps: Disable
    9 Mbps: Disable

Multicast rate:
1    24  Mbps
2    24  Mbps
3    24  Mbps
4    24  Mbps
5    24  Mbps
6    24  Mbps
7    24  Mbps
8    24  Mbps
11   24  Mbps
12   24  Mbps
13   24  Mbps
14   24  Mbps
15   24  Mbps
16   24  Mbps
17   24  Mbps
18   24  Mbps
19   24  Mbps
100  24  Mbps
1000 24  Mbps
1048 24  Mbps

Session limit:
 Session limit : 255

wlan 1, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 2, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 3, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
```

band select.

wlan 4, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 5, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 6, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 7, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 8, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 11, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 12, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 13, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 14, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 15, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the band select.

wlan 16, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the

```
band select.

wlan 17, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 18, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 19, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 100, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 1000, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

wlan 1048, Band select: enable
 -----> If there are a few devices work in 5.8GHz, suggest to disable the
band select.

RRM status:
RRM 11a status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
RRM 11b status: dca[disable] mode[NA]
                tpc[disable] mode[NA]
 -----> If there are co-channel and adjacent channel interference, suggest
to enable RRM.

Speed limit:
 wlan[1   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[2   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[3   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[4   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
256 Kbps, burst: 300 Kbps]
 wlan[5   ] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average:
```

	256 Kbps, burst: 300 Kbps] wlan[6] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[7] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[8] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[11] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[12] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[13] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[14] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[15] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[16] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[17] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[18] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[19] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[100] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1000] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps] wlan[1048] down-speed[average: 256 Kbps, burst: 300 Kbps] up-speed[average: 256 Kbps, burst: 300 Kbps]

1.4.12 Configuring Intelligent Network Optimization

Configuration Effect

Perform intelligent network optimization based on network conditions.

Configuration Steps

Run the **wis enable** command in configuration mode.

Command	**wis enable**
Parameter Description	N/A
Defaults	Intelligent network optimization is not configured.
Command	AC global configuration mode

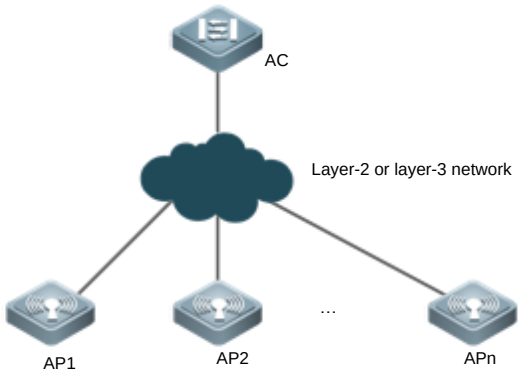
Mode	
Usage Guide	After this command is run on a running network, intelligent optimization can be performed for the network. In normal cases, this command is used by network administrators.

Verification

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

Configuration Examples

Configuring Intelligent Network Optimization

Scenario Figure1-15	
Configuration Steps	Enable intelligent network optimization on the AC.
AC	`Hostname# configure terminal` `Hostname(config-ac)# wis enable`
Verification	● After intelligent network optimization is configured, display the configuration. ● Run the **show running-config** command to display information about intelligent network optimization.

	`Hostname# show running-config`
	`!`
	`wis enable`
	`!`

1.4.13 Configuring Mcell

Configuration Effect

Enable dense deployment optimization.

Configuration Steps

Run the **mcell** command in AP configuration mode.

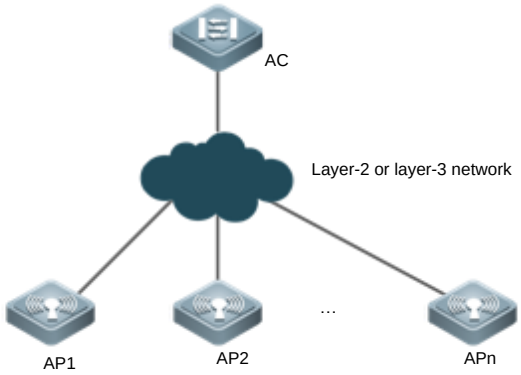
Command	mcell enable **radio** *radio-id*
Parameter Description	*radio-id*: Indicates the index of an RF port. The value range is from 1 to 96.
Defaults	Mcell is disabled.
Command Mode	AP configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Configuring Mcell

Scenario Figure 1-16	
Configuration Steps	Enable the Mcell function on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config AP1`
	`Hostname(config-ap)# mcell enable radio 1`

Verification	● After the Mcell function is configured, display the configuration. ● Run the **show running-config** command to display information about the Mcell function.

	`Hostname# show ap-config running-config`
	`ap-config AP1`
	` mcell enable radio 1`

1.4.14 Configuring Roaming Stickiness

Configuration Effect

Configure this function to enable roaming stickiness monitoring or navigation.

Notes

WIS must be enabled.

Configuration Steps

Configure roaming stickiness in AP-all configuration or AP group configuration mode.

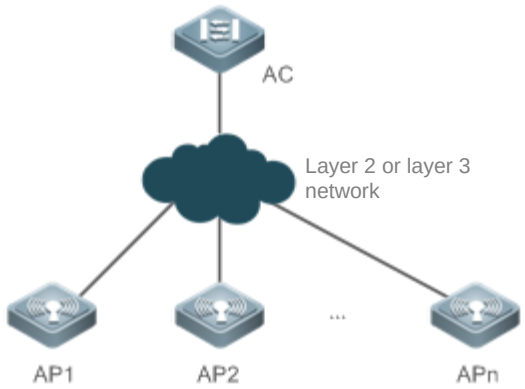
Command	**sticky-steering** { **monitor-only** | **enable** }
Parameter Description	**monitor-only**: Indicates the monitoring mode, that is, only roaming stickiness is monitored. **enable**: Indicates the navigation mode, that is, roaming stickiness navigation is performed if roaming stickiness is detected.
Defaults	Roaming stickiness is disabled.
Command Mode	Configure roaming stickiness for all AP groups in ap-all configuration mode, and configure roaming stickiness for a single AP group in AP group configuration mode.
Usage Guide	N/A

Verification

Run **show running-config** to query the corresponding configuration.

Configuration Example

Configuring Roaming Stickiness

Scenario **Figure 1-17**	
Configuration Steps	● Configure roaming stickiness monitoring on the AC. ● Configure roaming stickiness navigation on the AC.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-config all`
	`Hostname(config-ap)# sticky-steering monitor-only`
	`Hostname(config-ap)# ap-group test1`
	`Hostname(config-group)# sticky-steering enable`

Verification	Run **show running-config** to query the roaming stickiness configuration.

	`Hostname# show running-config`
	`ap-group test1`
	` sticky-steering enable`
	`!`

	ap-group test2 sticky-steering monitor-only ! ap-group test3 sticky-steering monitor-only !

1.4.15 Configuring Automatic Device Information Upload

Configuration Effect

Enable automatic upload of AC and AP software and hardware version information to the WIS cloud.

Notes

- If WIS is not enabled, AC and AP software and hardware version information will also be automatically uploaded after this function is enabled.
- If the WIS client address is configured, the information is uploaded to the WIS client.
- If the WIS client is not configured but the device can access to the WIS public cloud, the information will be uploaded to the WIS public cloud.
- If the WIS client is not configured and the device cannot access to the WIS public cloud, the device information is not uploaded.

Configuration Steps

Perform this operation in global configuration mode.

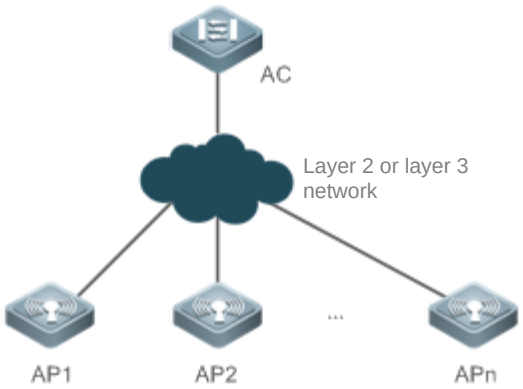
Command	**wis devinfo enable**
Parameter Description	**enable**: Indicates that device information is automatically uploaded.
Defaults	By default, automatic device information upload is enabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Run **show running-config** to query the configuration.

Configuration Example

↘ **Configuring Automatic Device Information Upload**

Scenario **Figure 1-19**	
Configuration Steps	Disable automatic device information upload on the AC.
AC	`Hostname# configure terminal` `Hostname(config)# no wis devinfo enable`
Verification	Run **show running-config** to query the configuration of automatic device information upload.

	`Hostname# show running-config`
	`no wis devinfo enable!`
	`!`

1.5 Monitoring

Displaying

Command	Function
show running-config	Display all configuration information.
show ap-config running *ap-name*	Display the configuration information of a specified AP.
show ap-config radio	Display the radio information of all APs.
show ap-config radio *radio-id* **config** *ap-name*	Display the configuration information of a specified AP's specified radio.
show ap-config radio *radio-id* **status** *ap-name*	Display the detailed status information of an AP's specified radio.
show ap-config radio status *ap-name*	Display the radio list of an AP.
show band-select statistics	Display the running statistics of band selection.
show wopt	Display the network optimization information.

1 Configuring WIS

1.1 Overview

If a large number of access points (APs) connect to a wireless network and the network configuration is improperly planned, the wireless network quality deteriorates easily or the STA experience is poor. In this situation, you can connect the wireless access controller (AC) to the Wireless Intelligent Service (WIS) cloud platform. The AC collects network data of a wireless network, such as version information, basic AP information, and radio frequency (RF) information, analyzes the data, and sends the data analysis result to WIS. Based on the data analysis result, WIS delivers a proper network optimization policy to improve the wireless network quality. In addition, WIS enables network administrators to quickly learn about the network running status.

Protocols and Standards

N/A

1.2 Applications

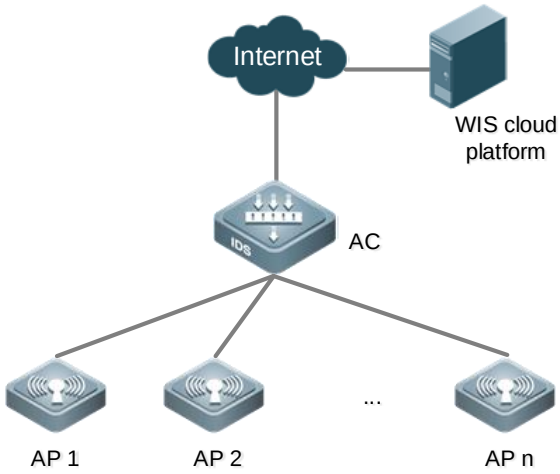
Application	Description
Configuring Intelligent Network Optimization	Enable intelligent wireless network optimization.
Configuring STA Diagnosis	Enable STA diagnosis.

1.2.1 Configuring Intelligent Network Optimization

Scenario

Enable intelligent network optimization on a wireless local area network (WLAN) formed by multiple Fit APs. In Figure 1-1, AP 1, AP 2, ….AP n are Fit APs.

Figure 1-1



Deployment

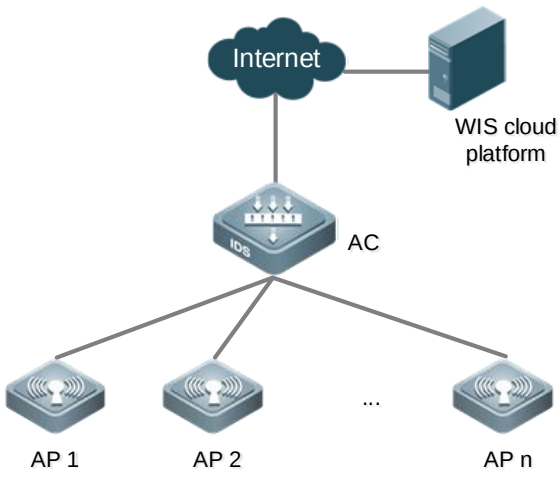
- Connect the AC to WIS.
- Enable intelligent network optimization on the AC.
- The AC periodically reports network data to WIS, and WIS delivers a proper network optimization policy based on the data analysis result.

1.2.2 Configuring STA Diagnosis

Scenario

Enable STA diagnosis on a WLAN formed by multiple Fit APs.

Figure 1-2



Deployment

- Enable STA diagnosis on the AC. The AC sends STA running data, such as association packets, disassociation packets, and diagnosis results to WIS.
- Enable Dynamic Host Configuration Protocol (DHCP) packet parsing on the AC. APs send DHCP packets of STAs to the AC, and the AC forwards them to WIS.
- Display STA diagnosis information on the AC.
- Display STA diagnosis result on WIS.

1.3 Features

Basic Concepts

↘ WIS

WIS is a wireless intelligent service system deployed on the cloud. It receives network data from the AC and delivers network optimization policies.

Overview

Feature	Description

Feature	Description
Configuring Intelligent Network Optimization	Automatically performs network optimization.
Configuring Periodic Version Information Reporting	Configures automatic upload of the AC and AP software and hardware version numbers.
Configuring STA Diagnosis	Enables the diagnosis function. When a STA is faulty, key packet information can be diagnosed to help locate the fault.
Data Reporting of High-Frequency Telemetry	Configures key indicator reporting for APs and STAs.

1.3.1 Configuring Intelligent Network Optimization

Working Principle

The AC periodically reports network data to WIS. Based on the real-time network running status displayed on WIS, a network administrator selects a proper network optimization policy.

Data that the AC sends to WIS periodically includes:

- Wireless network scale data

  Number of APs and STAs

- Wireless network configuration data

  Parameter configuration of network devices

- STA experience data

  MAC address, wireless access status, delay, packet loss, rate, signal strength, load, traffic, STA capability, STA features, and STA type of a certain user or users of a certain area accessing the network

  Wireless network access or disconnection of STAs

Network optimization policies include:

- One-click network optimization

  A network administrator enables automatic network optimization through one-click network optimization on WIS. WIS automatically delivers network optimization policies to the AC.

- Access optimization

  A network administrator can also manually plan proper network configurations and deliver them to the AC, such as reducing the signal strength of APs in areas with serious interference and adjusting the working channels of APs.

1.3.2 Configuring Periodic Version Information Reporting

Working Principle

The AC sends software and hardware version numbers of the AC and AP to WIS using the Hypertext Transfer Protocol (HTTP) or HTTP Secure (HTTPS) protocol to enable network administrators to view version information about managed devices.

1.3.3 Configuring STA Diagnosis

Working Principle

APs report processed control service flows to the AC. Based on the reported service data, the AC analyzes the STA running status and reports it to WIS. A network administrator can view the STA diagnosis result on WIS and quickly learn about STA fault causes.

Control network data that APs report to the AC does not include DHCP packets of STAs. After APs periodically send DHCP packets to the AC, the AC can analyze DHCP packets to diagnose STA fault causes in the IP address obtaining phase.

1.3.4 Data Reporting of High-Frequency Telemetry

Working Principle

To achieve real-time visualized monitoring of network-wide wireless experience and locate problems within 5 minutes, key indicators of APs and wireless STAs need to be monitored in real time at second level, and historical records can be traced. APs collect all indicators and write the indicators into metrics. Then, APs periodically report specified indicators in metrics to the cloud.

1.4 Configuration

Configuration	Description and Command	
Configuring Intelligent Network Optimization	⚠ (Mandatory)	
	wis enable	Enables intelligent network optimization.
Configuring Periodic Version Information Reporting	⚠ (Optional)	
	wis devinfo enable	Enables the AC to report version information periodically.
Configuring STA Diagnosis of the WIS	⚠ (Optional)	
	wis tsr enable	Enables STA diagnosis of WIS.
	wis tsr packet-parser enable	Enables APs to send DHCP packets to the AC.
Configuring Data Reporting of High-frequency Telemetry	⚠ (Optional)	
	wis hfmg app-upload enable *apg_nam*	Enables indicator reporting for a specified application group.
	wis hfmg app-upload interval *value*	Configures the indicator reporting period for an application.
	wis hfmg ap-upload enable *ap_mac*	Enables indicator reporting for a specified AP.
	wis hfmg ap-upload interval *value*	Configures the indicator reporting period for an AP.
	wis hfmg radio-upload enable *ap_mac radio_id*	Enables indicator reporting on a specified radio of a specified AP.

Configuration	Description and Command	
	wis hfmg radio-upload interval *value*	Configures the indicator reporting period for a radio.
	wis hfmg sta-upload enable *sta_mac*	Enables indicator reporting for a specified STA.
	wis hfmg sta-upload interval *value*	Configures the indicator reporting period for a STA.

1.4.1 Configuring Intelligent Network Optimization

Configuration Effect

After intelligent network optimization is enabled, the AC periodically reports network data to WIS. A network administrator performs intelligent network optimization through WIS.

Notes

Before enabling the intelligent network optimization function, connect the AC to WIS.

Configuration Steps

↘ Enabling Intelligent Network Optimization

- Mandatory.
- Run the **wis enable** command in global configuration mode.

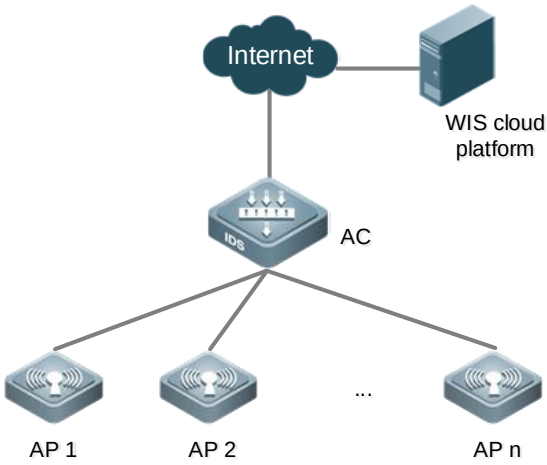
Command	**wis enable**
Parameter Description	N/A
Defaults	Intelligent network optimization is disabled by default.
Command Mode	Global configuration mode
Usage Guide	1. After this function is enabled, all APs on a network will send network data to the AC. The function will consume the performance of CAPWAP channels between the APs and AC. It is recommended that this function be used only by network administrators and enabled when the network is idle. 2. In hot standby networking, this function needs to be configured on both the active and standby devices. 3. In AC virtualized networking, this function only needs to be configured on the active AC.

Verification

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

Configuration Example

↘ Configuring Intelligent Network Optimization

Scenario **Figure 1-3**	
Configuration Steps	Enable intelligent network optimization on the AC.
AC	`Hostname#configure terminal` `Hostname(config)# wis enable`
Verification	After intelligent network optimization is enabled, run the **show running-config** command to display the configuration on the AC.

	`Hostname#show running-config`
	`!`
	`wis enable`
	`!`

Common Errors

N/A

1.4.2 Configuring Periodic Version Information Reporting

Configuration Effect

Software and hardware version information of the AC and AP is uploaded to WIS periodically.

Notes

N/A

Configuration Steps

- In global configuration mode of the AC, enable the AC to periodically report version information to WIS. Version information includes the software and hardware version information.
- Optional.

Command	**wis devinfo enable**
Parameter Description	N/A

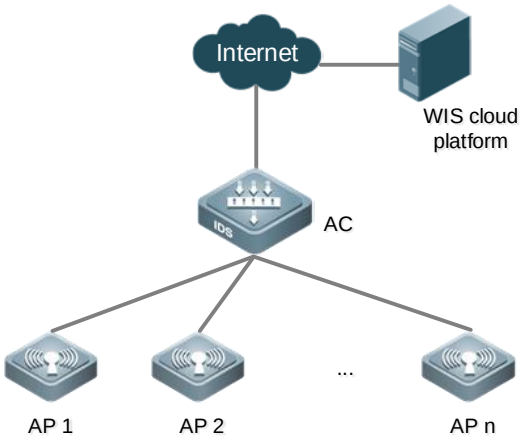
Defaults	Periodic information reporting is enabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Configuring Automatic Upload of Device Information to WIS

Scenario Figure 1-4	
Configuration Steps	Disable automatic version information upload to WIS on the AC.
AC	`Hostname# configure terminal` `Hostname(config)# no wis devinfo enable`
Verification	Run the **show running-config** command to display the configuration.

	`Hostname# show running-config`
	`no wis devinfo enable!`
	`!`

Common Errors

N/A

1.4.3 Configuring STA Diagnosis of the WIS

Configuration Effect

After the STA diagnosis function of WIS is enabled, the AC diagnoses the STA fault causes based on the network data sent by APs and sends the diagnosis results to WIS.

Notes

- STA diagnosis is enabled by default.

- APs periodically send DHCP packets to the AC.

Configuration Steps

Configuring STA Diagnosis

- STA diagnosis is enabled by default.
- Optional.

Command	**wis tsr enable**
Parameter Description	N/A
Defaults	STA diagnosis is enabled by default.
Command Mode	Global configuration mode
Usage Guide	STA diagnosis information on the AC will be aged periodically. A network administrator can view all diagnosis information on WIS.

Configuring APs to Send DHCP Packets to the AC

- APs send DHCP packets to the AC by default.
- Optional.

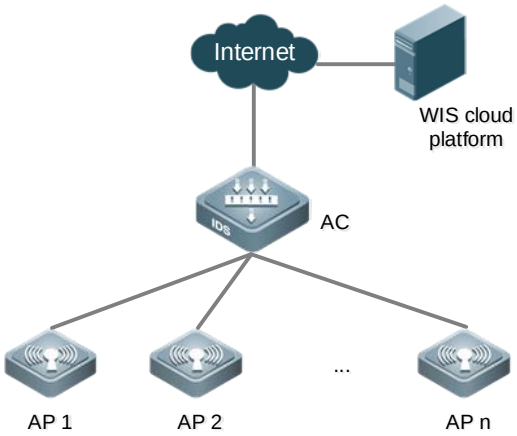
Command	**wis tsr packet-parser enable**
Parameter Description	N/A
Defaults	APs send DHCP packets to the AC by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Run the **show wis tsr status** command to display the STA diagnosis function.

Configuration Example

Enabling STA Diagnosis of WIS

Scenario **Figure 1-5**	

Configuration Steps	Disable STA diagnosis of WIS on the AC.
AC	`Hostname#configure terminal` `Hostname(config)# no wis devinfo enable`
Verification	Run the **show running-config** command to display the configuration.

	`Hostname#show running-config`
	`no wis devinfo enable!`
	`!`

Common Errors

N/A

1.4.4 Configuring Data Reporting of High-frequency Telemetry

Configuration Effect

Data reporting of high-frequency telemetry can be used to control the reporting period and reporting status (enabled/disabled) of indicators related to apps, APs, STAs, and radios.

Notes

- The default period of reporting all types of indicators is 20 seconds.
- By default, no indicator is reported.
- This function can be used only after the **wis enable** command is enabled.
- When you configure the period, the parameter represents n times 5 seconds, and the actual configuration effect is n x 5 seconds.

Configuration Steps

Enabling Indicator Reporting for a Specified Application Group

Command	**wis hfmg app-upload enable** *apg_name*
Parameter Description	*apg_name*: Indicates the name of the application group.
Defaults	Disabled
Command Mode	Global configuration mode
Usage Guide	Up to 114 entries can be configured.

Configuring the Indicator Reporting Period for an Application

Command	**wis hfmg app-upload interval** *value*
Parameter Description	*value*: Indicates the value in the unit of 5 seconds. When value is 1, the effective period is 5 seconds.
Defaults	20 seconds
Command	Global configuration mode

Mode	
Usage Guide	N/A

Enabling Indicator Reporting on a Specified AP

Command	**wis hfmg ap-upload enable** *ap_mac*
Parameter Description	*ap_mac*: Indicates the MAC address of the AP.
Defaults	Disabled
Command Mode	Global configuration mode
Usage Guide	Up to 500 entries can be configured.

Configuring the Indicator Reporting Period for an AP

Command	**wis hfmg ap-upload interval** *value*
Parameter Description	*value*: Indicates the value in the unit of 5 seconds. When value is 1, the effective period is 5 seconds.
Defaults	20 seconds
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Indicator Reporting on a Specified Radio of a Specified AP

Command	**wis hfmg radio-upload enable** *ap_mac radio_id*
Parameter Description	*ap_mac radio_id*: Indicates the MAC address of the AP and the ID of the radio on the AP respectively.
Defaults	Disabled
Command Mode	Global configuration mode
Usage Guide	Up to 500 entries can be configured.

Configuring the Indicator Reporting Period for a Radio

Command	**wis hfmg radio-upload interval** *value*
Parameter Description	*value*: Indicates the value in the unit of 5 seconds. When value is 1, the effective period is 5 seconds.
Defaults	20 seconds
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Indicator Reporting on a Specified STA

Command	**wis hfmg sta-upload enable** *sta_mac*
Parameter Description	*sta_mac*: Indicates the MAC address of the STA.
Defaults	Disabled
Command	Global configuration mode

Mode	
Usage Guide	Up to 500 entries can be configured.

Configuring the Indicator Reporting Period for a STA

Command	**wis hfmg sta-upload interval** *value*
Parameter Description	*value*: Indicates the value in the unit of 5 seconds. When value is 1, the effective period is 5 seconds.
Defaults	20 seconds
Command Mode	Global configuration mode
Usage Guide	N/A

1.5 Monitoring

Clearing

N/A

Debugging

N/A

Displaying

Command	Description
show wis tsr status	Displays the STA diagnosis function.
show wis tsr [*sta-mac-address*]	Displays STA diagnosis information.

1 Configuring STA-TRACE

1.1 Overview

As a tool for tracing key stations (STAs) and obtaining key packets, STA-TRACE identifies key packets, parses key fields in packets, and analyzes the field meaning to determine whether the protocol exchange process is normal. It helps users collect STA online fault information conveniently, quickly locate STA faults, and improve the user experience.

With STA-TRACE enabled, access points (APs) controlled by an access controller (AC) obtain key packets of key STAs. This function makes full use of APs on a network and can collect complete fault information onsite at a time. Fault reproduction is not required for fault processing. STA-TRACE can automatically identify network exceptions and collect key information onsite to facilitate fault analysis and locating and improve the fault processing efficiency.

Protocols and Standards

N/A

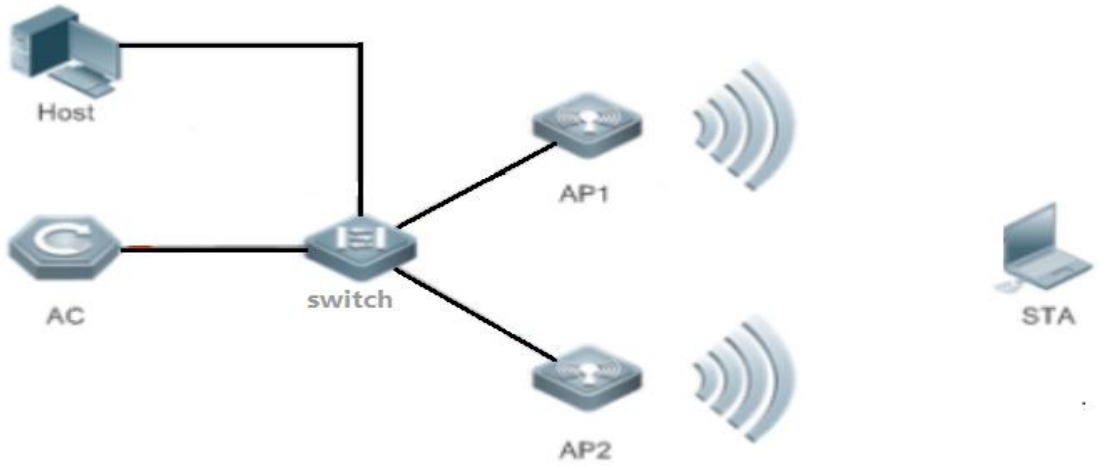
1.2 Applications

Application	Description
Enabling STA-TRACE in Fit AP Mode	In a Fit AP environment, enable STA-TRACE on the AC. A remote host can download packet files through Wireless Intelligent Service (WIS) Cloud or Eweb.

1.2.1 Enabling STA-TRACE in Fit AP Mode

Scenario

In Fit AP mode, APs controlled by the AC trace key STAs, obtain packets on a network, and report them to the AC, as shown in the following figure.



Deployment

- Enable STA-TRACE.
- Configure the media access control (MAC) address of the STA to be traced.

1.3 Features

Basic Concepts

STA, AP, AC

- STA: indicates a wireless station equipped with network interface cards (NICs), for example, portable computer or mobile phone
- AP: provides wireless signals for STAs to access a network.
- AC: provides wireless connections and services.

Fast Forwarding Channel

A fast forwarding channel refers to the communication channel between the kernel and processes. The fast forwarding method of the fast forwarding framework is used for communication.

CAPWAP Tunnel

In the Fit AP architecture, the AC centrally manages all APs through a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel. Control policies sent to APs do not need to be independently configured on the APs. The CAPWAP protocol is used for establishing control and data channels between the APs and AC. The control channels are used by the AC to configure APs and by APs to send event advertisements to the AC, and the data channels are used to send data packets between the APs and AC.

Control Channel and Data Channel

- Control channel: is used by the AC to configure APs and APs to send event advertisements to the AC.
- Data channel: is used to send data packets between the APs and AC.

Overview

Feature	Description
Enabling STA-TRACE	The AC obtains key packets sent and received by APs during the STA login process.

1.3.1 Enabling STA-TRACE

The STA-TRACE function enables the AC to control APs and obtain key packets sent and received by APs during the online process of key STAs. This ensures key packet tracing of key STAs on the entire network and real-time packet analysis remotely.

Working Principle

The STA-TRACE function obtains key packets during the STA online process to monitor the STA online behavior. APs filter wired or wireless packets sent by STAs to trace the STA online behavior and use the CAPWAP data channels to send the data to the AC. The AC stores the data to the Redis database and periodically sends it to the WIS in file format.

Key packets include the management frames, four-way handshake packets, DHCP packets, AR packets, and ICMP packets.

The AC controls APs to enable STA-TRACE.

1 APs filter out key packets from wired or wireless packets.

2 APs add required fields for key packets and transparently forward them to the AC through the CAPWAP tunnel.

3 The AC stores the packets in the Redis database, adds the PCAP header to the packet files, and sends the packet files to the WIS module or Eweb of the remote host.

4 The remote host uses a tool that can parse custom packet protocols (such as WireShark) to analyze and process the packets.

1.4 Configuration

Configuration	Description and Command	
Enabling STA-TRACE	(Mandatory) It is used to enable the STA-TRACE service on APs controlled by the AC. Perform either of the following configurations.	
	sta-trace enable all-trace	Enables the STA-TRACE service to filter out all key packets.
	sta-trace enable wireless	Enables the STA-TRACE service to filter out wireless packets.
Configuring STA Information	(Mandatory) It is used to configure the device to monitor STA information.	
	sta-trace sta	Configures the MAC address of a STA.
Configuring the Limited Number of Packets	(Optional) It is used to configure the number of packets captured.	
	sta-trace pkt-count	Configures the number of packets stored in the Redis database.
Configuring the Size of a Stored File	(Optional) It is used to configure the size of a stored file.	
	sta-trace file-size	Configures the size of a stored file.

1.4.1 Enabling STA-TRACE

Configuration Effect

- To trace key packets, the STA-TRACE service must be enabled.
- You can select whether to filter out all packets or wireless packets only.

Notes

- After the STA-TRACE service is enabled, the MAC address of the STA needs to be configured to start packet obtaining.

Configuration Steps

Enabling STA-TRACE

- Mandatory.
- To trace key packets, enable the STA-TRACE service on the AC.
- Run the **sta-trace enable all-trace** command to enable the STA-TRACE service.
- Run the **sta-trace enable wireless-trace** command to enable the STA-TRACE service on the wireless end.

Command	sta-trace enable all-trace/wireless-trace
Parameter Description	N/A
Defaults	The STA-TRACE service is disabled by default.
Command Mode	Global configuration mode
Usage Guide	After the STA-TRACE service is enabled, the MAC address of the STA needs to be configured.

Verification

Run the **show running-config** command to display the function and check whether the STA-TRACE service is configured.

Configuration Example

Enabling STA-TRACE in a Fit AP Environment

Configuration Steps	

AC	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# sta-trace enable`

Verification	● Display the function.

AC	`Hostname# show running-config`
	`!`
	`sta-trace enable all-trace`
	`!`

Common Errors

N/A

1.4.2 Configuring STA Information

Configuration Effect

After STA information is entered on the AC, APs automatically obtain packets of associated STAs.

Notes

N/A

Configuration Steps

Configuring STA Information

- Mandatory.
- To trace key packets on an AP, STA information needs to be configured on the AC.
- Run the **sta-trace sta** *H.H.H* command to configure the STAs to be traced.
- Configure STA information and enable STA-TRACE.

Command	**sta-trace sta** *H.H.H*
Parameter Description	*H.H.H*: MAC address of a STA.
Defaults	N/A
Command Mode	Global configuration mode
Usage Guide	Only online APs that support STA-TRACE will trace STA packets.

Verification

- Display STA information. Configured STA information is displayed.
- Run the **show running-config** command to display configured STA information.

Configuration Example

Configuring STA Information in a Fit AP Environment

Configuration Steps	● Configure the STA whose MAC address is 1032.7e5d.6ecf as a key STA.

AC	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# sta-trace enable all-trace`
	`Hostname(config)# sta-trace sta 1032.7e5d.6ecf`

Verification	● Display the STA configuration.

AC	`Hostname# show sta-trace sta-info`
	`Mac Address    Pkt Number File Number`
	`-------------- ---------- ------------`
	`7cc3.a19d.63fb 14371      2`
	`7cc3.a19d.63fc 11163      2`
	`7cc3.a19d.63fd 11135      2`
	`7cc3.a19d.63fe 11129      2`
	`7cc3.a19d.63ff 11104      2`
	`1032.7e5d.6ecf 11096      2`
	
	`Send Fail ToAP Add Fail ToREDIS`
	`-------------- ----------------`
	`0              0`

Common Errors

N/A

1.4.3 Configuring the Limited Number of Packets

Configuration Effect

Configure the number of packets that can be stored for each STA to restrict the number of packets stored in the Redis database.

Notes

N/A

Configuration Steps

Configuring the Number of Packets Obtained

- Optional.
- Perform this configuration on the AC.
- Run the **sta-trace pkt-count pktnum** command on the AC to configure the number of packets stored.

Command	**sta-trace pkt-count** *pktnum*
Parameter Description	*pktnum*: Number of packets that can be stored for each STA. The value range is from 0 to 1000000. The default value is 5000.
Defaults	The default number of packets stored for each STA is 5000.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Configuring the Number of Packets on the AC

Configuration Steps	Enter the global configuration mode on the AC.

AC	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# sta-trace pkt-count 1000`

Verification	Display the configuration on the AC.

AC	`Hostname#show running-config`
	`mac-address-table filtering 1032.7e5d.6ecf vlan 5`
	`!`
	`sta-trace enable all-trace`

	sta-trace sta 1032.7e5d.6ecf sta-trace pkt_count 1000 ! wlan-cap forward central

1.4.4 Configuring the Size of a Stored File

Configuration Effect

Configure the size of an STA packet file to restrict the storage capacity of a file.

Notes

N/A

Configuration Steps

Configuring the Size of a Stored File

- Optional.
- Perform the configuration on the AC.
- Run the **sta-trace file-size size** command on the AC to configure the number of packets stored.

Command	**sta-trace file-size** *size*
Parameter Description	*size*: Size of each STA packet file, in MB. The value is 1, 2, or 3.
Defaults	The default file size is 1 MB.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Configuring the Number of Packets on the AC

Configuration Steps	Enter the global configuration mode on the AC.
AC	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# sta-trace file-size 2
Verification	Display the configuration on the AC.
AC	Hostname#show running-config mac-address-table filtering 1032.7e5d.6ecf vlan 5

```
!
sta-trace enable all-trace
sta-trace sta 1032.7e5d.6ecf
sta-trace file-size 2
!
wlan-cap
 forward central
```

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show sta-trace sta-info	Displays the STA-TRACE configuration.
show wlan-cap stat	Displays AP-related configuration on an AP.

Debugging

N/A

1 Configuring Broadcast Forwarding Control

1.1 Overview

Broadcast forwarding control includes weight-based broadcast forwarding control and broadcast forwarding control in wireless mode.

- Weight-based broadcast forwarding control means restricting weights of packet types for broadcast forwarding, so as to prevent stations (STAs) from being affected when a certain type of packets occupy all resources. This mode is applicable to all packets to be flooded.
- Broadcast forwarding control in wireless mode means forwarding only required packets to a wireless network, so as to prevent some useless broadcast packets from occupying substantial radio frequency (RF) resources. This mode is applicable to all packets to be sent to the air interface.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Broadcast Forwarding Control	The Fit AP networking contains at least one access controller (AC) and one Fit access point (AP).

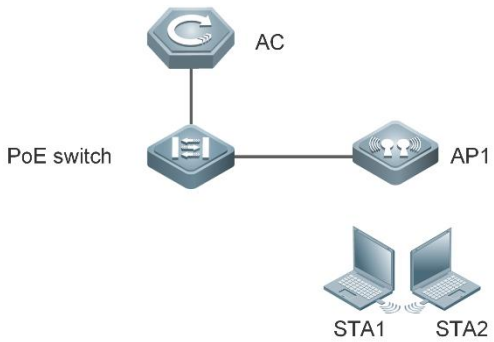
1.2.1 Broadcast Forwarding Control

Scenario

An AC is deployed on a wireless network and enabled with broadcast forwarding control in wireless mode.

The AC controls wireless forwarding of broadcast packets, as shown in Figure 1-1.

Figure 1-1



Deployment

Enable broadcast forwarding control in wireless mode on the AC.

1.3 Features

Basic Concepts

Weight-based Broadcast Forwarding 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 Forwarding Control in Wireless Mode

This function is used to forward only required broadcast packets to a wireless network, so as to prevent certain broadcast packets from occupying substantial air interface resources and improve network rates of STAs.

ARP Broadcast Control

In some scenarios, intra-LAN ARP discovery is prevented. That is, users on a LAN do not respond to ARP request packets from an 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. CAPWAP tunnel interfaces can be enabled to mutually broadcast ARP or ND packets.

Allowing mDNS Packets to Pass Through

For broadcast forwarding control in wireless mode, Multicast DNS (mDNS) packets are not allowed to pass through by default. In some scenarios such as screen mirroring, mDNS keepalive packets from the screen end to a terminal are blocked by the AC, causing a mirroring disconnection. To restore mirroring, configure the AC to allow mDNS packets to pass through.

Allowing SSDP Packets to Pass Through

For broadcast forwarding control in wireless mode, Simple Service Discovery Protocol (SSDP) packets are not allowed to pass through by default. The AC can be configured to allow SSDP packets to pass through as required.

Allowing OSPF Packets to Pass Through

For broadcast forwarding control in wireless mode, Open Shortest Path First (OSPF) packets are not allowed 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 AC can be configured to allow OSPF packets to pass through.

Allowing VRRP Packets to Pass Through

For broadcast forwarding control in wireless mode, Virtual Router Redundancy Protocol (VRRP) packets are not allowed to pass through by default. The AC can be configured to allow VRRP packets to pass through as required.

Broadcast and Multicast Packet Optimization on Air Interfaces

On wireless networks, data is transmitted over air interfaces. Both APs and STAs need to compete for air interface channels. On the same channel, only one device can transmit data at a time. In this case, broadcast or multicast packets compete for air interface resources, which will affect the quality of the service network.

- To ensure stable transmission of broadcast or multicast packets over air interfaces, the protocol stipulates that broadcast or multicast packets are transmitted at the lowest rate on wireless networks. However, the competition of for air interface resources by broadcast and multicast packets will reduce the overall rate on the service network.
- Broadcast or multicast packets are used to request a service, and many STAs on the network will receive these packets. Typically, only one STA needs to respond, while the unnecessary broadcast or multicast packets consume wireless network and device resources.
- On wireless networks, numerous protocols (such as ARP and DHCP) require the transmission of broadcast or multicast packets over air interfaces, which will occupy a large number of air interface resources. This may cause network congestion and results in a decrease in Wi-Fi performance.

Therefore, it is necessary to identify and analyze broadcast and multicast packets, and implement a series of measures to reduce the forwarding of broadcast and multicast packets.

- Respond to only specific devices in the network topology by proxy or by converting broadcast or multicast packets into unicast packets.
- Discard broadcast and multicast packets that are not allowed to be transmitted over air interfaces.
- Implement rate limiting for broadcast and multicast packets transmitted over air interfaces.

Overview

Feature	Description
Weight-based Broadcast Forwarding Control	Restricts weights of packet types for broadcast forwarding, so as to protect broadcast forwarding resources from being occupied by a certain type of packets and thereby guarantee normal forwarding of other packets.
Broadcast Forwarding Control in Wireless Mode	Controls whether to forward broadcast packets to a 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.
ARP or ND Broadcast Isolation	Configures the AC to mutually broadcast ARP or ND packets between CAPWAP tunnel interfaces.
mDNS Packet Control	Configures the AC to allow mDNS packets to pass through.
SSDP Packet Control	Configures the AC to allow SSDP packets to pass through.
OSPF Packet Control	Configures the AC to allow OSPF packets to pass through.
VRRP Packet Control	Configures the AC to allow VRRP packets to pass through.
Intra-VLAN STA isolation	Enables intra-VLAN STA isolation.
Prohibition of Downstream Broadcast and Multicast Packets on Air Interfaces	Prohibits the device from sending downstream broadcast or multicast packets to air interfaces.
Control over Broadcast and Multicast Packets of Different Types	Configures forwarding policies and rate limit for different types of broadcast and multicast packets.
Rate Limiting on Broadcast and Multicast Packets	Configures a rate limit for broadcast and multicast packets of different types or different protocols as required.

Intelligent ARP Packet Forwarding	Configures intelligent ARP packet forwarding.
Intelligent DHCP Packet Forwarding	Configuring intelligent DHCP packet forwarding.

1.3.1 Weight-based Broadcast Forwarding Control

This function 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

- Classify packets. Packets can be classified into 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 Forwarding Control in Wireless Mode

This function is used to forward only some 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. On a wireless network, air interface resources are shared by STAs and APs which often becomes a bottleneck for STAs. Broadcast packets are sent at low rates, which occupies more air interface resources.

In practice, some broadcast packets are useless for STAs. Forwarding these packets to a wireless network will result in fewer air interface resources and lowered 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.

On the AC, ARP broadcast packets are parsed to disallow STA from sending gratuitous ARP, sending ARP spoofing packets pretending to be the gateway, or forwarding ARP packets with non-trusted destination IPs for uplink ARP. Only ARP packets with trusted source IPs are allowed to be forwarded for downlink ARP.

1.3.4 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.

1.3.5 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 where broadcast forwarding control in wireless mode is disabled, you can run the command to send mDNS packets to the CAPWAP tunnel interface.

1.3.6 SSDP Packet Control

When broadcast forwarding control in wireless mode 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 where broadcast forwarding control in wireless mode is disabled, you can run the command to send SSDP packets to the CAPWAP tunnel interface.

1.3.7 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 where broadcast forwarding control in wireless mode is disabled, you can run the command to send OSPF packets to the CAPWAP and roaming tunnel interfaces.

1.3.8 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 where broadcast forwarding control in wireless mode is disabled, you can run the command to send VRRP packets to the CAPWAP and roaming tunnel interfaces.

1.3.9 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.

1.3.10 Prohibition of Downstream Broadcast and Multicast Packets on Air Interfaces

Working Principle

The AC and AP are prohibited from sending broadcast and multicast packets, which reduces the number of broadcast and multicast packets sent to air interfaces and alleviate the competition for air interface resources.

1.3.11 Control over Broadcast and Multicast Packets of Different Types

Working Principle

In scenarios where you need to configure the AC and AP to control broadcast and multicast packets of different types, configure forwarding policies for specified broadcast and multicast packets.

By default, the AC and AP are allowed to forward all broadcast and multicast packets.

To specify the type of packets that are not allowed to be forwarded, configure the device to block specified broadcast and multicast packets.

To specify the type of packets that can be forwarded, disable the forwarding of all broadcast and multicast packets and then permit specified broadcast and multicast packets, or permit specified broadcast and multicast packets directly.

1.3.12 Rate Limiting on Broadcast and Multicast Packets

Working Principle

You can limit the rate of broadcast and multicast packets of different types or different protocols as required.

Broadcast and multicast types include well-known multicast, unknown multicast, broadcast, and unknown unicast. You can limit the rate of packets based on the broadcast and multicast types. If the broadcast and multicast packets of a specific protocol are configured to be forwarded, you can also limit the rate of the broadcast and multicast packets of different protocols. This effectively reduces resource competition and improves air interface performance.

1.3.13 Intelligent ARP Packet Forwarding

On an IPv4 network, the most common broadcast and multicast packets are ARP and DHCP packets. These packets usually require a specific server or client to respond, but are broadcast on Layer 2 WLANs. Intelligent ARP packet forwarding can be used to intelligently identify ARP packets and forward only the ARP packets required by clients.

Working Principle

The AP processes the broadcast ARP request packet received by the air interface as follows:

- Proxy ARP is configured so that the AC or AP can respond to the ARP request packet.
- If the STA corresponding to the IP address in the ARP request packet is not connected to the AP, the AP considers that the STA is connected to another AP and discards the ARP request packet.

1.3.14 Intelligent DHCP Packet Forwarding

Working Principle

When a STA goes online, it sends a DHCP broadcast request packet that needs to be forwarded to the DHCP server, not to other STAs. Therefore, the AP does not need to forward the DHCP broadcast request packet over the air interface to prevent other wireless STAs from receiving the packet.

Some STAs require the DHCP server to respond to DHCP broadcast request packets. Therefore, DHCP broadcast response packets exist on the network. These packets need to be sent only to specific STAs. The AP can intelligently identify the STA addresses in DHCP broadcast response packets:

- If the STA is connected to the AP, the AP converts the DHCP response packet into a unicast packet and sends it to the client.
- If the STA is not connected to the AP, the AP discards the DHCP response packet.

1.4 Configuration

Configuration	Description and Command	
Configuring	⚠ (Optional) It is used to set the weights of packet types for broadcast forwarding.	
	data-plane queue-weight	Configures the weights of packet types for broadcast forwarding on the AC or AP.
	data-plane token	Configures the refresh interval of the broadcast token bucket and bucket-based rate on the AC or AP.
Configuring Broadcast Forwarding	⚠ (Optional) It is used to enable the broadcast wireless forwarding function.	
	data-plane wireless-broadcast	Enables or disables broadcast forwarding control in wireless mode on the AC or AP.
Configuring ARP Broadcast Control	⚠ (Optional) It is used to enable ARP broadcast control to prevent ARP discovery on 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.
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 broadcast forwarding control in wireless mode is disabled.
	data-plane close-ssdp-filter	Allows SSDP packets to pass through when broadcast forwarding control in wireless mode is disabled.
	data-plane close-ospf-filter	Allows OSPF packets to pass through when broadcast forwarding control in wireless mode is disabled.
	data-plane close-vrrp-filter	Allows VRRP packets to pass through when broadcast forwarding control in wireless mode 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.
Configuring a Forwarding Policy for Broadcast or Multicast Packets	Optional. It is used to configure forwarding policies for broadcast and multicast packets.	
	data-plane bcmc deny all	Disables the AC and AP from sending broadcast and multicast packets to air interfaces.
	data-plan bcmc { **arp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **ssdp** | **ospf** | **vrrp** | **igmp** | **mld** | **other-broadcast** | **other-multicast** } **disable**	Disables the AC and AP from forwarding broadcast and multicast packets of different protocols.
	data-plane bcmc { **arp** | **igmp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **ssdp** | **other-broadcast** | **other-multicast** } **packets**	Configures a rate limit for broadcast and multicast packets of different protocols on the AC and AP.
	data-plane bcmc [**broadcast** | **multicast** | **unicast** | **unknown-multicast** | **unknown-unicast**] **packets**	Configures a rate limit for broadcast, multicast, and unknown unicast packets on the AC and AP.
Configuring Intelligent ARP Packet Forwarding	Optional. It is used to configure intelligent ARP packet forwarding. This function needs to be used with proxy ARP.	
	data-plane bcmc smart arp forward	Configures the AP to discard ARP broadcast packets of STAs not associated with the AP.
Configuring Intelligent	Optional. It is used to configure intelligent DHCP packet forwarding.	

DHCP Packet Forwarding	**data-plane bcmc smart dhcp forward**	Configures the AP to discard DHCP broadcast response packets for STAs not associated with the AP.

1.4.1 Configuring Weights for Broadcast Forwarding

Networking Requirements

You can control the weight of a packet type for forwarding according to the network situation, so as to avoid network congestion due to excessive burst traffic.

Notes

N/A

Configuration Steps

Configuring Weights for Broadcast Forwarding

- Optional. Run the **data-plane queue-weight** command to configure the broadcast forwarding weights.
- For centralized forwarding, configure this command in global configuration mode on the AC.
- For local forwarding, configuration this command in AP configuration mode on the AC.

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 weight for forwarding unicast packets. The value range is from 1 to 100. The default weight is 16. *multicast-packet-weight*: Sets the weight for forwarding multicast packets. The value range is from 1 to 50. The default weight is 4. *broadcast-packet-weight*: Sets the weight for forwarding broadcast packets. The value range is from 1 to 50. The default weight is 2. *unknown-multicast-packet-weight*: Sets the weight for forwarding unknown multicast packets. The value range is from 1 to 25. The default weight is 1. *unknown-unicast-packet-weight*: Sets the forwarding weight of unknown unicast packets. The value 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 the Refresh Interval of Broadcast Token Bucket and Bucket-based Rate

- Optional. Run the **show run** command to display the configuration.
- For centralized forwarding, configure this command in global configuration mode on the AC.
- For local forwarding, configuration this command in AP configuration mode on the AC.

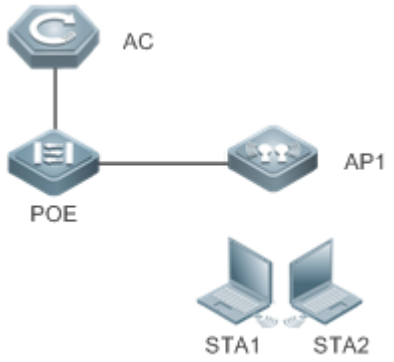
Command	**data-plane token** *token-interval token-base-rate*

Parameter Description	*token-interval*: Indicates the refresh interval of broadcast token bucket, in 10 ms. The default interval is 1. The value range is from 1 to 10,000. *token-base-rate*: Indicates the token bucket-based rate. The default rate is 64 for the AC and 5 for the AP. The value range is from 1 to 1,000,000.
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 Example: Broadcast rate per second for the AC = 1 x (1 / 0.01) x 64 = 6400 pps

Configuration Example

Configuring Weights for Broadcast Forwarding

Figure 7-1



Configuration Steps	Configure weights of packet types for broadcast forwarding in global configuration mode.

AC	`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 running-config** command to display the configuration.

AC	`Hostname#show running-config`
	`…`
	`!`
	`cwmp`
	`!`
	`data-plane queue-weight 100 50 50 25 25`
	`data-plane token 10 10`
	`!`
	`…`

Common Errors

N/A

1.4.2 Configuring Broadcast Forwarding Control in Wireless Mode

Networking Requirements

Useless broadcast packets are not forwarded to the air interface.

Notes

N/A

Configuration Steps

Configuring Broadcast Forwarding

- Optional.
- Broadcast packets on a network are limited by default.
- You can configure this function accordingly if you want to remove the limitation on broadcast packets on the network.

Command	**data-plane wireless-broadcast** { **enable** | **disable** }
Parameter Description	**enable**: Permits all broadcast packets to be forwarded to the air interface. **disable**: Prevents all broadcast packets from being forwarded to the air interface.
Defaults	Broadcast forwarding control in wireless mode is disabled; that is, broadcast packets are not forwarded to the wireless network.
Command Mode	Global configuration mode
Usage Guide	N/A

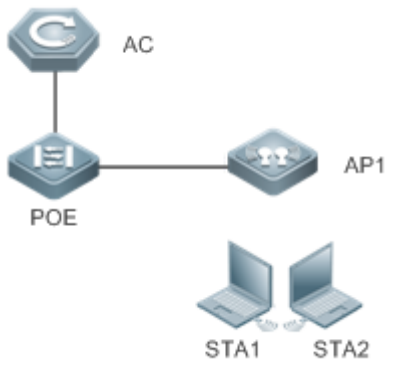
Verification

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

Configuration Example

Enabling Broadcast Forwarding Control in Wireless Mode

Figure 7-2



Configuration	Enable broadcast forwarding control in wireless mode in global configuration mode.

Steps	
AC	Hostname#configure terminal Hostname(config)#data-plane wireless-broadcast enable
Verification	Run the **show running-config** command to display the configuration.
AC	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.
- Configure this command in AC 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 Ruijie Cloud scenarios, configure this command in AC global configuration mode.

Command	**data-plane arp-control vlan** *vlan-id* **trusted-host** *ipv4-address*

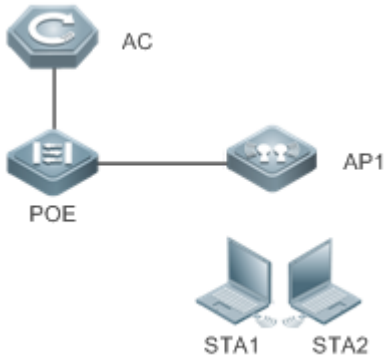
Parameter Description	*vlan-id*: Indicates the ID of the VLAN to be enabled with ARP broadcast control. The value range is from 1 to 4094. *ipv4-address*: Indicates the trusted IP address. Up to 64 IP addresses are allowed.
Defaults	No trusted IP address is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Enabling ARP Broadcast Control

Scenario Figure1-1	
Configuration Steps	● Enable ARP broadcast control in global configuration mode.
AC	`Hostname#configure terminal` `Hostname(config)# data-plane arp-control enable`
Verification	● Run the **show running-config** command to display the configuration.

AC	`Hostname# show running-config`
	`!`
	`cwmp`
	`!`
	`data-plane arp-control enable`
	`!`

Common Errors

N/A

1.4.4 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.
- 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.
Command Mode	Global configuration mode
Usage Guide	N/A

Disabling ND Broadcast Isolation

- Optional.
- Configure this function if you want to broadcast ND packets to the CAPWAP tunnel interface.
- Configure this command in global configuration mode.

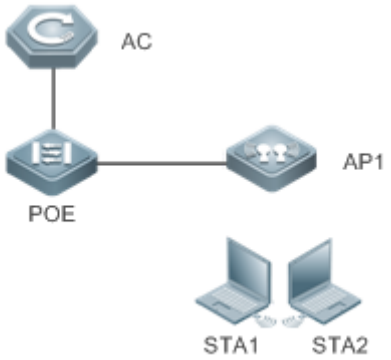
Command	**data-plane close-nd-filter** { **enable** | **disable** }
Parameter Description	**enable**: Allows ND packets to be broadcast to the CAPWAP tunnel interface. **disable**: Prevents ND packets from being broadcast to the CAPWAP tunnel interface.
Defaults	ND packets are not broadcast to the CAPWAP tunnel interface.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Disabling ARP Broadcast Isolation

Scenario **Figure 1-2**	
Configuration Steps	Disable ARP broadcast isolation in global configuration mode.
AC	`Hostname#configure terminal` `Hostname(config)#data-plane close-arp-filter enable`
Verification	Run the **show running-config** command to display the configuration.

AC	`Hostname# show running-config`
	`!`
	`cwmp`
	`!`
	`data-plane close-arp-filter enable`
	`!`

Common Errors

N/A

1.4.5 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.
- 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	**enable**: Allows mDNS packets to be forwarded to the air interface.

Description	**disable**: Prevents mDNS packets from being forwarded to the air interface.
Defaults	mDNS packets are not forwarded to the wireless network.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring SSDP Packet Control

- Optional.
- 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.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring OSPF Packet Control

- Optional.
- 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.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring VRRP Packet Control

- Optional.
- Configure this function if you want to allow VRRP packets to pass through.
- Configure this command in global configuration mode.

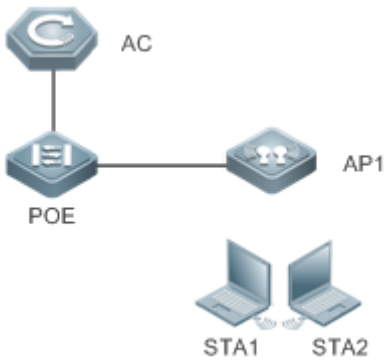
Command	**data-plane close-vrrp-filter** { **enable** | **disable** }
Parameter Description	**enable**: Allows VRRP packets to be forwarded to the air interface. **disable**: Prevents VRRP packets from being forwarded to the air interface.
Defaults	VRRP packets are not forwarded to the wireless network.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Configuring the Device to Allow OSPF Packets to Pass Through

Scenario **Figure 1-3**	
Configuration Steps	Configure the device to allow OSPF packets to pass through in global configuration mode.
AC	`Hostname#configure terminal` `Hostname(config)#data-plane close-ospf-filter enable`
Verification	Run the **show running-config** command to display the configuration.

AC	`Hostname# show running-config`
	`!`
	`cwmp`
	`!`
	`data-plane close-ospf-filter enable`
	`!`

Common Errors

N/A

1.4.6 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, 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*: Indicates the ID of the VLAN for which STA isolation is enabled. The value range is from 1 to 4094.
Defaults	STAs in a VLAN are not isolated by default.
Command Mode	AP group 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 group.

Configuring an Allowlist

Optional.

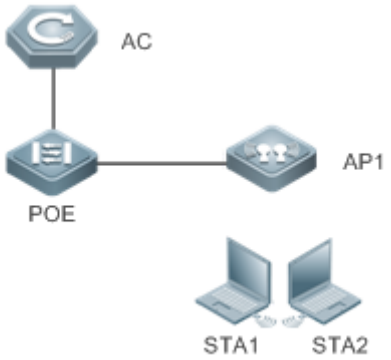
Command	**data-plane user-isolation** { **trusted-mac** *H.H.H* | **trusted-ip** *ipv4_address* } **vlan** *vid*
Parameter Description	*H.H.H*: Indicates the MAC address of a STA to be allowed to communicate with other STAs in the VLAN. *ipv4_address*: Indicates the IPv4 address of a STA to be allowed to communicate with other STAs in the VLAN. *vid*: Indicates the ID of the VLAN for which STA isolation is enabled.
Defaults	STAs in a VLAN are not isolated by default.
Command Mode	AP group configuration mode
Usage Guide	A maximum of 64 allowlists can be configured for intra-VLAN STA isolation on an AP group.

Verification

Run the **show data-plane user-isolation ap-group** *ap_group_name* 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 AP group configuration mode of the AC, add the STA whose MAC address is 0010.1111.2222 to the allowlist.

AC	`Hostname# configure terminal`
	`Hostname(config)# ap-group ap1`
	`Hostname(config-group)# data-plane user-isolation vlan 10`
	`Hostname(config-group)# data-plane user-isolation trusted-mac 0010.1111.2222 vlan 10`

Verification	Run the **show data-plane user-isolation ap-group** *ap_group_name* command to display the configuration.

AC	`Hostname# show show data-plane user-isolation ap-group ap1`
	`!`
	`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.

1.4.7 Configuring a Forwarding Policy for Broadcast or Multicast Packets

Configuration Effect

After this function is configured, the number of broadcast and multicast packets forwarded to wireless STAs will be reduced, alleviating the competition for air interface resources and improving network quality.

Notes

- N/A

Configuration Steps

↘ Disabling the Forwarding of Broadcast and Multicast Packets to Air Interfaces

- Optional.
- Configure this function to prevent all broadcast and multicast packets from being sent to wireless STAs.

Command	data-plane bcmc deny all
Parameter Description	N/A
Defaults	All broadcast and multicast packets can be forwarded.
Command Mode	Global configuration mode, AP configuration mode, or all-AP configuration mode
Usage Guide	On a large Layer 2 wireless network where numerous broadcast and multicast packets affect normal services, run this command to prevent all broadcast and multicast packets from being sent to air interfaces. To permit specified packets, configure the forwarding of broadcast and multicast packets of different types.

Disabling the Forwarding of Broadcast and Multicast Packets of Different Protocols

- Optional.
- All broadcast and multicast packets can be forwarded by default on the network.
- Configure this function to prevent specific broadcast and multicast packets from being forwarded on the network.

Command	**data-plan bcmc** { **arp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **ssdp** | **ospf** | **vrrp** | **igmp** | **mld** | **other-broadcast** | **other-multicast** } **disable**
Parameter Description	**disable**: Disables the forwarding of broadcast and multicast packets to air interfaces.
Defaults	All broadcast and multicast packets can be forwarded.
Command Mode	Global configuration mode, AP configuration mode, or all-AP configuration mode
Usage Guide	1. By default, all broadcast and multicast packets are allowed to be sent to air interfaces. 2. In a service scenario where only packets of a specified type need to be forwarded on the network, run the **data-pane bcmc deny all** command to disable the forwarding of all broadcast and multicast packets, and then enables the forwarding of specified packets. For example, in a scenario where only printers and speakers require support, run the **data-pane bcmc deny all** command to disable the forwarding of all packets, and then run the **no data-plane bcmc arp disable** and **no data-plane bcmc mdns disable** commands to enable the forwarding of ARP and MDNS packets. 3. In service scenarios where you need to disable the forwarding of broadcast and multicast packets of a specified type, run this command. If you need to disable the forwarding of SSDP packets, run the **data-plane bcmc ssdp disable** command**.** 4. The **other-broadcast** and **other-multicast** parameters indicates other broadcast or multicast packets not predefined in this command. 5. The forwarding configuration for all packets takes priority over the forwarding configuration for specific packets. For example, run the **data-plane bcmc deny arp disable** command to disable ARP packet forwarding, and then run the **no data-plane bcmc deny all** command to enable the forwarding of all broadcast and multicast packets so that ARP packets can be also forwarded. Or run the **data-plane bcmc deny all** command to disable the forwarding of broadcast and multicast packets, then run the **no data-plane bcmc deny arp disable** command to enable ARP packet forwarding, and then run the **data-plane bcmc deny all** command to prevent ARP packets from being forwarded.

Configuring a Rate Limit for Broadcast and Multicast Packets of Different Protocols

- Optional.
- Configure this function to limit the rate of broadcast or multicast packets of a specific protocol on the network.

Command	**data-plan bcmc** { **arp** | **nd** | **dhcp** | **dhcpv6** | **mdns** | **ssdp** | **ospf** | **vrrp** | **igmp** | **mld** | **other-broadcast** | **other-multicast** } **packets** *packets-rate*
Parameter Description	*packets-rate*: Indicates the rate limit, in pps. The value range is from 1 to 1000000.
Defaults	The rate limiting function for packet forwarding is disabled.
Command Mode	Global configuration mode, AP configuration mode, or all-AP configuration mode
Usage Guide	N/A

Configuring a Rate Limit for Broadcast and Multicast Packets of Different Types

- Optional.
- Configure this function to limit the rate of broadcast packets, multicast packets, unicast packets, unknown unicast packets, and unknown multicast packets on the network.

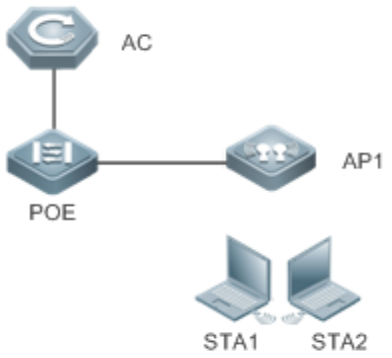
Command	**data-plan bcmc** { **broadcast** | **multicast** | **unicast** | **unknown-multicast** | **unknown-unicast** } **packets** *packets-rate*
Parameter Description	*packets-rate*: Indicates the rate limit, in pps. The value range is from 1 to 1000000.
Defaults	The rate limiting function for packet forwarding is disabled.
Command Mode	Global configuration mode, AP configuration mode, or all-AP configuration mode
Usage Guide	1. Supported packet types include broadcast, multicast, unicast, unknown unicast, and unknown multicast. 2. This function can be used together with the rate limiting function for broadcast and multicast packets of specified protocols to implement multi-level rate limit control. For example, the rate limit for broadcast packets is set to 1000 pps, and the rate limit for ARP packets is set to 200 pps.

Verification

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

Configuration Examples

Configuring a Forwarding Policy for Downstream Broadcast or Multicast Packets on Air Interfaces

Scenario	
Configuration Steps	1. On the AC, disable AP1 from forwarding downstream broadcast and multicast packets to the air interface. 2. Disable AP2 from forwarding downstream MDNS broadcast and multicast packet to the air interface. 3. Set the rate limit of downstream SSDP packets on the air interface of AP2 to 100 pps. **4.** Set the rate limit of broadcast packets for AP2 to 1000 pps.

AC	`Hostname(config)#ap-config AP1`
	`Hostname(config-ap)#data-plane bcmc deny all`
	`Hostname(config-ap)#exit`
	`Hostname(config)#ap-config AP2`
	`Hostname(config-ap)#data-plane bcmc mdns disable`
	`Hostname(config-ap)#data-plane bcmc ssdp packets 100`
	`Hostname(config-ap)#data-plane bcmc broadcast packets 1000`

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

AC	`Hostname# show ap-config running`
	`!`
	`cwmp`
	`!`
	`ap-config AP1`
	` data-plane bcmc arp disable`
	` data-plane bcmc nd disable`
	` data-plane bcmc dhcp disable`
	` data-plane bcmc dhcpv6 disable`
	` data-plane bcmc mdns disable`
	` data-plane bcmc ssdp disable`
	` data-plane bcmc igmp disable`
	` data-plane bcmc mld disable`
	` data-plane bcmc ospf disable`
	` data-plane bcmc vrrp disable`

	data-plane bcmc other-multicast disable data-plane bcmc other-broadcast disable ap-config AP2 data-plane bcmc mdns disable data-plane bcmc ssdp packets 100 data-plane bcmc broadcast packets 1000

Common Errors

N/A

1.4.8 Configuring Intelligent ARP Packet Forwarding

Configuration Effect

If the STA corresponding to the IP address in the ARP request packet is not connected to the AP, the AP determines that the STA is connected to another AP and discards the ARP request packet.

Notes

- To enable intelligent ARP packet forwarding, enable DHCP snooping first. Otherwise, other STAs and management devices cannot learn the MAC address of the current STA.
- User IP addresses must be obtained through DHCP. Currently, only IPv4 addresses are supported. If user IP addresses are not obtained through DHCP, user IP addresses need to be added to the intelligent ARP forwarding allowlist.
- The default gateway IP address needs to be configured for the DHCP address pool.
- Proxy ARP needs to be configured on the AC or AP.

Configuration Steps

↘ Configuring Intelligent ARP Packet Forwarding

- Optional.
- Configure this function for the AP to discard ARP broadcast packets of STAs that are not connected to the AP on the network.

Command	**data-plane bcmc smart arp forward**
Parameter Description	N/A
Defaults	This function is disabled. That is, ARP broadcast packets of STAs not connected to the AP are not discarded.
Command Mode	Global configuration mode, AP configuration mode, or all-AP configuration mode
Usage Guide	1. If the STA corresponding to the IP address in the ARP request packet is not connected to the AP, the AP determines that the STA is connected to another AP. In this case, the AP discards the ARP request packet.

	2. STA lookup is implemented through proxy ARP and DHCP snooping. If proxy ARP and DHCP snooping are not configured, enabling this function will cause other devices to fail to learn the MAC address of the STA. 3. Use IP addresses must be obtained through DHCP. If user IP addresses are not obtained through DHCP, you need to add them to the intelligent ARP forwarding allowlist.

Configuring an Allowlist for Intelligent ARP Packet Forwarding

- Optional.
- To forward the ARP request packet from the STA that is not connected to the AP, add the IP address of the STA to the the intelligent ARP forwarding allowlist.

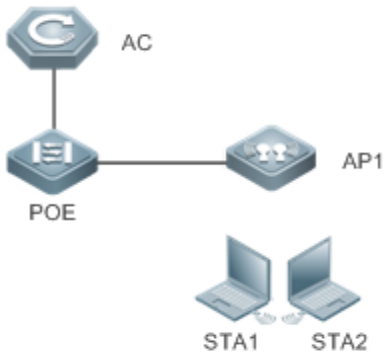
Command	**data-plane bcmc smart arp forward permit-ip**
Parameter Description	N/A
Defaults	No allowlist is configured.
Command Mode	Global configuration mode, AP configuration mode, or all-AP configuration mode
Usage Guide	1. To forward the ARP request packet from the STA that is not connected to the AP, add the IP address of the STA to the intelligent ARP forwarding allowlist. 2. Intelligent ARP packet forwarding takes effect only for users who obtain IP addresses through DHCP. To enable intelligent ARP packet forwarding for users with static IP addresses, add the user IP addresses to the intelligent ARP forwarding allowlist.

Verification

Run the **show running-config** and **show ap-config running** commands to display the configurations.

Configuration Examples

Configuring Intelligent ARP Packet Forwarding

Scenario	
Configuration Steps	● Configure DHCP snooping and proxy ARP on the AC. ● Configure intelligent ARP packet forwarding for AP1 on the AC.

AC	`Hostname(config)#ip dhcp snooping`
	`Hostname(config)#proxy-arp enable`
	`Hostname(config)#ap-config AP1`

	`Hostname(config-ap)#data-plane bcmc smart arp forward`
Verification	Run the **show running** and **show ap-config running** commands to display the configurations.

AC	`Hostname# show running`
	`!`
	`ip dhcp snooping`
	`proxy-arp enable`
	
	`Hostname# show ap-config running`
	`!`
	`cwmp`
	`!`
	`ap-config ap`
	`data-plane bcmc smart arp forward`

Common Errors

- Proxy ARP is not configured.
- The user IP address is not configured to be obtained through DHCP, and the user IP address is not added to the intelligent ARP forwarding allowlist.
- DHCP snooping is not enabled.

1.4.9 Configuring Intelligent DHCP Packet Forwarding

Configuration Effect

When a STA goes online, it sends a DHCP broadcast request packet that needs to be forwarded to the DHCP server, not to other STAs. Therefore, the AP does not need to forward the DHCP broadcast request packet over the air interface to prevent other wireless STAs from receiving the packet.

Some STAs require the DHCP server to respond to DHCP broadcast request packets. Therefore, DHCP broadcast response packets exist on the network. These packets need to be sent only to specific STAs. The AP intelligently identifies and checks the STA addresses in the received DHCP broadcast response packets.

- If the STA is connected to the AP, the AP converts the DHCP response packet into a unicast packet and sends it to the STA.
- If the STA is not connected to the AP, the AP discards the DHCP response packet.

Notes

- By default, the DHCP request packet from a wireless STA is not forwarded to other wireless STAs.
- By default, the DHCP broadcast packets replied by the DHCP server are converted into unicast packets for forwarding.

Configuration Steps

Configuring Intelligent DHCP Packet Forwarding

- Optional.
- Configure this function for the AP to intelligently discard broadcast packets replied by the DHCP server to STAs that are not connected to the AP.

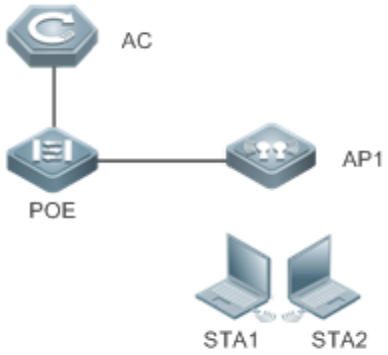
Command	data-plane bcmc smart dhcp forward
Parameter Description	N/A
Defaults	This function is disabled. That is, the AP does not discard broadcast packets replied by the DHCP server to STAs that are not connected to the AP.
Command Mode	Global configuration mode, AP configuration mode, or all-AP configuration mode
Usage Guide	N/A

Verification

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

Configuration Examples

Configuring Intelligent DHCP Packet Forwarding

Scenario	
Configuration Steps	• On the AC, disable AP1 from converting DHCP broadcast response packets into unicast packets for STAs. • On the AC, configure intelligent DHCP packet forwarding for AP1.
AC	`Hostname(config)#ap-config AP1` `Hostname(config-ap)#data-plane bcmc smart dhcp forward`
Verification	Run the **show ap-config running** command to display the configuration.

AC	`Hostname# show ap-config running`
	`!`
	`cwmp`
	`!`
	`ap-config ap`
	`data-plane bcmc smart dhcp forward`

Common Errors

N/A

1.5 Monitoring

Clearing

N/A

Displaying

Function	Command
show data-plane user-isolation { **summary** | **ap-group** *ap_group_name* }	Displays the configuration of intra-VLAN STA isolation.
show data-plane user-isolation state	Displays the allowlists configured for intra-VLAN STA isolation.

Debugging

N/A

1 Configuring Metric Monitoring

1.1 Overview

Metric monitoring 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
Metric Monitoring	Commands can be run to display and clear data of a specified metric on a specified device.

1.2.1 Metric Monitoring

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) It is used to 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	*group-name*: Indicates the name of a specified metric group.

Description	*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. 4. 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`
	`Hostname#`

Common Errors

N/A

1.4 Monitoring

Clearing

N/A

Displaying

Command	Description
show metrics define summary	Displays the summary of existing metrics.
show metrics define summary group *group-name*	Displays the summary of existing metrics in a specified metric group.
show metrics detail *group-name metrics-name*	Displays metric details.
show metrics summary	Displays the summary of all metrics.
show metrics summary group *group-name*	Displays the summary of all metrics in a specified metric group.

Debugging

N/A

Configuring Security

1. Configuring ACL
2. Configuring ARP Check
3. Configuring Gateway-targeted ARP Anti-spoofing
4. Configuring Global IP-MAC Binding
5. Configuring IP Source Guard
6. Configuring IPv6 Source Guard
7. Configuring CPP
8. Configuring NFPP
9. Configuring Password Policy
10. Configuring SSH

1 Configuring the ACL

1.1 Overview

An access control list (ACL) is also called access list. The ACL defines rules to determine whether to forward or drop data packets arriving at a network interface.

ACLs are classified into two types by function:

- Security ACLs: are used to control data flows that are allowed to pass through a network device.
- Quality of service (QoS) ACLs: are used to classify and process data flows by priority.

ACLs are typically used in the following situations:

- Network access control: To ensure network security, define rules to limit users' access to some services (for example, only access to web and email services is permitted, and access to other services such as Telnet is prohibited), to allow users to access services in a specified period of time, or to allow only specified hosts to access a network.
- QoS: QoS ACLs are used to preferentially classify and process important data flows. For details about QoS ACLs, see *Configuring QoS*.

1.2 Applications

Application	Description
Access Control of an Enterprise Network	On an enterprise network, network access rights of each department, for example, access rights of servers and use permissions of chatting tools such as Facebook Messenger, must be controlled as needed.

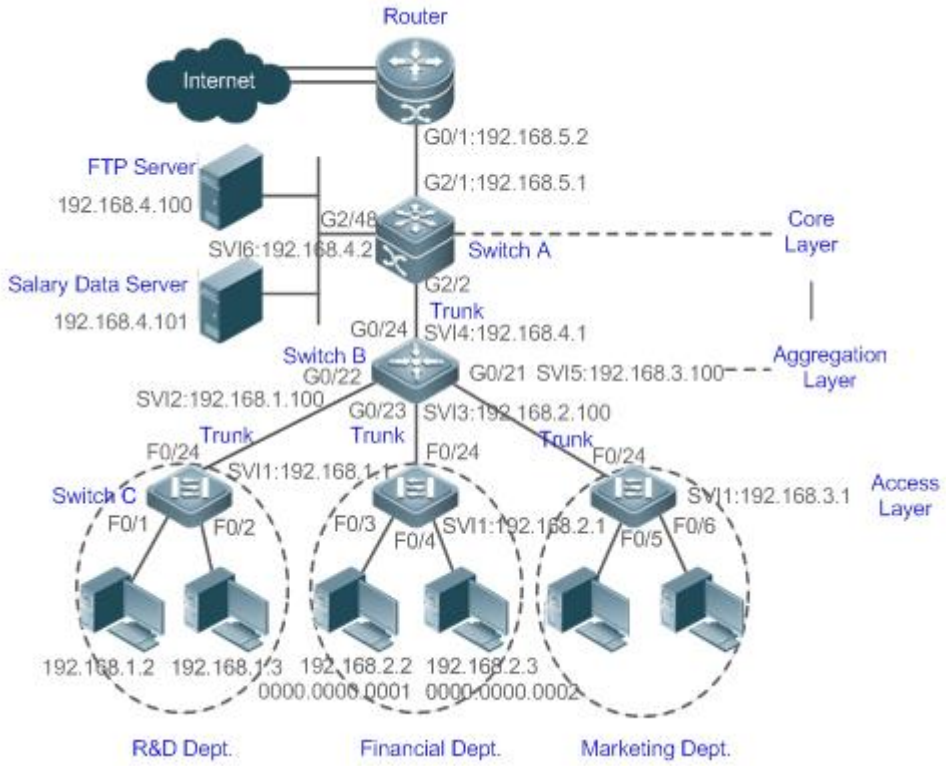
1.2.1 Access Control of an Enterprise Network

Scenario

Internet viruses can be found everywhere. Therefore, it is necessary to block interfaces that are often attacked by viruses to ensure security of an enterprise network:

- Allow only internal PCs to access the server.
- Prohibit PCs of a non-financial department from accessing PCs of the financial department, and prohibit PCs of a non-R&D department from accessing PCs of the R&D department.
- Prohibit the staff of the R&D department from using chatting tools such as Facebook Messenger during working hours from 09:00 to 18:00.

Figure 1-1



Remarks	Switch C at the access layer: is connected to PCs of each department and to Switch B at the aggregation layer through the 1000M optical fiber (trunk mode). Switch B at the aggregation layer: Is connected to the Switch A at the core layer through the 10GE optical fiber (trunk mode). Multiple virtual local area networks (VLANs) are divided, and a VLAN is allocated to each department. Switch A at the core layer: is connected to various servers, such as the File Transfer Protocol (FTP) server and Hypertext Transfer Protocol (HTTP) server, and to the Internet through firewalls.

Deployment

- Configure extended ACLs on G2/1 to filter data packets, protecting the network against viruses. This interface is located on Switch A and connects Switch A to G2/1 of a router.
- Allow only internal PCs to access servers, and prohibit external PCs from accessing servers. Define and apply the extended IP ACLs on G2/2 or switch virtual interface (SVI) 2 that is used to connect Switch A to an aggregation layer device or server.
- Prohibit mutual access between specified departments. Define and apply the extended IP ACLs on G0/22 and G0/23 of Switch B.
- Configure and apply the time-based extended IP ACLs on SVI 2 of Switch B to prohibit the R&D department from using chatting tools such as Facebook Messenger in a specified period of time.

1.3 Features

Basic Concepts

ACL

ACLs include basic and dynamic ACLs.

You can select basic or dynamic ACLs as required. In most situations, basic ACLs can meet security requirements. However, attackers may use certain software to access a network by means of IP address spoofing. If dynamic ACLs are used, users are requested to pass identify authentication before accessing a network, which prevents attackers from intruding the network. Therefore, you can use dynamic ACLs in some sensitive areas to guarantee network security.

ACLs cannot eliminate IP address spoofing. Attackers may use forged IP addresses to access a 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 for attackers to attack a network. The other is to encrypt network data using IP Security (IPsec), which ensures that all data is encrypted when arriving at a device.

ACLs are 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 interfaces

ACL statements must be executed in strict compliance with their sequence in the ACL. The device matches packets with the ACL starting 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 addresses can be specified, or the subnet can be used to define a type of data flows.)
- Destination IP address field (All destination IP addresses 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, both TCP source and destination ports are specified, or the range of the source or destination port is specified.
- Either a UDP source or destination port is specified, both UDP source and destination ports are specified, or the range of the source or destination port is specified.

Filtering fields refer to the fields in packets that can be used to identify or classify packets when an ACE is generated. A filtering field template is a combination of these fields. For example, when an ACE is generated, packets are identified and classified based on the destination IP address field in each packet; when another ACE is generated, packets are identified and classified based on the source IP address field and UDP source port field in each packet. The two ACEs use different filtering field templates.

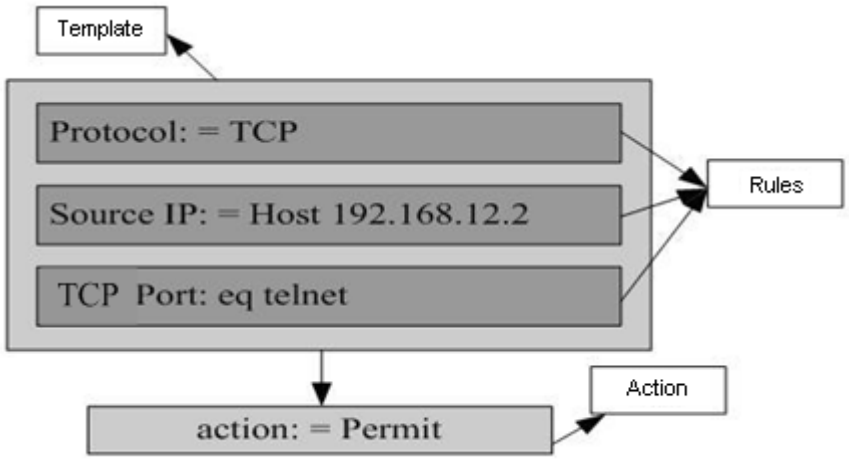
Rules refer to values of fields in the filtering field template of an ACE. For example, the content of an ACE is as follows.

```
permit tcp host 192.168.12.2 any eq telnet
```

In this ACE, the filtering field template is a combination of the following fields: source IP address field, IP protocol field, and TCP destination port field. The corresponding values (rules) are as follows:

- Source IP address = Host 192.168.12.2
- IP protocol = TCP
- TCP destination port = Telnet

Figure 1-2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet



- A filtering field template can be a combination of 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 outbound direction supports the standard IP, extended IP, extended MAC, and expert ACLs.
- If an extended MAC 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 a standard IP ACL, extended IP 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 subnet IP address range of VLAN 1 is 192.168.64.1 255.255.255.0, and an IP extended ACL is created and contains the ACE of **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 unicast and multicast packets but not unknown unicast packets. That is, such an ACL is ineffective for the unknown or broadcast packets.
- When the input 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 input 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 an expert ACL is configured and applied to the outbound direction of an interface, and some ACEs in this ACL contain Layer 3 matching information (for example, IP address and Layer 4 port), non-IP packets sent to the device from this interface cannot be controlled by the permit and deny ACEs in this ACL.
- If ACEs of an ACL (IP ACL or extended expert ACL) are configured to match non-Layer 2 fields (such as SIP and DIP), the ACL is invalid for tagged MPLS packets.

Overview

Feature	Description

Feature	Description
IP ACL	Control incoming or outgoing IPv4 packets of a device based on Layer 3 or Layer 4 information in the IPv4 packet header.
Extended MAC ACL	Control incoming or outgoing Layer 2 packets of a device based on Layer 2 information in the Ethernet packet header.
Extended Expert ACL	Combine the IP ACL and extended MAC 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 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 802.1X 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 configure the device to permit or deny specific IPv4 packets to control IP users' access to network resources.

Working Principle

Define a series of IP access rules in an IP ACL, and then apply the IP ACL in the inbound or outbound 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 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 is used to forward or block packets based on the source IP address, whereas the extended IP ACL 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 to the same ACL. However, more statements increase the difficulty in reading and understanding the ACL.

For routing products, the ICMP code field in an ACE is ineffective for ICPM packets whose ICPM type is 3. If the ICPM code of ICMP packets to be matched is configured in an ACE, the ACL matching result of incoming ICMP packets of a device whose ICPM type is 3 may be different from the expected result.

Implicit Statement of Deny All Traffic

At the end of every IP ACL is an implicit statement of deny all traffic. Therefore, if a packet does not match any rule, the packet will be denied.

Example:

```
access-list 1 permit host 192.168.4.12
```

This ACL permits only packets sent from the source host at 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, packets sent from any host will be denied when passing through this interface.

```
access-list 1 deny host 192.168.4.12
```

When defining an ACL, you must consider the routing update packets. As the implicit statement of deny all traffic 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 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 in which rule statements were 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.

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 subsequent rule statements any more.

Related Configuration

Configuring an IP ACL

By default, no IP ACL is configured on a device.

Run the **ip access-list** { **standard** | **extended** } { ***acl-name*** | ***acl-id*** } command in global configuration mode to create a standard or an extended IP ACL and enter the standard or extended IP ACL mode.

Adding ACEs to an IP ACL

By default, a created IP ACL contains an implicit ACE that denies all IPv4 packets. This ACE is hidden, but takes effect when the ACL is applied to an interface. That is, all IPv4 packets will be discarded. Therefore, if the device needs to receive or send some specific IPv4 packets, add some ACEs to the ACL.

For a standard IP ACL, add ACEs as follows:

- Regardless of whether the standard IP ACL is a named or numbered ACL, you can run the following command in standard IP ACL mode to add an ACE:

  [*sn*] { **permit** | **deny** } { **host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**url-group** *url-group-id*]

- For a numbered standard IP ACL, you can also run the following command in global configuration mode to add an ACE:

  access-list *acl-id* { **permit** | **deny** } { **host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*] [**url-group** *url-group-id*]

For an extended IP ACL, you can add ACEs as follows:

- Regardless of 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*] { **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*] [**url-group** *url-group-id*]

- 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* { **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*] [**url-group** *url-group-id*]

Applying an IP ACL

By default, an 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 Extended MAC 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 specific Layer 2 packets on 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 extended MAC ACL, and then apply the ACL to the inbound or outbound direction of an interface. The device checks whether the incoming or outgoing packets match the rules and accordingly forwards or blocks these packets.

To configure an extended MAC 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 extended MAC ACLs.

Protocol	ID Range
Extended MAC ACL	700–799

Typical rules defined in an extended MAC ACL include the following items:

- Source MAC address
- Destination MAC address
- Ethernet protocol type

The extended MAC ACL is used to filter packets based on the source or destination MAC address and the Ethernet type in the packets.

For an individual extended MAC ACL, define multiple independent ACL statements in multiple rules. All statements reference the same ID or name so that these statements are bound to the same ACL. However, more statements increase the difficulty in reading and understanding the ACL.

If ACEs in an extended MAC 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 extended MAC ACL does not filter IPv6 packets. To filter IPv6 packets, use the extended IPv6 ACL.

Implicit Rule Statement of Deny All Traffic

At the end of every extended MAC ACL is an implicit rule statement of deny all traffic. Therefore, if a packet does not match any rule, the packet will be denied.

Example:

```
access-list 700 permit host 00d0.f800.0001 any
```

This ACL permits only packets from the host with the MAC address of 00d0.f800.0001, and denies packets from all other hosts. This is because the following statement exists at the end of this ACL: **access-list 700 deny any any**.

Related Configuration

Configuring an Extended MAC ACL

By default, no extended MAC ACL is configured on a device.

Run the **mac access-list extended {*acl-name* | *acl-id* }** command in global configuration mode to create an extended MAC ACL and enter the extended MAC ACL mode.

Adding ACEs to an Extended MAC ACL

By default, a created extended MAC ACL contains an implicit ACE that denies all Layer 2 packets. This ACE is hidden, but takes effect when the ACL is applied to an interface. That is, all Layer 2 packets will be discarded. Therefore, if the device needs to receive or send some specific Layer 2 packets, add some ACEs to the ACL.

You can add ACEs to an extended MAC ACL as follows:

- Regardless of whether the extended MAC ACL is a named or numbered ACL, you can run the following command in MAC extended ACL mode to add an ACE:

  [*sn*] { **deny** | **permit** } { *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* **]**

- For a numbered MAC extended ACL, you can also run the following command in global configuration mode to add an ACE:

  access-list *acl-id* { **deny** | **permit** } { *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* **]**

Applying an Extended MAC ACL

By default, the extended MAC 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 an MAC extended ACL to a specified interface.

1.3.3 Extended Expert ACL

You can create an extended expert ACL to match Layer 2 and Layer 3 information in packets using the same rule. The extended expert ACL can be treated as a combination and enhancement of the IP ACL and extended MAC ACL because the extended expert ACL can contain ACEs in both the IP ACL and extended MAC ACL. In addition, the VLAN ID can be specified in the extended expert ACL to filter packets.

Working Principle

Define a series of access rules in the extended expert ACL, and then apply the ACL in the inbound or outbound 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 extended expert 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 extended expert ACL.

Protocol	ID Range
Extended expert ACL	2700–2899

When an extended expert 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 extended expert ACL include the following items:

- All information in the basic ACL and extended MAC ACL
- VLAN ID

The extended expert ACL is a combination of the basic ACL and extended MAC ACL, and can filter packets based on the VLAN ID.

For an individual extended expert ACL, define multiple independent statements in multiple rules. All statements reference the same ID or name so that these statements are bound to the same ACL.

If rules in an extended expert 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 Rule Statement of Deny All Traffic

At the end of every expert extended ACL is an implicit rule statement of deny all traffic. Therefore, if a packet does not match any rule, the packet will be denied.

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 Extended Expert ACL

By default, no extended expert ACL is configured on a device.

Run the **expert access-list extended** { ***acl-name*** | ***acl-id*** } command in global configuration mode to create an extended expert ACL and enter the extended expert ACL mode.

Adding ACEs to an Extended Expert ACL

By default, a created extended expert ACL contains an implicit ACE that denies all packets. This ACE is hidden, but takes effect when the ACL is applied to an interface. That is, all Layer 2 packets will be discarded. Therefore, if the device needs to receive or send some specific Layer 2 packets, add some ACEs to the ACL.

You can add ACEs to an extended expert ACL as follows:

- Regardless of whether the extended expert ACL is a named or numbered ACL, you can run the following command in extended expert ACL mode to add an ACE:

  [*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*]

- For an extended expert ACL with a numeric index, in addition to configuring an ACE by using the preceding command in extended MAC ACL mode, you can add an ACE to the extended expert ACL in configuration mode by using **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*].

Applying an Extended Expert ACL

By default, an extended expert ACL is not applied to any interface, that is, the created extended expert 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 extended expert 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 specific IPv6 packets on a network as needed to control IPv6 users' access to network resources.

Working Principle

Define a series of IPv6 access rules in an IPv6 ACL, and then apply the ACL in the inbound or outbound 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, extended MAC ACL, and extended expert ACL, you can specify only a name but not an ID for the IPv6 ACL.

Only one IP ACL, or one extended MAC ACL, or one extended expert ACL can be applied to the inbound or outbound direction of an interface. Besides, one more IPv6 ACL can be applied.

Implicit Rule Statement of Deny All Traffic

At the end of every IPv6 ACL is an implicit rule statement of deny all IPv6 traffic. Therefore, if a packet does not match any rule, the packet will be denied.

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 rule statement of deny all IPv6 traffic 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 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 in which rule statements were 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 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 the IPv6 ACL mode.

Adding ACEs to an IPv6 ACL

By default, a created IPv6 ACL contains an implicit ACE that denies all IPv6 packets. This ACE is hidden, but takes effect when the ACL is applied to an interface. That is, all IPv6 packets will be discarded. Therefore, if the device needs to receive or send some specific IPv6 packets, add some ACEs to the ACL.

Run the following command in IPv6 ACL mode to add an ACE:

[*sn*] { **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*]

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 matching some characteristics need to be not checked by access control applications. For example, before 802.1X authentication, users are allowed to log in to a specified website to download the 802.1X authentication client. The security channel can be used. When the security channel configuration command is executed to apply a secure ACL globally or to an interface, this ACL becomes a security channel.

Working Principle

The security channel is also an ACL, and can be configured globally or for a specified interface. When arriving at an interface, packets are checked on the security channel. If the packets meet matching conditions of the security channel, they enter a switch without access control, such as port security, web-based authentication, 802.1X, and IP+MAC binding check. A globally applied security channel takes effect on all interfaces except excluded 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 rule statement of deny all traffic at the end of the ACL. If packets do not meet matching conditions of the security channel, the device checks the packets against access control rules.
- You can configure up to eight excluded interfaces for the global security channel. In addition, you cannot configure interface-based security channel on these exclusive interfaces.
- If both interface-based migratable authentication mode and security channel are applied to an interface, the security channel does not take effect.
- An IPv6 ACL cannot be configured as a security channel.

Related Configuration

Configuring an ACL

Before configuring the security channel, configure an ACL. For details, see 1.3.1 IP ACL, 1.3.2 Extended MAC ACL, 1.3.3 Extended Expert ACL, or 1.3.4 IPv6 ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see 1.3.1 IP ACL, 1.3.2 Extended MAC ACL, 1.3.3 Extended Expert ACL, or 1.3.4 IPv6 ACL.

Configuring a Security Channel for an Interface

By default, no security channel is configured for an interface on a device.

Run the **security access-group** { *acl-id* | *acl-name* } command in interface configuration mode to configure a 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 Excluded Interface for the Global Security Channel

By default, no excluded 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 excluded interface of the global security channel.

1.4 Configuration

Configuration	Description and Command	
Configuring an IP ACL	⚠ (Optional) It is used to filter IPv4 packets.	
	ip access-list standard	Configures a standard IP ACL.
	ip access-list extended	Configures an extended IP ACL.
	permit host any time-range	Adds a permit ACE to a standard IP ACL.
	deny host any time-range	Adds a deny ACE to a standard IP ACL.
	permit host any host any 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.

Configuration	Description and Command	
	ip access-list resequence	Rearranges sequence numbers of ACEs for an IP standard or extended ACL.
Configuring an Extended MAC ACL	(Optional) It is used to filter Layer 2 packets.	
	mac access-list extended	Configures an extended MAC ACL.
	permit any host any host cos inner time-range	Adds a permit ACE to an extended MAC ACL.
	deny any host any host cos inner time-range	Adds a deny ACE to an extended MAC ACL.
	mac access-list resequence	Rearranges sequence numbers of ACEs for an extended MAC ACL.
	mac access-group in out	Applies an extended MAC ACL.
Configuring an Extended Expert ACL	(Optional) It is used to filter Layer 2 and Layer 3 packets.	
	expert access-list extended	Configures an extended expert ACL.
	permit cos inner VID inner host any host any host any host any precedence tos fragment range time-range	Adds a permit ACE to an extended expert ACL.
	deny cos inner VID inner host any host any host any host any precedence tos fragment range time-range	Adds a deny ACE to an extended expert ACL.
	expert access-list resequence	Rearranges sequence numbers of ACEs for an extended expert ACL.
	expert access-group in out	Applies an extended expert ACL.
Configuring an IPv6 ACL	(Optional) It is used to filter IPv6 packets.	
	ipv6 access-list	Configures an IPv6 ACL.
	permit host any host any range dscp flow-label fragment time-range	Adds a permit ACE to an IPv6 ACL.
	deny host any host any range dscp flow-label fragment time-range	Adds a deny ACE to an IPv6 ACL.
	ipv6 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 matching some characteristics not to be checked by access control applications, such as 802.1X and web-based authentication.	

Configuration	Description and Command	
	security access-group	Enables the security channel in interface configuration mode.
	security global access-group	Enables the security channel in global configuration mode.
	security uplinkenable	Configures an interface as the excluded interface of the global security channel in interface configuration mode.
Configuring ACEs Based on the Time Range	(Optional) It is used to configure an ACE based on the 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 global configuration mode.
	remark	Configures a comment for an ACE in ACL configuration mode.

1.4.1 Configuring an IP ACL

Configuration Effect

Configure and apply an IP ACL to an interface to control all incoming and outgoing IPv4 packets of this interface/VXLAN. 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 Step

↘ **Configuring an IP ACL**

- Mandatory. Configure an IP ACL to control access of IPv4 users to network resources.

- You can configure this ACL on an access device, an aggregation device, or a core device based on user distribution. 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 no ACE 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 interface so that the IP ACL can take effect.
- Based on user distribution, you can apply an extended IP ACL to a specified interface of the access, aggregation, or core device.
- Mandatory. You must apply an IP ACL to a specified interface so that the IP ACL can take effect.
- You can apply an IP ACL on a specified interface of the access, aggregation, or core device based on user distribution.

Verification

Use the following methods to verify the configuration 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 FTP resources on the network through FTP.

Related Commands

Configuring an IP ACL

Command	**ip access-list** { **standard** | **extended** } { *acl-name* | *acl-id* }
Parameter Description	**standard**: Indicates that a standard IP ACL is created. **extended**: Indicates that an extended IP ACL is created. *acl-id*: Indicates the ID that uniquely identifies a standard or extended IP ACL. If this parameter is specified, 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 parameter is specified, a named ACL is created. The value is a string of 1 to 99 characters. It cannot

	start with numerals (0–9), or cannot be **in** or **out**.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a standard or an extended IP ACL and enter the standard or extended IP ACL configuration mode. To control users' access to network resources by checking the source IP address of each packet, configure a standard IP ACL. To control users' access to network resources by checking the source or destination IP address, protocol number, and TCP/UDP source or destination port, configure an extended IP ACL.

Adding ACEs to an IP ACL

- Add ACEs to a standard IP ACL.

Use either of the following methods to add ACEs to a standard IP ACL.

Command	[*sn*] { **permit** | **deny** } { **host** *source* | **any** | *source source-wildcard* } [**time-range** *time-range-name*] [**url-group** *url-group-id*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value range is from 1 to 2,147,483,647. The sequence number determines the priority of the 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 ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a new ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. **url-group** *url-group-id*: Indicates that this ACE is associated with the URL group of a packet. For details about the URL group, see the configuration guide of application identification.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs in standard IP ACL configuration mode. The ACL can be a named or numbered ACL.

Command	**access-list** *acl-id* { **permit** | **deny** } { **host** *source* | **any** | *source source-wildcard* } [**time-range** *tm-rng-name*] [**url-group** *url-group-id*]

Parameter Description	*acl-id*: Indicates the ID of a numbered ACL. It uniquely identifies an ACL. The value range of *acl-id* is 100–199 and 1300–1999. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range. **url-group** *url-group-id*: Indicates that this ACE is associated with the URL group of a packet. For details about the URL group, see the configuration guide of application identification.
Command Mode	Standard IP ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in global configuration mode. It cannot be used to add ACEs to a named IP ACL.

- Add ACEs to an extended IP ACL.

Use either of the following methods to add ACEs to an extended IP ACL.

Command	[*sn*] { **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*] [**url-group** *url-group-id*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value range is from 1 to 2,147,483,647. The sequence number determines the priority of the 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 ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a new 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 range is from 0 to 255. To facilitate usage, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered.

	host *destination:* Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the **any** keyword is configured, IP packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **any**: Indicates that IP packets sent to or from any host are filtered. **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. **url-group** *url-group-id*: Indicates that this ACE is associated with the URL group of a packet. For details about the URL group, see the configuration guide of application identification.
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-name*] [**url-group** *url-group-id*]
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 range is from 1 to 2,147,483,647. The sequence number determines the priority of the 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 new 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 range is from 0 to 255. To facilitate usage, the system provides frequently-used abbreviations to replace the specific IP protocol numbers, including eigrp, gre, icmp, igmp, ip, ipinip, nos, ospf, tcp, and udp. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *destination:* Indicates that IP packets sent to a host with the specified destination IP address are filtered. If the **any** keyword is configured, IP packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **any**: Indicates that IP packets sent to or from any host are filtered. **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. **url-group** *url-group-id*: Indicates that this ACE is associated with the URL group of a packet. For details about the URL group, see the configuration guide of application identification.
Command Mode	Extended IP ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered IP ACL in extended IP ACL configuration mode. It cannot be used to add ACEs to a named extended IP ACL.

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 standard or extended IP ACL. *acl-name*: Indicates the named standard or extended IP 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 standard or extended IP 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.

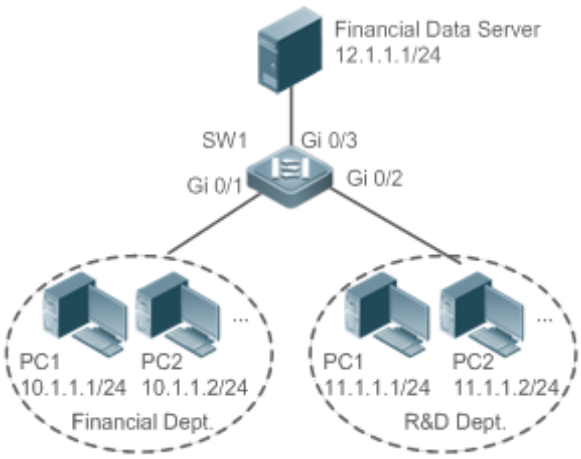
Applying an IP ACL

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. **reflect:** Indicates that the reflexive ACL is enabled.
Command Mode	Interface configuration mode
Usage Guide	This command makes an IP ACL take effect on the incoming or outgoing packets of a specified interface.

Configuration Example

The following configuration example describes only ACL-related configurations.

Configuring an IP ACL to Prohibit Departments Except the Financial Department from Accessing the Financial Data Server

Scenario Figure 1-3	
Configuration Steps	● Configure an IP ACL. ● Add ACEs to the IP ACL. ● Apply the IP ACL to the outbound direction of the interface connected to the financial data server.
SW1	`sw1(config)#ip access-list standard 1`

	sw1(config-std-nacl)#permit 10.1.1.0 0.0.0.255 sw1(config-std-nacl)#deny 11.1.1.1 0.0.0.255 sw1(config-std-nacl)#exit sw1(config)#int gigabitEthernet 0/3 sw1(config-if-GigabitEthernet 0/3)#ip access-group 1 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.
SW1	sw1(config)#show access-lists ip access-list standard 1 10 permit 10.1.1.0 0.0.0.255 20 deny 11.1.1.0 0.0.0.255 sw1(config)#show access-group ip access-group 1 out Applied On interface GigabitEthernet 0/3

1.4.2 Configuring an Extended MAC ACL

Configuration Effect

Configure and apply an extended MAC ACL to an interface to control all incoming and outgoing IPv4 packets of this interface. You can permit or deny specific Layer 2 packets on a network to control users' access to network resources based on Layer 2 packets.

Notes

N/A

Configuration Step

↘ **Configuring an Extended MAC ACL**

- Mandatory. Configure an extended MAC 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 device, an aggregation device, or a core device based on user distribution. The MAC extended ACL takes effect only on the local device, and does not affect other devices on the network.

Adding ACEs to an Extended MAC ACL

- Optional. An ACL may contain no ACE or multiple ACEs. If no ACE is configured, all incoming L2 Ethernet 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 Extended MAC ACL

- Mandatory. Apply an extended MAC ACL to a specified interface to make the ACL take effect.
- You can apply an extended MAC ACL on a specified interface of an access device, an aggregation device, or a core device based on user distribution.

Verification

Use the following methods to verify the configuration of the extended MAC ACL:

- If an extended MAC ACL is configured to permit or deny some IP packets, run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, an extended MAC ACL is configured to prevent a device interface from receiving IP packets (Ethernet type is 0x0800), run the **ping** command for verification.
- If an extended MAC ACL is configured to permit or deny some non-IP packets such as ARP packets, 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 matching some specified characteristics to check whether the extended MAC ACL takes effect. Typically, prepare two PCs, construct and send Layer 2 packets on one PC, enable packet obtaining on another PC, and check whether packets are forwarded as expected (forwarded or blocked) according to the action specified in the ACEs.

Related Commands

Configuring an Extended MAC ACL

Command	**mac access-list extended** { *acl-name* | *acl-id* }
Parameter Description	*acl-name*: Indicates the name of an extended MAC ACL. If this parameter is specified, a named ACL is created. The value is a string of 1 to 99 characters. It cannot start with numerals (0–9), or cannot be **in** or **out**. *acl-id*: Indicates the ID that uniquely identifies an MAC extended ACL. If this parameter is specified, a numbered ACL is created. The value range of *acl-id* is 700–799.
Command	Global configuration mode

Mode	
Usage Guide	Run this command to configure an extended MAC ACL and enter the extended MAC ACL configuration mode. You can configure an extended MAC ACL to control users' access to network resources by checking Layer 2 information of Ethernet packets.

Adding ACEs to an Extended MAC ACL

Use either of the following methods to add ACEs to an extended MAC ACL:

- Add ACEs in extended MAC 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 range is from 1 to 2,147,483,647. The sequence number determines the priority of the 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 ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a new 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-addr*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. *source-mac-mask*: Indicates that bits of the source MAC address are inverted. **any**: Indicates that Layer 2 packets sent to any host are filtered. **host** *destination-mac-addr*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. *destination-mac-mask*: Indicates that bits of the destination MAC address are inverted. *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.
Command Mode	Extended MAC ACL configuration mode
Usage Guide	Run this command to add ACEs in extended MAC ACL configuration mode. The ACL can be a named or numbered ACL.

- Add ACEs to an extended MAC ACL in global configuration mode.

Command	**access-list** *acl-id* { **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	*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-addr*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. *source-mac-mask*: Indicates that bits of the source MAC address are inverted. **any**: Indicates that Layer 2 packets sent to any host are filtered. **host** *destination-mac-addr*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. *destination-mac-mask*: Indicates that bits of the destination MAC address are inverted. *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.
Command Mode	Global configuration mode
Usage Guide	Run this command to add ACEs to a numbered extended MAC ACL in global configuration mode. It cannot be used to add ACEs to a named extended MAC 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 extended MAC ACL. *acl-name*: Indicates the named extended MAC 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 extended MAC 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 Extended MAC ACL

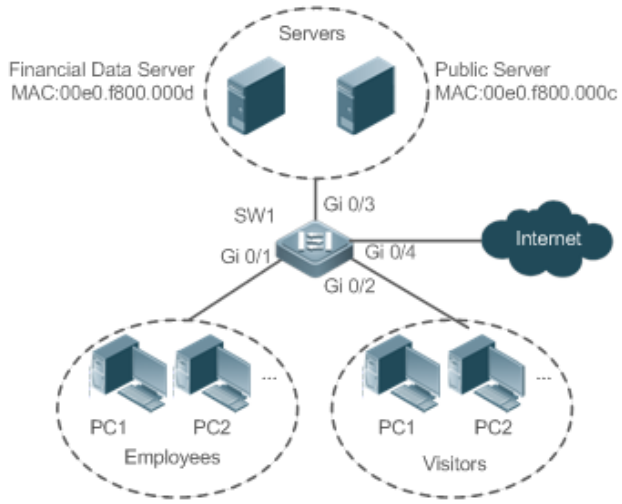
Command	**mac access-group** { *acl-id* | *acl-name* } { **in** | **out** }
Parameter Description	*acl-id*: Indicates that a numbered extended MAC ACL will be applied to the interface. *acl-name*: Indicates that a named extended MAC ACL will be applied to the interface. **in**: Indicates that this ACL 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 extended MAC 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 Extended MAC ACL to Restrict Resources Accessed by Guests

Scenario Figure 1-4	
Configuration Steps	● Configure an extended MAC ACL. ● Add ACEs to the extended MAC ACL. ● Apply the extended MAC ACL to the outbound direction of the interface connected to the guest area so that guests 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 of 00e0.f800.000d.

SW1	`sw1(config)#mac access-list extended 700`
	`sw1(config-mac-nacl)#deny any host 00e0.f800.000d`
	`sw1(config-mac-nacl)#permit any any`
	`sw1(config-mac-nacl)#exit`
	`sw1(config)#int gigabitEthernet 0/2`
	`sw1(config-if-GigabitEthernet 0/2)#mac access-group 700in`

Verification	● On a guest's PC, ping the financial data server. Verify that the ping operation fails. ● On a guest's PC, ping the public resource server. Verify that the ping operation

	succeeds. ● On a guest's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.

SW1	`sw1(config)#show access-lists`
	`mac access-list extended 700`
	` 10 deny any host 00e0.f800.000d etype-any`
	`20 permit any any etype-any`
	`sw1(config)#show access-group`
	`mac access-group 700in`
	`Applied On interface GigabitEthernet 0/2`

1.4.3 Configuring an Extended Expert ACL

Configuration Effect

Configure and apply an extended expert ACL to an interface to control incoming and outgoing packets of the interface based on Layer 2 and Layer 3 information, and allow or prohibit specific packets on a network. In addition, you can configure an extended expert 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. Typically, you can use an extended expert ACL if you want to incorporate ACEs of the IP ACL and MAC extended ACL into one ACL.

Configuration Step

↘ **Configuring an Extended Expert ACL**

- Mandatory. Configure an extended expert ACL if you want to control users' access to network resources based on the Layer 2 packet header, for example, VLAN ID.
- You can configure this ACL on an access device, an aggregation device, or a core device based on user distribution. The extended expert ACL takes effect only on the local device, and does not affect other devices on the network.

↘ **Adding ACEs to an Expert Extended ACL**

- Optional. An ACL may contain no ACE or multiple ACEs. If no ACE is configured, all incoming 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 Extended Expert ACL**

- Mandatory. Apply an extended expert ACL to a specified interface to make this ACL take effect.
- You can apply an extended expert ACL in the inbound or outbound direction of a specified interface of an access device, an aggregation device, or a core device based on user distribution.

Verification

Use the following methods to verify the configuration of the extended expert ACL:

- Use the following methods to verify the configuration of the expert extended ACL:
- If IP address-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 address-based access rules are configured in an expert extended ACL to permit or deny some L2 packets (e.g. ARP packets), also run the **ping** command to check whether ACEs of this ACL takes effect on the specified interface. For example, to filter out ARP packets, run the **ping** command for verification.
- If VLAN ID-based access rules are configured in an expert extended ACL to permit or deny some L2 packets in some network segments (e.g., to prevent communication between VLAN 1 users and VLAN 2 users), ping PCs of VLAN 2 on a PC of VLAN 1. If the ping operation fails, the rules take effect.

Related Commands

Configuring an Expert Extended ACL

Command	**expert access-list extended** { *acl-name* | *acl-id* }
Parameter Description	*acl-name*: Indicates the name of an expert extended ACL. If this parameter is specified, a named ACL is created. The value is a string of 1 to 99 characters. It cannot start with numerals (0–9), or cannot be **in** or **out**. *acl-id*: Indicates the ID of an extended expert ACL. If this parameter is specified, a numbered ACL is created. The value range of *acl-id* is 2700-2899.
Command Mode	Configuration mode
Usage Guide	Run this command to configure an extended expert ACL and enter the extended expert ACL configuration mode.

Adding ACEs to an Extended Expert ACL

Use either of the following methods to add ACEs to an extended expert ACL:

- Add ACEs in extended expert ACL configuration mode.

Command	[*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*]
Parameter Description	*sn*: Indicates the sequence number of an ACE. The value range is from 1 to 2,147,483,647. The sequence number determines the priority of the 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 ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a new 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 usage, 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** *cos*: Indicates that Layer 2 packets with the specified cos field in the outer tag are filtered. **inner cos** *in*: Indicates that Layer 2 packets with the specified cos field in the inner tag are filtered. **VID** *vid*: Indicates that Layer 2 packets with the specified VLAN ID field in the outer tag are filtered. **inner** *vid*: Indicates that Layer 2 packets with the specified VLAN ID field in the inner tag are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that Layer 2 packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified IP network segment are filtered. **host** *destination*: Indicates that IP packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IP packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. **any**: Indicates that 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. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range.
Command Mode	Extended expert ACL configuration mode
Usage Guide	Run this command to add ACEs in extended expert ACL configuration mode. The ACL can be a named or numbered ACL.

- Add ACEs to an extended expert ACL in global configuration mode.

Command	**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*]
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 usage, 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** *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. **VID** *vid*: Indicates that Layer 2 packets with the specified VLAN ID field in the outer tag are filtered. **inner** *vid*: Indicates that Layer 2 packets with the specified VLAN ID field in the inner tag are filtered. *source source-wildcard:* Indicates that IP packets sent from hosts in the specified IP network segment are filtered. **host** *source*: Indicates that IP packets sent from a host with the specified source IP address are filtered. **any**: Indicates that IP packets sent from any host are filtered. **host** *source-mac-address*: Indicates that IP packets sent from a host with the specified source MAC address are filtered. **any**: Indicates that Layer 2 packets sent to any host are filtered. *destination destination-wildcard:* Indicates that IP packets sent to hosts in a specified

	IP network segment are filtered. **host** *destination*: Indicates that IP packets sent to a host with the specified destination IP address are filtered. **any**: Indicates that IP packets sent to any host are filtered. **host** *destination-mac-address*: Indicates that IP packets sent to a host with the specified destination MAC address are filtered. **any**: Indicates that 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. **time-range** *time-range-name:* Indicates that this ACE is associated with a time range. The ACE takes effect only within this time range.
Command Mode	Extended expert ACL configuration mode
Usage Guide	Run this command to add ACEs to a numbered extended expert ACL in global configuration mode. It cannot be used to add ACEs to a named extended expert 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 extended expert ACL. *acl-name*: Indicates the named extended expert 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 extended expert 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 Extended Expert ACL

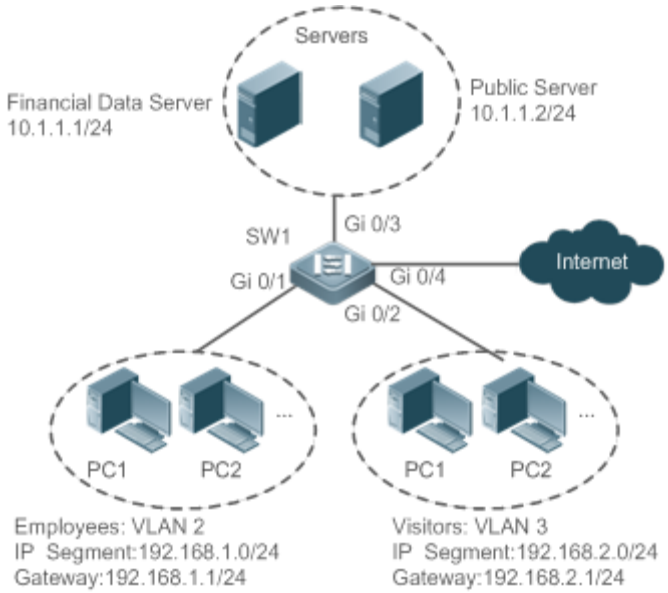
Command	**expert access-group** { *acl-id* **|** *acl-name* } { **in** | **out** }
Parameter Description	● *acl-id*: Indicates that a numbered extended expert ACL will be applied to the interface. ● *acl-name*: Indicates that a named extended expert ACL will be applied to the interface. ● **in**: Indicates that this ACL controls incoming L2 packets of the interface. ● **out**: Indicates that this ACL controls outgoing L2 packets of the interface.
Command	Interface configuration mode

Mode	
Usage Guide	This command makes an extended expert 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 Extended Expert ACL to Restrict Resources Accessed by Guests (Guests and Employees Cannot Communicate with Each Other, and Guests Can Access the Public Server but Not the Financial Data Server of the Company)

Scenario Figure 1-5	
Configuration Steps	● Configure an extended expert ACL. ● Add an ACE to deny packets sent from PCs in the guest area (VLAN 3) to employee PCs in VLAN 2. ● Add an ACE to prevent guests from accessing the financial data server of the company. ● Add an ACE to permit all packets. ● Apply the ACL to the inbound direction of the interface of the switch that connects to the guest area.

SW1	`sw1(config)#expert access-list extended 2700`
	`sw1(config-exp-nacl)#deny ip any any 192.168.1.0 0.0.0.255 any`
	`sw1(config-exp-nacl)#deny ip any any host 10.1.1.1 any`
	`sw1(config-exp-nacl)#pemit any any any any`
	`sw1(config-exp-nacl)#exit`
	`sw1(config)#int gigabitEthernet 0/2`

	`sw1(config-if-GigabitEthernet 0/2)#expert access-group 2700 in`
Verification	● On a guest's PC, ping the financial data server. Verify that the ping operation fails. ● On a guest's PC, ping the public server. Verify that the ping operation succeeds. ● On a guest's PC, ping the gateway address 192.168.1.1 of an employee. Verify that the ping operation fails. ● On a guest's PC, access the Internet, for example, visit the Baidu website. Verify that the webpage can be opened.

SW1	`sw1(config)#show access-lists`
	`expert access-list extended 2700`
	` 10 deny ip any any 192.168.1.0 0.0.0.255 any`
	`20 deny ip any any host 10.1.1.1 any`
	` 30 permit ip any any any any`
	
	`sw1(config)#show access-group`
	`expert access-group 2700 in`
	`Applied On interface GigabitEthernet 0/2`

1.4.4 Configuring an IPv6 ACL

Configuration Effect

Configure and apply an IPv6 ACL to an interface to control all incoming and outgoing IPv6 packets of this interface. You can permit or deny specific IPv6 packets on a network to control IPv6 users' access to network resources.

Configuration Step

↘ Configuring an IPv6 ACL

- Mandatory. Configure an IP ACL to control IPv4 users' access to network resources.
- You can configure this ACL on an access device, an aggregation device, or a core device based on user distribution. The IPv6 ACL takes effect only on the local device, and does not affect other devices on the network.

↘ Adding ACEs to an IPv6 ACL

- Optional. An ACL may contain no ACE or multiple ACEs. If no ACE is configured, all incoming IPv6 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 IPv6 ACL

- Mandatory. Apply an IPv6 ACL to a specified interface on a device to make this ACL take effect.
- You can apply an IPv6 ACL on a specified interface/VXLAN of an access device, an aggregation device, or a core device based on user distribution.

Verification

Use the following methods to verify the configuration 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 ACL. If this parameter is specified, a named ACL is created. The value is a string of 1 to 99 characters. It cannot start with numerals (0–9), or cannot be **in** or **out**.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an IPv6 ACL and enter the 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 range is from 1 to 2,147,483,647. The sequence number determines the priority of the 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 ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a new ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *ipv6-protocol*: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate usage, 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. **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 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 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 TCP or UDP packets with the Layer destination port number in the specified range 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.
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. The sequence number determines the priority of the 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 ACL. For example, if the sequence number of the last ACE is 100, the sequence number of a new ACE will be 110 by default. You can adjust the increment using a command. **permit**: Indicates that the ACE is a permit ACE. **deny**: Indicates that the ACE is a deny ACE. *ipv6-protocol*: Indicates the IPv6 protocol number. The value ranges from 0 to 255. To facilitate usage, 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.
Command Mode	IPv6 ACL configuration mode
Usage Guide	Run this command to add ACEs in IPv6 ACL configuration mode.

↘ Rearranging Sequence Numbers of ACE

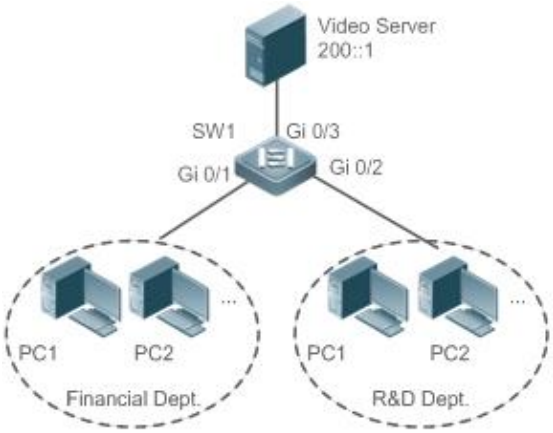
Command	**ipv6 access-list resequence** *acl-name start-sn inc-sn*
Parameter Description	*acl*-name: Indicates the IPv6 ACL name. *start-sn*: Indicates that the start value of the sequence number is configured. *inc-sn*: Indicates that the sequence number increment is configured.
Command Mode	Global 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 1-6	
Configuration Steps	● Configure an IPv6 ACL. ● Add an ACE to the IPv6 ACL to prevent access to the video server. ● Add an ACE to the IPv6 ACL to permit all IPv6 packets. ● Apply the IPv6 ACL to the incoming direction of the interface connected to the R&D department.

SW1	`sw1(config)#ipv6 access-list dev_deny_ipv6video`
	`sw1(config-ipv6-nacl)#deny ipv6 any host 200::1`
	`sw1(config-ipv6-nacl)#permit ipv6 any any`
	`sw1(config-ipv6-nacl)#exit`
	`sw1(config)#int gigabitEthernet 0/2`
	`sw1(config-if-GigabitEthernet 0/2)# ipv6 traffic-filter dev_deny_ipv6videoin`

Verification	● On a PC of the R&D department, ping the video server. Verify that the ping operation fails.
SW1	`sw1(config)#show access-lists`

	ipv6 access-list dev_deny_ipv6video 10 deny ipv6 any host 200::1 20 permit ipv6 any any sw1(config)#show access-group ipv6 traffic-filter dev_deny_ipv6video in Applied On interface GigabitEthernet 0/2

1.4.5 Configuring a Security Channel

Configuration Effect

Configure a security channel to enable packets matching the security channel rules not to be checked by access control applications. Configure the security channel if an access control application (such as 802.1X) is enabled on an uplink interface of a user, but the user should be allowed to log in to a website to download some resources (for example, downloading the authentication client) before 802.1X authentication.

Configuration Step

↘ Configuring an ACL

- Mandatory. Configure an ACL before configuring the security channel.
- You can configure this ACL on an access device, an aggregation device, or a core device based on user distribution. 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 no ACE or multiple ACEs. If no ACE is configured for an ACL, the security channel does not take effect.

↘ Configuring a Security Channel on a Specified Interface or Globally

- Configure a security channel on an interface to make this security channel take effect on the interface. Configure a global security channel to make this security channel take effect globally. You must configure the interface-based or global security channel.
- You can configure a security channel on an access device, an aggregation device, or a core device based on user distribution.

Configuring an Excluded Interface for the Global Security Channel

- Optional. Configure an interface as the excluded interface for the global security channel if the global security channel is required not to take effect on this interface.

Configuring an Access Control Application

- Optional. You can enable 802.1X or web-based authentication to verify the security channel function.
- You can configure the access control function on an access device, an aggregation device, or a core device based on user distribution.

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 be not checked by 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 1.3.1 IP ACL, 1.3.2 Extended MAC ACL, 1.3.3 Extended Expert ACL, or 1.3.4 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	Global configuration mode

Mode	
Usage Guide	Run this command to configure the specified ACL as the global security channel.

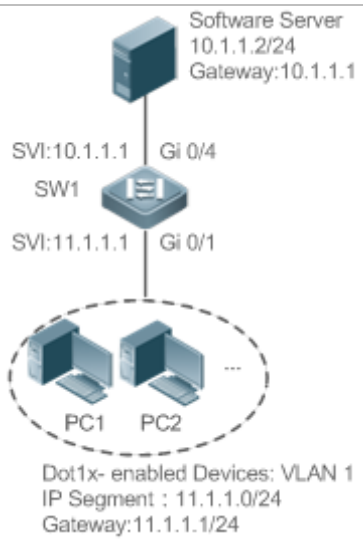
Configuring an Excluded Interface for the Global Security Channel

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 excluded 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 extended expert ACL named **exp_ext_esc**. ● Add an ACE to allow packets to the destination host at 10.1.1.2. ● Add an ACE to permit DHCP packets. ● Add an ACE to permit ARP packets. ● On the interface where 802.1X authentication is enabled, configure the ACL **exp_ext_esc** as the security channel.

SW1	`sw1(config)#expert access-list extendedexp_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 departments 1 and 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 ACEs Based on the Time Range

Configuration Effect

Configure the time range for ACEs to make the ACEs take effect or to become invalid in a specified period of time.

Configuration Step

↘ **Configuring an ACL**

- Mandatory. Configure an ACL before configuring ACEs based on the time range.

- You can configure this ACL on an access device, an aggregation device, or a core device based on user distribution. 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.

Applying an ACL

- Mandatory. Apply the ACL to a specified interface to make ACEs take effect in the specified time range.
- You can apply an IP ACL on a specified interface of an access device, an aggregation device, or a core device based on user distribution.

Verification

In the time range during which 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 on how to configure an ACL, see 1.3.1 IP ACL, 1.3.2 Extended MAC ACL, 1.3.3 Extended Expert ACL, or 1.3.4 IPv6 ACL.

Adding an ACE with the Time Range Specified

For details on how to configure an ACE, see 1.3.1 IP ACL, 1.3.2 Extended MAC ACL, 1.3.3 Extended Expert ACL, or 1.3.4 IPv6 ACL.

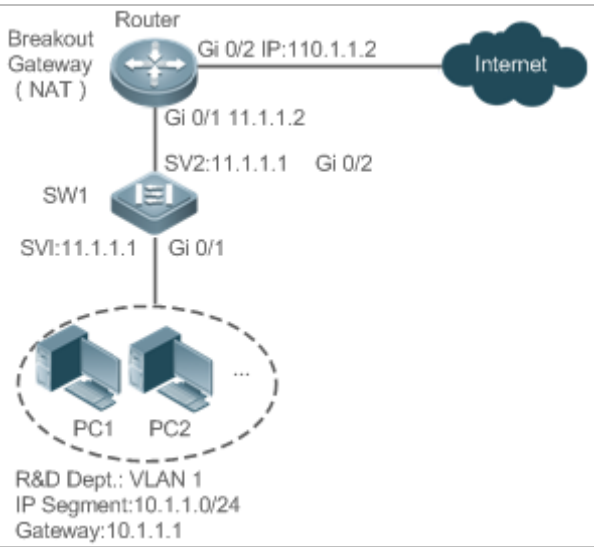
Applying an ACL

For details on how to apply an ACL, see 1.3.1 IP ACL, 1.3.2 Extended MAC ACL, 1.3.3 Extended Expert ACL, or 1.3.4 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 14-8**	
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 named **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 outbound direction of the interface connected to the egress gateway.

SW1	`Hostname(config)# time-range access-internet`
	`Hostname(config-time-range)# periodic daily 12:00 to 13:30`
	`Hostname(config-time-range)# exit`
	`sw1(config)# ip access-list standard ip_std_internet_acl`
	`sw1(config-std-nacl)# permit 10.1.1.0 0.0.0.255 time-range access-internet`
	`sw1(config-std-nacl)# deny 10.1.1.0 0.0.0.255`
	`sw1(config-std-nacl)# permit any`
	`sw1(config-std-nacl)# exit`
	`sw1(config)#int gigabitEthernet 0/2`
	`sw1(config-if-GigabitEthernet 0/2)# ip access-group ip_std_internet_acl 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.

SW1	`sw1#show time-range`
	
	`time-range entry: access-internet (inactive)`
	`  periodic Daily 12:00 to 13:30`
	
	`sw1#show access-lists`
	
	`ip access-list standard ip_std_internet_acl`
	` 10 permit 10.1.1.0 0.0.0.255 time-range access-internet (inactive)`
	` 20 deny 10.1.1.0 0.0.0.255`
	` 30 permit any`
	
	`sw1#show access-group`
	`ip access-group ip_std_internet_acl out`
	`Applied On interface GigabitEthernet 0/2`

1.4.7 Configuring Comments for ACLs

Configuration Effect

During network maintenance, if many ACLs are configured without any comments, it is difficult to distinguish these ACLs. You can configure comments for ACLs to better understand usage of ACLs.

Configuration Step

↘ **Configuring an ACL**

- Mandatory. Configure an ACL before configuring a security channel.
- You can configure this ACL on an access device, an aggregation device, or a core device based on user distribution. 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 no ACE or multiple ACEs. If no ACE is configured, the security channel does not take effect.

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 1.3.1 IP ACL, 1.3.2 Extended MAC ACL, 1.3.3 Extended Expert ACL, or 1.3.4 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 Mode	Configuration mode
Usage Guide	Run this command to configure the comment for a specified ACL.

Adding ACEs to an ACL

For details about how to add ACEs to an ACL, see 1.3.1 IP ACL, 1.3.2 Extended MAC ACL, 1.3.3 Extended Expert ACL, or 1.3.4 IPv6 ACL.

Configuring Comments for ACEs

Use either of the following two methods to configure a comment for an ACE.

Command	**remark** *comment*
Parameter Description	*comment*: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	ACL configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE. If *sn* is not configured, the comment is configured for the last ACE.

Command	**access-list** *acl-id* [*sn*] **remark** *comment*
Parameter Description	*acl-id*: Indicates the ID of an ACL. *sn*: Indicates the sequence number of an ACE for which a comment is required. *comment*: Indicates the comment. The value is a string of 1 to 100 characters. A comment longer than 100 characters will be truncated to 100 characters.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure the comment for a specified ACE. If *sn* is not configured, the comment is configured for the last ACE.

1.5 Monitoring

Clearing

Command	Description
clear counters access-list [*acl-id* | *acl-name*]	Clears the ACL packet matching counters.
clear access-list counters [*acl-id* | *acl-name*]	Clears statistics on denied packets.

Displaying

Command	Description
show access-lists [*acl-id* | *acl-name*] [**summary**]	Displays basic ACLs.
show access-group [**interface** *interface-name*] | **wlan** *wlan-id*	Displays the ACL applied to an interface.
show ip access-group [**interface** *interface-name* | **wlan** *wlan-id*]	Displays the IP ACL applied to an interface.
show mac access-group [**interface** *interface-name*| **wlan** *wlan-id*]	Displays the extended MAC ACL applied to an interface.

show expert access-group [**interface** *interface-name* | **wlan** *wlan-id*]	Displays the extended expert ACL applied to an interface.
show ipv6 traffic-filter [**interface** *interface-name*]	Displays the IPv6 ACL applied to an interface.

Debugging

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

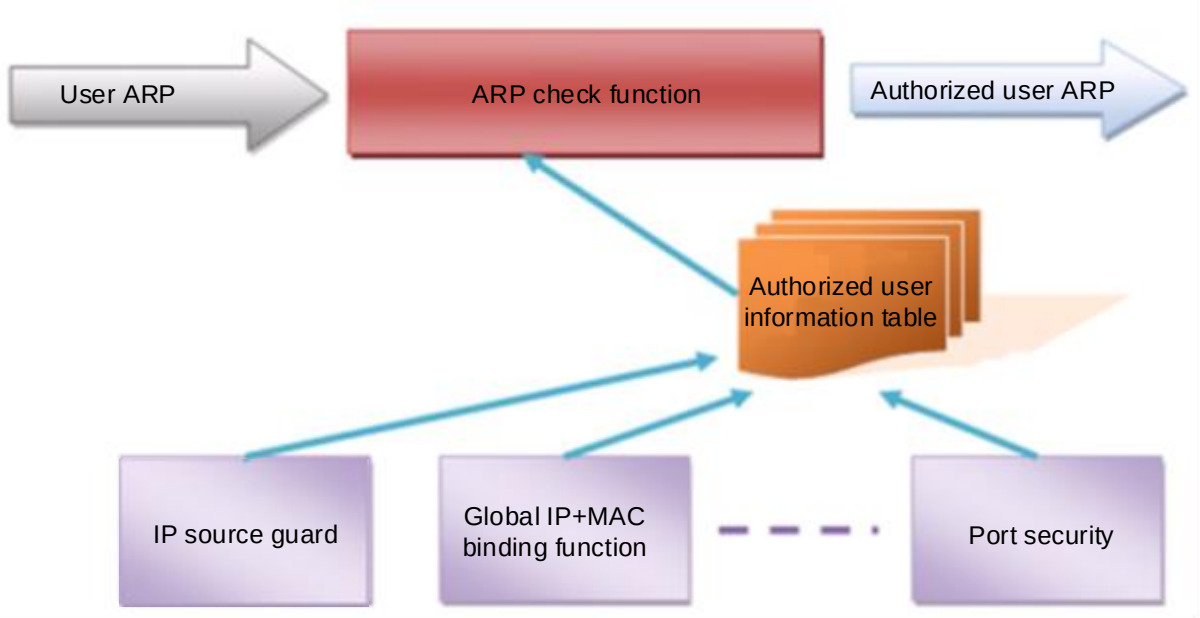
Command	Description
debug acl acld event	Debugs the ACL running process.
debug acl acld client-show	Debugs ACL clients.
debug acl acld acl-show	Debugs ACLs created by all ACL clients.

1 Configuring ARP Check

1.1 Overview

The Address Resolution Protocol (ARP) check filters all ARP packets on interfaces (including wired Layer 2 switching interfaces, 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 spoofing through networks and to promote network stability. On devices supporting ARP check, unauthorized ARP packets ion networks will be ignored according to authorized user information (IP-based or IP-MAC information) generated by security application modules such as IP source guard, global IP+MAC binding, 802.1X authentication, Global Security Network (GSN) binding, web-based authentication, and port security.

Figure 5-1



In Figure 5-1, security modules generate authorized user information (IP-based or IP-MAC based information). ARP check uses the information to detect whether the Sender IP field or the <Sender IP, Sender MAC> fields in all ARP packets on interfaces match those in the list of authorized user information. If not, such ARP packets will be discarded.

Protocols and Standards

RFC826: An Ethernet Address Resolution Protocol or Converting Network Protocol Addresses

1.2 Applications

Application	Description
Filtering ARP Packets on a Network	Unauthorized users on a network launch attacks using forged ARP packets.

1.2.1 Filtering ARP Packets on a Network

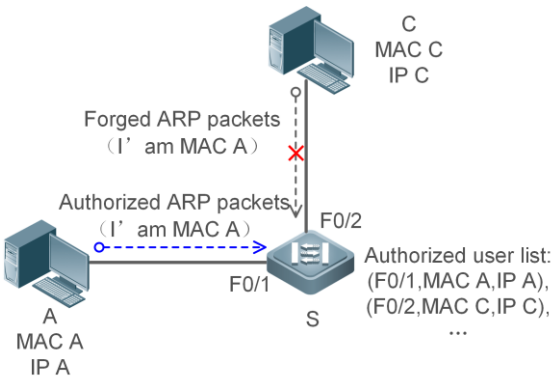
Scenario

ARP check enables the device to check ARP packets from untrusted interfaces and filter out ARP packets with addresses not matching the results assigned by the DHCP server.

In Figure 5-2, the device checks ARP packets sent by DHCP clients.

The interface receiving ARP packets, and the MAC address and IP address of the sender that sends ARP packets must be consistent with DHCP packets sent by the device for detection.

Figure 5-2



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 interfaces on S as DHCP untrusted interfaces.
- Enable IP source guard and ARP check on all untrusted interfaces of S to realize ARP packet filtering.

1.3 Features

Basic Concepts

Compatible Security Modules

ARP check can be used with the following security modules:

- IP-based mode: port security and IP source guard manually configured
- IP-MAC-based mode: port security, global IP+MAC binding, 802.1X authorization, IP source guard, GSN binding, and web-based authentication

Two Modes of APR Check

ARP check can be enabled or disabled. It is enabled by default.

1 Enabling ARP check

ARP check enables the device to check ARP packets based on IP-based or 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-based authentication
- IP+MAC binding or IP binding of port security

⚠ When only ARP Check is enabled on an interface, the device allows all packets to pass through. On the device enabled with ARP check and the above-mentioned modules, if user information cannot be generated, all ARP packets from this interface will be discarded.

⚠ When ARP check and VRRP are enabled on an interface, if the physical IP address and virtual IP address of the interface can be used as the gateway address, configure the device to allow packets from the physical IP address and virtual IP address to pass. Otherwise, ARP packets sent to the gateway will be filtered out.

2 Disabling ARP check

ARP packets on an interface are not checked.

Overview

Feature	Description
Filtering ARP Packets	Check the source IP and source MAC addresses of ARP packets to filter out unauthorized ARP packets.

1.3.2 Filtering ARP Packets

Enable ARP check on specified interfaces to filter unauthorized ARP packets.

Working Principle

A device matches the source IP and source MAC addresses of ARP packets received on its interfaces with authorized user information of the device. If information matches, packets are forwarded. Otherwise, they will be discarded.

Related Configuration

↘ Enabling ARP Check on Interfaces

By default, ARP check is disabled on interfaces.

Use the **arp-check** command to enable ARP check.

Unless otherwise specified, ARP check is typically configured on interfaces 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 interfaces.
- ARP check cannot be configured on the trusted interface of DHCP snooping.
- ARP check cannot be configured on global IP+MAC excluded interfaces.
- ARP check can be enabled only on wired switching interfaces, Layer aggregate interfaces, Layer 2 encapsulation sub-interfaces, as well as WLAN interfaces. Enable ARP check for the wired service in interface configuration mode, while for the wireless service in WLAN security configuration mode.
- For fit APs in wired access mode, ARP check needs to be enabled in all-AP configuration 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 interfaces** { *interface-type interface-number* } **arp-check list** command to display filtering entries.

Related Commands

Enabling ARP Check

Command	**arp-check**
Parameter Description	N/A
Command	Interface configuration mode, WLAN security configuration mode, or all-AP configuration mode
Usage Guide	This command is used to generate ARP filtering information according to authorized user information about security application modules to filter out unauthorized ARP packets on a network. When the ARP check function is enabled in all-AP configuration mode, the function is enabled on wired interfaces of all APs.

Configuration Example

The following configuration example introduces only the configuration related to ARP check.

Enabling ARP Check on Interfaces

Configuration Steps	• Enable ARP check. Restricted ARP packets must match entries of IP source guard, port security, 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(config)#interface gigabitethernet 0/4 Hostname(config-if-GigabitEthernet 0/4)# arp-check Hostname(config-if-GigabitEthernet 0/4)#exit Hostname(config)#interface gigabitethernet 0/5 Hostname(config-if-GigabitEthernet 0/5)# arp-check Hostname(config-if-GigabitEthernet 0/5)#end Hostname# configure terminal Hostname(config)#wlan-config 1 TEST-SSID Hostname(config-wlan)#end Hostname# configure terminal Hostname(config)#wlansec 1 Hostname(config-wlansec)# ip verify source port-security Hostname(config-wlansec)#arp-check Hostname(config-wlansec)#end Hostname# configure terminal 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 effective ARP check entries on 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
GigabitEthernet 0/4      00d0.f800.0003       192.168.1.3
address-bind
GigabitEthernet 0/4                           192.168.1.5
port-security
GigabitEthernet 0/5      00d0.f800.0003       192.168.1.3
address-bind

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 on an interface need to be checked but APR check is disabled, APR check will not take effect.

1.5 Monitoring

Displaying

Command	Description
show interfaces [*interface-type interface-number*] **arp-checklist**	Displays effective ARP check entries on interfaces.
show wlan [*wlan-id*] **arp-checklist**	Displays effective ARP check entries based on a WLAN.

1 Configuring Gateway-targeted ARP Anti-spoofing

1.1 Overview

Gateway-targeted Address Resolution Protocol (ARP) anti-spoofing effectively prevents gateway-targeted ARP spoofing by checking whether the source IP addresses of ARP packets (Sender IP fields of ARP packets) on the logical interface are the configured gateway IP addresses.

Protocols and Standards

RFC 826: Ethernet Address Resolution Protocol

1.2 Applications

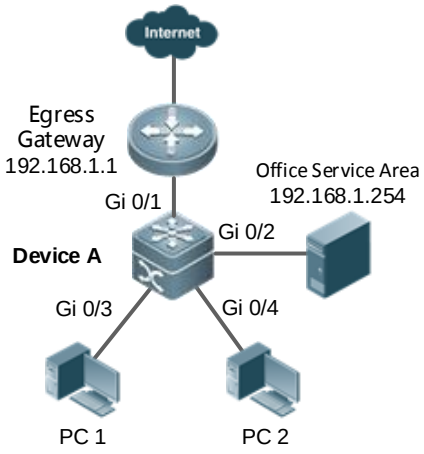
Application	Description
Gateway-targeted ARP Anti-spoofing	ARP spoofing packets with forged gateway addresses and intranet server IP addresses are blocked so that users can access the Internet.

1.2.1 Gateway-targeted ARP Anti-spoofing

Scenario

- PCs access the office server through the access device (Device A) and connect to the Internet through the gateway.
- If any malicious user hosts use forged gateway IP addresses or server IP addresses for ARP spoofing, the other user hosts cannot access the Internet or the server.
- ARP spoofing packets with forged gateway addresses and intranet server IP addresses must be blocked so that users can access the Internet.

Figure 1-1 Typical Topology of Gateway-targeted ARP Anti-spoofing



Deployment

Enable gateway-targeted ARP anti-spoofing on interfaces (Gi 0/3 and Gi 0/4 in this example) of the access device (Device A) that are directly connected to PCs. The gateway address is the intranet gateway address and the intranet server address.

1.3 Features

Basic Concepts

ARP

ARP, a TCP/IP protocol, obtains physical addresses based on IP addresses.

A host broadcasts ARP request packets to all hosts on the network and receives the returned packets to determine physical addresses of the target IP addresses, and saves IP addresses and hardware addresses in the local ARP cache, which are queried in response to future request packets. For ARP, all the hosts on a network trust 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 authenticity. In this way, attackers can send forged ARP response packets to target hosts so that packets sent from these hosts cannot reach the target host or reach the non-target 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. In the ARP response packet, the gateway IP address is the source IP address of the packet, and User B's MAC address is the source MAC address. When receiving the ARP response packet, User A considers User B's device 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 communication information is intercepted, thereby causing ARP spoofing.

Overview

Feature	Description
Gateway-targeted ARP Anti-spoofing	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 Anti-spoofing

Working Principle

Gateway-targeted Anti-spoofing

Gateway-targeted ARP anti-spoofing effectively prevents gateway-targeted ARP spoofing by checking whether the source IP addresses of ARP packets on the logical interface are the 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 incorrect ARP response packets. If not, the packet will not be handled. In this way, only the devices connected to the device can send ARP packets of the gateway, and forged ARP response packets sent from the other PCs are filtered by the device.

Related Configuration

Configuring the Gateway-targeted Anti-spoofing Address

- By default, no gateway-targeted ARP anti-spoofing address is configured.
- Run the **anti-arp-spoofing ip** command to configure the gateway-targeted ARP anti-spoofing address.

1.4 Configuration

Configuration	Description and Command	
Configuring Gateway-targeted Anti-spoofing	⚠ Optional.	
	anti-arp-spoofing ip	Configures gateway-targeted ARP anti-spoofing on the logical interface and specifies the gateway IP address.

1.4.1 Configuring Gateway-targeted Anti-spoofing

Configuration Effect

Enable gateway-targeted ARP anti-spoofing.

Configuration Steps

Configuring Gateway-targeted ARP Anti-spoofing

- Gateway-targeted ARP anti-spoofing is mandatory. It must be enabled.

Verification

- Run the **show running-config** command to check the configuration.
- Run the **show anti-arp-spoofing** command to display all data of gateway-targeted ARP anti-spoofing.

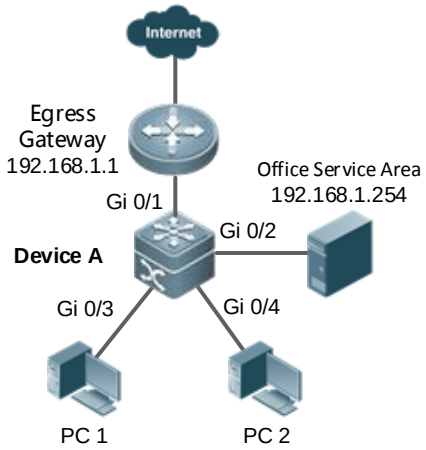
Related Commands

Configuring Gateway-targeted ARP Anti-spoofing

Command	**anti-arp-spoofing ip** *ipv4-address*
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the gateway.
Command Mode	Interface configuration mode or wireless security configuration mode
Usage Guide	This configuration is supported only on Layer 2 interfaces. This configuration is supported on wireless ACs in wireless security configuration mode only.

Configuration Example

Configuring Gateway-targeted ARP Anti-spoofing

Scenario **Figure 1-2**	
	PCs access the office server through the access device (Device A) and connect to the Internet through the gateway. If any malicious user hosts use forged gateway IP addresses or server IP addresses to perform ARP spoofing, the other user hosts cannot access the Internet or the server. The ARP spoofing packets with forged gateway addresses and intranet server IP addresses must be blocked so that users can access the Internet.
Configuration Steps	Enable gateway-targeted ARP anti-spoofing on the interfaces connected to the PCs.

	`DeviceA# configure terminal`
	`DeviceA(config)# interface range gigabitethernet 0/3-4`
	`DeviceA(config-if-range)# anti-arp-spoofing ip 192.168.1.1`
	`DeviceA(config-if-range)# anti-arp-spoofing ip 192.168.1.254`

Verification	Run the **show anti-arp-spoofing** command to check for data of gateway-targeted ARP anti-spoofing.

	`DeviceA# show anti-arp-spoofing`
	`NO PORT IP STATUS`
	`----- ---------- ---------- ----------`
	`3 Gi0/3 192.168.1.1 active`
	`4 Gi0/3 192.168.1.254 active`
	`5 Gi0/4 192.168.1.1 active`
	`6 Gi0/4 192.168.1.254 active`

1.5 Monitoring

Displaying

Command	Description
show anti-arp-spoofing	Displays all data on gateway-targeted ARP spoofing prevention.

1 Configuring Global IP-MAC Binding

1.1 Overview

Global IP-MAC binding is configured manually to verify bindings between IP addresses and MAC addresses in input packets. If a specified IP address is bound to a MAC address, the device receives only the IP packets containing matched IP address and MAC address, and discards other packets.

Global IP-MAC binding can be used to strictly verify the source of input packets. Note that this feature takes precedence over 802.1X authentication, port security, and access control list (ACL).

1.2 Applications

N/A

1.3 Features

Basic Concepts

IPv6 Address Binding Mode

IPv6 address binding has three modes: 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 forwarding rules described in the following table.

Mode	IPv4 Packet Forwarding Rule	IPv6 Packet Forwarding Rule
Strict	Packets matching the IPv4-MAC binding are forwarded.	Packets matching the global IPv6-MAC binding are forwarded.
Loose	Packets matching the IPv4-MAC binding are forwarded.	If IPv6-MAC binding is configured, packets matching the IPv6-MAC binding are forwarded. If IPv6-MAC binding does not exist, all IPv6 packets are forwarded.
Compatible	Packets matching the IPv4-MAC binding are forwarded.	If the IPv6 packets contain a MAC address matching the MAC address in the IPv4-MAC binding, the IPv6 packets are forwarded. Packets matching the global IPv6-MAC binding 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 can be also generated through global IP-MAC binding or other access security functions, such as port security and IPv6 source guard.

Overview

Feature	Description
Configuring an IPv6 Address Binding Mode	Changes IPv6 packet forwarding rules.

1.3.1 Configuring an IPv6 Address Binding Mode

Working Principle

After the IPv6-MAC binding is configured and access security functions are enabled, IPv6 packets are forwarded based on the IPv6 address binding mode. IPv6 address binding has three modes: compatible, loose, and strict.

Related Configuration

↘ Configuring an 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.

1.4 Configuration

Configuration	Description and Command	
Configuring an IPv6 Address Binding Mode	⚠ (Optional) It is used to configure an IPv6 address binding mode.	
	address-bind ipv6-mode	Configures an IPv6 address binding mode.

1.4.1 Configuring an IPv6 Address Binding Mode

Configuration Effect

Change the IPv6 address binding mode so as to change forwarding rules for IPv6 packets.

Configuration Step

↘ Configuring the IPv6 Address Binding Mode

Optional. Perform this configuration when you want to change forwarding rules for IPv6 packets.

Verification

Run the **show running-config** command to check whether the configuration takes effect.

Related Commands

↘ Configuring an 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	Global configuration mode

Mode	
Usage Guide	N/A

Configuration Example

Configuring an IPv6 Address Binding Mode

Configuration Steps	● Configure global IP-MAC binding. ● Enable address binding. ● Set the IPv6 address binding mode to compatible.

	`Hostname# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# address-bind ipv6-mode compatible`

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

1.5 Monitoring

Clearing

N/A

Displaying

N/A

Debugging

N/A

1 Configuring IP Source Guard

1.1 Overview

The IP source guard function realizes hardware-based IP packet filtering. This ensures 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
IP/MAC Spoofing Attack	On a network, users use unauthorized IP addresses and malicious users launch attacks by forging IP packets.

1.2.1 IP/MAC Spoofing Attack Defense

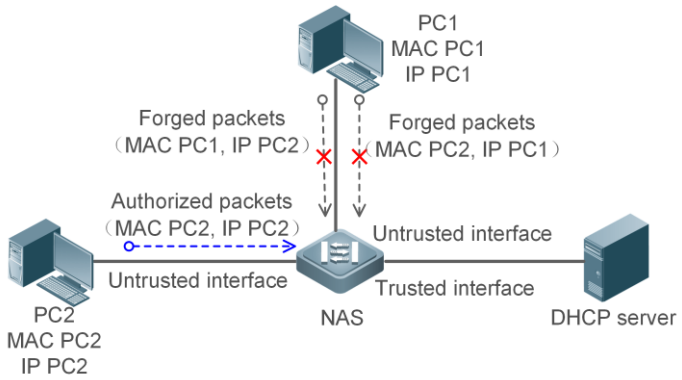
Scenario

The device checks IP packets from DHCP untrusted interfaces. Forged IP packets will be filtered out based on the address or IP and MAC addresses.

In Figure 1-1, the device checks IP packets sent by DHCP clients.

- 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 MAC addresses in DHCP request packets from clients.

Figure 1-1



Deployment

- Enable DHCP snooping on the NAS to realize DHCP monitoring.
- Set all downlink interfaces on the NAS as DHCP untrusted interfaces.
- Enable IP source guard on the NAS to realize IP packet filtering.

- Configure the IP-MAC mode for IP source guard on the NAS, which filters IP packets based on IP and MAC addresses.

1.3 Features

Basic Concepts

Source IP Address

Source IP address field of an IP packet.

Source MAC Address

Source MAC address field of an IP packet.

IP-based Filtering

Only source IP addresses of all IP packets (except DHCP packets) passing through an interface are checked. It is the default filtering policy of IP source guard.

IP-MAC based Filtering

Both 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 allowed to pass through.

Address Binding Database

It is the basis for security control of IP source guard. Data in the address binding database comes from the DHCP snooping binding database or statically configured. When IP source guard is enabled, 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 an interface, it is valid for all the VLANs on the interface. You can specify excluded VLANs, where the device does not check or filter IP packets. At most 32 excluded VLANs can be specified for an interface.

Overview

Feature	Description
Checking Source Address Fields of Packets	Filter IP packets passing through interfaces by IP-based or IP-MAC-based filtering.

1.3.1 Checking Source Address Fields of Packets

The device filters IP packets passing through interfaces based on source IP addresses or both source IP addresses and source MAC addresses to prevent malicious attacks by forging packets. When there is no need to check and filter IP packets within a VLAN, an excluded VLAN can be specified to allow such packets to pass through.

Working Principle

When IP source guard is enabled, the device checks source addresses of packets passing through an interface. The interface can be a wired switching interface, a Layer 2 aggregate interface, or a Layer 2 encapsulation sub-interface, or a WLAN interface. Such packets will pass through the interface only when source address fields of the packets match DHCP snooping binding entries, or the statically configured user set. There are two matching modes.

IP-based Filtering

Packets are allowed to pass through an interface only when source IP address fields of the packets belong to the address binding database.

IP-MAC-based Filtering

Packets are allowed to pass through an interface only when both Layer 2 source MAC addresses and Layer 3 source IP addresses of packets match an entry in the address binding database.

Specifying an Excluded VLAN

Packets within such a VLAN are allowed to pass through an interface without being checked or filtered.

Related Configuration

Enabling IP Source Guard on an Interface

- By default, IP source guard is disabled on interfaces.
- It can be enabled by using the **ip verify source** command.

IP source guard needs to be used with DHCP snooping. Therefore, DHCP snooping should also be enabled. DHCP snooping can be enabled on devices at any time, either before or after IP source guard is enabled.

Configuring Static Binding

- By default, authorized 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 valid for all the VLANs on an interface.
- Excluded VLANs can be specified by using the **ip verify source exclude-vlan** command.

Excluded VLANs can be specified only after IP source guard is enabled on an interface. Specified excluded VLANs will be deleted automatically when IP source guard is disabled on an interface.

The above-mentioned interface can be a wired switching interface, a Layer 2 aggregate interface, 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 an interface.

Configuration	Description and Command	
	ip source binding	Configures 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 packet forwarding may be affected. Typically, IP source guard is used with DHCP snooping.
- IP source guard cannot be configured on the trusted interfaces controlled by DHCP snooping.
- IP source guard cannot be configured on the global IP+MAC excluded interfaces.
- IP source guard can be configured and enabled only on the wired switching interface, a Layer 2 aggregate interface, a Layer 2 encapsulation sub-interface, or a WLAN interface. In a wired access scenario, this function is configured in interface configuration mode. In a wireless access scenario, this function is configured in WLAN security configuration mode.
- For a Fit AP in a wired access scenario, IP Source Guard is configured and enabled in all-AP configuration mode.

Configuration Step

- Enable DHCP snooping.
- Enable IP source guard.

Verification

Use monitoring commands to display the address binding database of IP source guard.

Related Commands

↘ Enabling IP Source Guard on an Interface

Command	**ip verify source** [**port-security**]
Parameter Description	**port-security**: Enables IP-MAC-based filtering.
Configuration Mode	Interface configuration mode, WLAN security configuration mode, or all-AP 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 an interface. In all-AP configuration mode, once IP source guard is enabled, it is valid for all wired interfaces of the AP.

↘ Configuring 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 static binding. **vlan-id**: Indicates the VLAN ID of static binding. It also refers to the outer VLAN ID of a QINQ-termination user. **ip-address**: The IP address of a static binding *interface-type interface-number*: Indicates the port ID (PID) of static binding. **wlan-id**: Indicates the WLAN ID of static binding. **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, authorized users can pass the check of IP source guard but not being controlled by DHCP. For a fit AP in a wireless scenario, an AC cannot access static information about users that are connected to a wired interface of a wireless AP.

Specifying an Excluded VLAN for IP Source Guard

Command	**ip verify source exclude-vlan** *vlan-id*
Parameter Description	*vlan-id*: Indicates the ID of an excluded VLAN where the device enabled with IP source guard does not check or filter such packets.
Configuration Mode	Interface configuration mode or WLAN security configuration mode
Usage Guide	By using this command, the device does not check or filter packets from the specified VLANs on an interface where IP source guard is enabled.

Configuration Example

Enabling IP Source Guard on an Interface

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)# exit`
	`Hostname(config)# wlansec 1`
	`Hostname(config-wlansec)# ip verify source port-security`
	`Hostname(config-wlansec)# end`

Verification	Display the address filtering table of IP source guard.
	`Hostname# show ip verify source`

Configuring Static Binding

Configuration Steps	● Enable DHCP snooping. ● Enable IP source guard. ● Configure 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	Display 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

↘ Enabling IP Source Guard on an Interface and 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)# exit 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 an interface.
	Hostname# show running-config

Common Errors

- IP source guard is enabled on a trusted interface of DHCP snooping.
- Specify an excluded VLAN before IP source guard is enabled.

1.5 Monitoring

Displaying

Command	Description
show ip verify source [**interface** *interface-type interface-number* | **wlan** *wlan-id*]	Displays the address filtering table of IP source guard.

Command	Description
show ip source binding	Displays the address binding database of IP source guard.

1 Configuring IPv6 Source Guard

1.1 Overview

The IPv6 source guard function realizes hardware-based IPv6 packet filtering. This ensures that only the users having their information in the binding database can access networks normally, preventing users from forging IPv6 packets.

1.2 Applications

Application	Description
IPv6/MAC Spoofing Attack Defense	On a network, malicious users launch attacks by forging IPv6 packets.

1.2.1 IPv6/MAC Spoofing Attack Defense

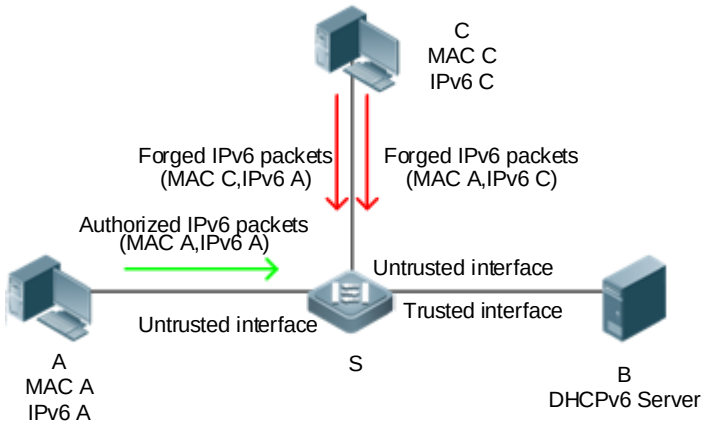
Scenario

The device checks IPv6 packets from DHCPv6 untrusted interfaces. Forged IPv6 packets will be filtered out based on the IPv6 address only or both IPv6 and MAC addresses.

In Figure 1-1, the device checks IPv6 packets sent by DHCPv6 clients.

- The Source IPv6 Address fields of IPv6 packets should match DHCPv6-assigned IPv6 addresses.
- The Source MAC Address fields of Layer 2 packets should match MAC addresses delivered through DHCPv6 snooping.

Figure 1-1



Remarks	S is an access device. A and C are PCs. B is the DHCPv6 server under control.

Deployment

- Enable DHCPv6 snooping on S to implement DHCPv6 packet monitoring.

- Configure all downlink interfaces on S as DHCPv6 untrusted interfaces.
- Enable IPv6 source guard on S to realize IPv6 packet filtering.
- Configure the IPv6-MAC mode for IPv6 source guard on S, which filters IPv6 packets based on IPv6 and MAC addresses.

1.3 Features

Basic Concepts

Source IPv6 Address

Source IPv6 address field of an IPv6 packet.

Source MAC Address

Source MAC address field of an IPv6 packet.

IPv6-based Filtering

Only source IPv6 addresses of all IPv6 packets (except DHCPv6 packets) passing through an interface are checked. It is the default filtering policy of IPv6 source guard.

IPv6-MAC-based Filtering

Both source IPv6 addresses and source MAC addresses of all IPv6 packets are checked, and only those user packets with these IPv6 addresses and MAC addresses existing in the binding database are allowed to pass through.

Address Binding Database

It is the basis for security control of IPv6 source guard. Data in the address binding database comes from the DHCPv6 snooping binding database or statically configured. When IPv6 source guard is enabled, data of the DHCPv6 snooping binding database is synchronized to the address binding database of IPv6 source guard, so that IPv6 packets can be filtered strictly through IPv6 source guard on a device with DHCPv6 snooping enabled.

Overview

Feature	Description
Checking Source Address Fields of Packets	Filters IPv6 packets passing through interfaces based on IPv6-based or IPv6-MAC-based filtering.

1.3.1 Checking Source Address Fields of Packets

The device filters IPv6 packets passing through interfaces based on source IPv6 addresses or both source IPv6 addresses and source MAC addresses to prevent malicious attacks by forging packets.

Working Principle

When IPv6 source guard is enabled, the device checks source addresses of packets passing through an interface. The interface can be a wired switching interface, a Layer 2 aggregate interface, or a Layer 2 encapsulation sub-interface, or a WLAN interface. Such packets will pass through the interface only when source address fields of the packets match DHCPv6 snooping binding entries, or the statically configured user set. There are two matching modes.

IPv6-based Filtering

Packets are allowed to pass through an interface only when source IPv6 address fields of the packets belong to the address binding database.

IPv6-MAC-based Filtering

Packets are allowed to pass through an interface only when both Layer 2 source MAC addresses and Layer 3 source IPv6 addresses of packets match an entry in the address binding database.

Related Configuration

Enabling IPv6 Source Guard on an Interface

- By default, IPv6 source guard is disabled on interfaces.
- It can be enabled by using the **ipv6 verify source** command.

IPv6 source guard needs to be used with DHCPv6 snooping. Therefore, DHCPv6 snooping should also be enabled. DHCPv6 snooping can be enabled on devices at any time, either before or after IPv6 source guard is enabled.

Configuring a Static Binding

- By default, authorized users passing IPv6 source guard check are all from the binding database of DHCPv6 snooping.
- Bound users can be added using the **ipv6 source binding** command.

1.4 Configuration

Configuration	Description and Command	
Configuring IPv6 Source Guard	(Mandatory) It is used to enable IPv6 source guard.	
	ipv6 verify source	Enables IPv6 source guard on an interface.
	ipv6 source binding	Configures a static binding.

1.4.1 Configuring IPv6 Source Guard

Configuration Effect

Check the source IPv6 addresses of input IPv6 packets.

Notes

IPv6 source guard should be used with DHCPv6 snooping. IPv6 source guard can take effect when configured on the untrusted interfaces controlled by DHCPv6 snooping. However, when IPv6 source guard is configured on trusted interfaces or interfaces on a VLAN that is not controlled by DHCPv6 snooping, this function cannot take effect.

Configuration Steps

- Enable DHCPv6 snooping.
- Enable IPv6 source guard.

Verification

Use monitoring commands to display the address binding database of IPv6 source guard.

Related Commands

Enabling IPv6 Source Guard on an Interface

Command	**ipv6 verify source** [**port-security**]
Parameter Description	**port-security**: Enables IPv6-MAC-based filtering.
Command Mode	WLAN security configuration mode
Usage Guide	Detection of users based on IPv6 address or both IPv6 and MAC addresses can be realized by enabling IPv6 source guard. After IPv6 source guard is enabled, packets with source IPv6 addresses as link-local addresses and unspecified addresses are filtered. On an IPv6 network, these two types of packets need to be permitted, so additional security rules are required to allow them to pass through.

Configuring a Static Binding

Command	**ipv6 source binding** *mac-address* **vlan** *vlan-id ipv6-address* { **interface** *interface-id* | **wlan** *wlan-id* | **ipv6-mac** | **ipv6-only** }
Parameter Description	*mac-address*: Indicates the MAC address of a static binding. *vlan-id*: Indicates the VLAN ID of a static binding. *ipv6-address*: Indicates the IPv6 address of a static binding. *interface-id*: Indicates the interface of a static binding. *wlan-id*: Indicates the WLAN ID of a static binding. **ipv6-mac**: Indicates the IPv6-MAC-based mode. **ipv6-only**: Indicates the IPv6-based mode.
Command Mode	Global configuration mode
Usage Guide	Through this command, authorized users can pass the check of IPv6 source guard but not being controlled by DHCPv6.

Configuration Example

Enabling IPv6 Source Guard on an Interface

Configuration Steps	● Enable DHCPv6 snooping.
	● Configure ACEs for a secure channel permit packets in which source IPv6 addresses are link-local addresses or 0.0.0.0.
	`Hostname(config)# ipv6 access-list v6-list`
	`Hostname(config-ipv6-nacl)# permit ipv6 fe80::/10 any`
	`Hostname(config-ipv6-nacl)# permit ipv6 ::/128 any`
	`Hostname(config-ipv6-nacl)# exit`
	`Hostname(config)# security global access-group v6-list`
	● Enable IPv6 source guard.

	Hostname(config)# wlansec 1 Hostname(config-wlansec)# ipv6 verify source Hostname(config-wlansec)# end
Verification	● Display the address filtering table of IPv6 source guard.
	Hostname# show ipv6 source binding

↘ Configuring a Static Binding

Configuration Steps	● Enable DHCPv6 snooping. ● Enable IPv6 source guard. ● Configure a static binding.
	Hostname# configure terminal Hostname(config)# ipv6 source binding 0001.0002.0006 vlan 1 2008::1 ip-mac Hostname(config)# end
Verification	● Display the address filtering table of IPv6 source guard.
	Hostname# show ipv6 source binding

Common Errors

- IPv6 source guard is enabled on a trusted interface of DHCPv6 snooping.

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show ipv6 source binding	Displays the address binding database of IPv6 source guard.

Debugging

N/A

1 Configuring CPP

1.1 Overview

Malicious attacks are often found on networks. Network devices are busy in processing forged management and protocol packets, so real management and protocol packets cannot be processed in a timely manner. Such attacks damage 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 access controller (AC) provides packet identification and rate limiting to protect processors.

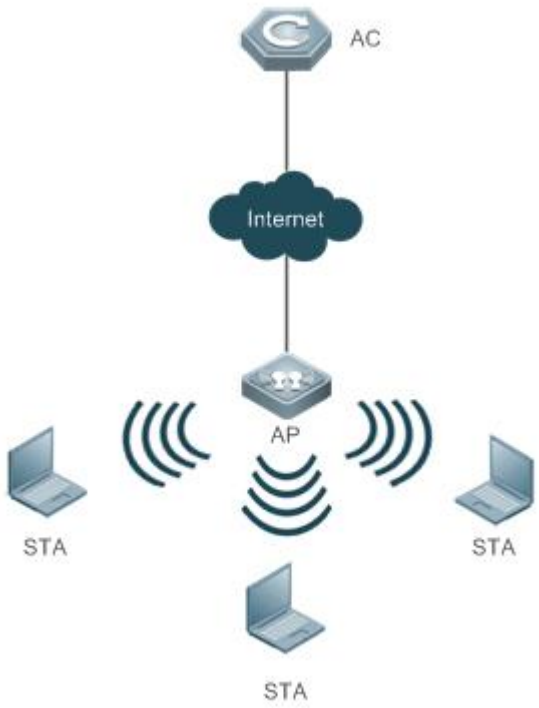
Figure 3-1 shows the networking topology of CPP.

1 An access point (AP) accesses the AC.

2 Multiple stations (STAs) access the AP.

3 Attacks of specified packets may occur on STAs on a network. The AC must be able to protect their CPU.

Figure 3-1 Networking Topology

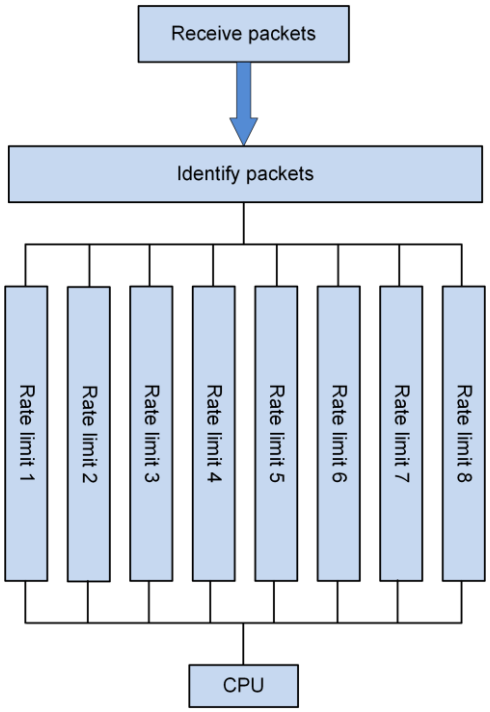


Deployment

Apply CPP to the AC to limit the rate of specified packets.

1.3 Features

Figure 3-2 Working Principle



Basic Concepts

Identifying Packets

All packets that are sent to the AC for protocol processing must be classified (such as ARP packets, BPDUs, and 802.1X packets) through packet identification.

Rate Limiting

An administrator can configure the rate limit for packets of each type, effectively suppressing high-rate attack packets on a network.

Overview

Feature	Description
Identifying Packets	All packets that are sent to CPU are classified through packet identification.
Rate	High-rate attack packets are suppressed by rate limiting.

1.3.1 Identifying Packets

All packets that are sent to CPU are classified through packet identification.

Working Principle

Identifying Packets

The CPP-enabled device classifies packets and automatically applies the packet identification function by default.

1.3.2 Rate Limiting

An administrator can configure the rate limit for packets of each type, effectively suppressing high-rate attack packets on a network.

Working Principle

Rate Limiting

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
Configuring the Rate Limit for Wireless Management Packets	⚠ (Optional) It is used to set the rate limit for wireless management packets.	
	mgmt-ratelimit disable	Enables or disables rate limiting of wireless management packets.
	mgmt-ratelimit per-cti pps *value*	Configures the CTI-based rate limit for wireless management packets.

	mgmt-ratelimit total pps *value*	Configures the AC-based rate limit for wireless management 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 Step

Configuring the Rate limit for Specified Packets

- Optional.
- Enable CPP on all ACs unless otherwise specified.
- You can adjust the default rate limit for packets of each type as needed.

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** | **tcp80 | tcp443** | **vrrp** } **pps** *value*
Parameter Description	**arp**: Specifies the Address Resolution Protocol (ARP) packet. **bpdu**: Specifies the IEEE Bridge Protocol Data Unit (BPDU). **capwap-disc**: Specifies the Control And Provisioning of Wireless Access Points (CAPWAP) discovery packet. **d1x**: Specifies the 802.1X Extensible Authentication Protocol over LAN (EAPOL) packet. **dhcp-option82**: Specifies the Dynamic Host Configuration Protocol (DHCP) Option 82 packet. **dhcp-relay-client**: Specifies the DHCP client's packet. **dhcp-relay-server**: Specifies the DHCP server's packet. **dhcps**: Specifies the DHCP snooping packet. **igmp**: Specifies the Internet Group Management Protocol (IGMP) packet. **ipmc**: Specifies the IPv4 multicast packet. **ipv6-nans**: Specifies the IPv6 neighbor discovery packet. **lldp**: Specifies the Link Layer Discovery Protocol Data Unit (LLDPDU). **ospf**: Specifies the Open Shortest Path First (OSPF) packet. **ospfv3**: Specifies the OSPFv3 packet. **pppoe**: Specifies the Point to Point Protocol over Ethernet (PPPoE) packet. **pim**: Specifies the Protocol Independent Multicast (PIM) packet. **rip**: Specifies the IPv4 Routing Information Protocol (RIP) packet. **ripng**: Specifies the IPv6 RIP packet. **tcp80**: Specifies the web-based authentication redirection packet. **Tcp443**: Specifies the Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) packet. **vrrp**: Specifies the Virtual Router Redundancy Protocol (VRRP) packet. **pps** *value*: Specifies the upper limit of packets per second. The value range is from 0 to 148810, in pps.

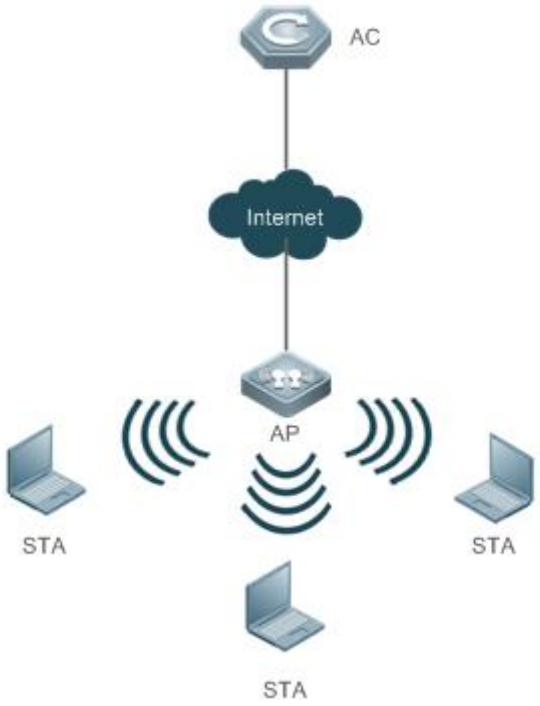
Defaults	The default values vary with the product model.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Run the **show cpu-protect summary** command to display the configuration.

Configuration Example

Configuring the Rate Limit for ARP Packets as 200 pps

Scenario Figure 3-3	
Configuration Steps	Configure the rate limit for ARP packets on the AC.
AC	`Hostname#configure terminal` `Hostname(config)#cpu-protect type arp pps 200`
Verification	After the rate limit for ARP packets is configured on the AC, the system limits the rate for ARP packets arriving at the CPU based on the new rate limit. ● Run the **show cpu-protect summary** command to check configured parameters. ● Run the **show cpu-protect type arp** command to display statistics about the received ARP packets.

AC	`Hostname#show cpu-protect summary`
	`Type Pps`
	`------------------- ---------`
	`arp 1000`

```
 d1x                  128
 bpdu                 128
 lldp                 128
 dhcp-relay-server    128
 dhcp-relay-client    128
 dhcps                128
 dhcp-option82        128
 capwap-disc          128
 ipv6-nans            128
 rip                  128
 pppoe                128
 ripng                600
 ospf                 600
 ospfv3               600
 vrrp                 128
 igmp                 500
 pim                  1000
 ipmc                 128
 tcp80                1200
 tcp443               100
Hostname#show cpu-protect type arp
Type                  Pps       Total     Drop
 -------------------- --------- --------- ---------
 arp                   1000      128089    0
```

Common Errors

N/A

1.4.2 Configuring the Rate Limit for Wireless Management Packets

Configuration Effect

Configure the rate limit for wireless management packets.

Notes

N/A

Configuration Step

↘ Configuring the Rate Limit for Wireless Management Packets

- Optional. This function is supported only on the AC. By default, the CTI-based rate limit is 8 pps. Different ACs adopt different default AC-based rate limits.
- Enable the rate limiting function for wireless management packets on all ACs unless otherwise specified.
- You can adjust the default rate limit based on the CTI or the AC as needed.

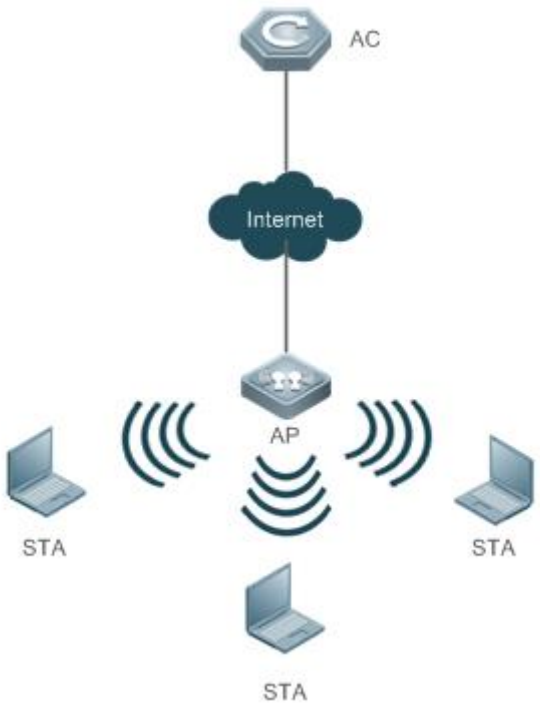
Command	**mgmt-ratelimit** { **disable** | **per-cti pps** *value* | **total pps** *value* }
Parameter Description	**disable**: Disables rate limiting for wireless management packets. It is enabled by default. **per-cti pps** *value*: Configures the CTI-based rate limit. The value range is from 1 to 10000, in pps. The default value is 8 pps. **total pps** *value*: Configures the AC-based rate limit. The value range is from 1 to 10000, in pps. Default values vary with different ACs.
Defaults	The rate limiting function is enabled by default. The default CTI-based rate limit is 8 pps. The default AP-based rate limit varies with different ACs.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

Run the **show running-config** command to display the rate limit of wireless management packets.

Configuration Example

Configuring the AC-based Rate Limit for Wireless Management Packets as 100 pps

Scenario Figure 3-4	
Configuration Steps	Configure the AC-based rate limit for wireless management packets.
AC	`Hostname#configure terminal` `Hostname(config)#mgmt-ratelimit total pps 200`
Verification	After the AC-based rate limit is set, the system filters wireless management packets based on the

	new rate limit. ● Run the **show running-config** command to display the rate limit of wireless management packets. ● Run the **show mgmt-ratelimit summary** command to display statistics about ARP packets.

AC	`Hostname#show running-config`
	`…`
	`mgmt-ratelimit total pps 200`
	`…`
	
	`Hostname#show mgmt-ratelimit summary`
	`pps max tpkts drop`
	`-------- -------- -------------------- --------------------`
	`0 40 1 0`

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show cpu-protect summary	Displays the rate limit for packets of various types.
show 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 | tcp80** | **tcp443** | **vrrp** }	Displays statistics about specified packets.
show running-config	Displays the rate limit for wireless management packets.
show mgmt-ratelimit cti *ifx*	Displays statistics about CTI-based wireless management packets.
show mgmt-ratelimit summary	Displays statistics about AP-based wireless management packets.

1 Configuring NFPP

1.1 Overview

The Network Foundation Protection Policy (NFPP) provides attack defense for devices.

Some malicious attacks are always found on a network. These attacks bring heavy burdens to devices, resulting in high CPU usage and abnormal device running. The following attacks often occur:

Denial of service (DoS) attacks may greatly consume the memory, entries, or other resources of a device to cause system services to be unavailable.

Massive attack traffic is sent 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 failures. Forwarding on the data plane will also be affected and the entire network will become abnormal.

A great number of attack packets directed to the CPU consume many CPU resources, resulting in a highly loaded CPU and thereby causing device management failures or abnormal running.

NFPP can effectively protect the system against these attacks. When attacks occur, 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 on a network, the CPU cannot process normal protocol and management traffic, causing protocol flapping or management failures. 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	Because normal service traffic is heavy, 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 failures. The centralized rate limiting and distribution function is used to increase the priority of such traffic so that devices can run stably.

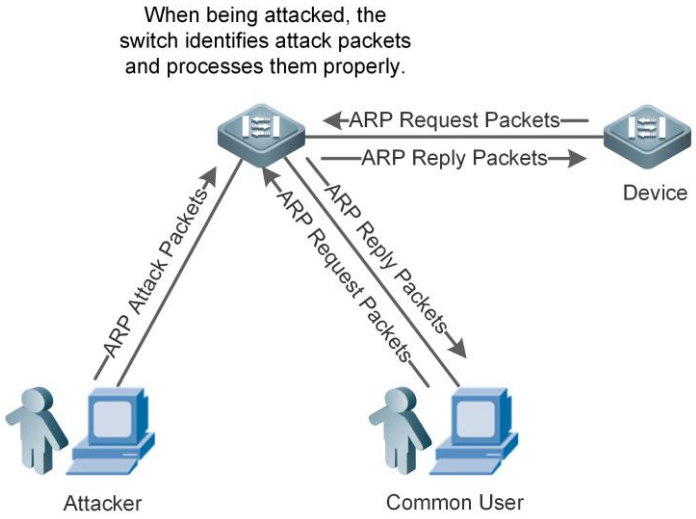
1.2.1 Attack Detection and Rate Limiting

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. ARP packets are used as an example here.

If an attacker sends ARP attack packets in the case of limited CPU capability, 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, normal ARP packets will be lost. As shown in Figure 4-1, common users will fail to access the network, and the device will fail to send ARP Reply packets to other devices.

Figure 4-1



Deployment

- By default, the ARP attack detection and rate limiting function is enabled, and 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 user will be generated and prompt information will be output.
- If an attacker's ARP packet rate exceeds the rate limit defined in CPP and affects normal ARP Reply packets, you can enable attack isolation to discard ARP attack packets based on an ACL and recover the network.

For details about the CPP configuration, refer to *Configuring CPP*.

To maximize the use of NFPP attack defense, change the rate limits for various services in CPP based on the application environment or use the configuration recommended by the system. You can run the **show cpu-protect summary** command to display the configuration.

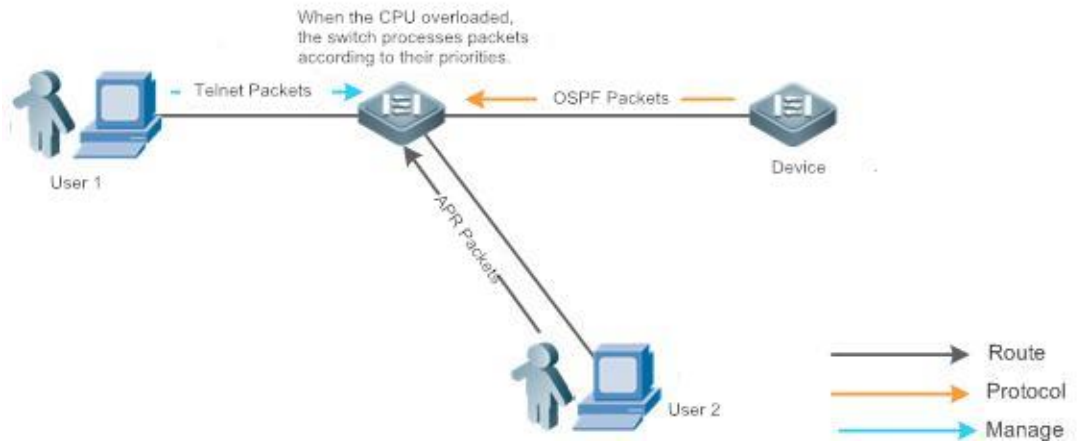
1.2.2 Centralized Rate Limiting and Distribution

Scenario

A device classifies services defined in CPP into three types: management, routing, and protocol packets. Each type of services has independent bandwidth. Different types of services cannot share their bandwidth. Traffic exceeding the bandwidth threshold is discarded. By such service classification, service packets of a certain type can be processed first.

As shown in Figure 4-2, 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 placed in the queue, causing various problems such as occasional Telnet disconnection, OSPF protocol flapping, and ARP access failure.

Figure 4-2



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 nonstop 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 Anti-attack

On local area networks (LANs), IP addresses are converted to MAC addresses through ARP, which is significant for safeguarding network security. A large number of unauthorized ARP packets are sent to the gateway through the network, causing a failure for 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

Attackers start scanning active hosts on a network before initiating hacker attacks and network virus intrusions. Therefore, many scanning packets rapidly occupy the network bandwidth, causing network communication failures.

To solve this problem, Layer 3 devices provide IP attack defense to prevent scanning by hackers and Blaster Worm viruses and reduce the CPU load. There are mainly two types of IP attacks:

- Scanning destination IP address changes: This type of scanning is the most harmful to networks. It consumes network bandwidth and increases device burden, and also serves as a precursor to many hacker attack methods.
- Sending IP packets to nonexistent destination IP addresses at a high rate: This type of attack is primarily designed to burden the device's CPU. For a Layer 3 device, if the destination IP address exists, the packet will be directly forwarded by the switching chip without consuming the device's CPU resources. However, if the destination IP address does not exist, the IP packet will be sent to the CPU, which will then send an ARP Request packet to query the MAC address corresponding to the destination IP address. If many packets are sent to the CPU, it will consume CPU resources. The harm caused by this type of attack is much less than that of the first type.

To prevent the latter type of attacks, limit the rate of IP packets and detect and isolate the attack source.

ICMP Attack Defense

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, consuming some 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 Attack Defense

DHCP is widely used on LANs to dynamically assign IP addresses. It greatly affects network security. The most common DHCP attacks, also called DHCP exhaustion attacks, use forged MAC addresses to broadcast DHCP Request packets. Various attack tools on the live network can initiate such attacks. A network attacker can send a large number of DHCP Request packets to use up the address space provided by the DHCP server within a period. In this case, authorized hosts will fail to request 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 Attack Defense

DHCP version 6 (DHCPv6) is widely used on 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 Request packets 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 Attack Defense

Neighbor Discovery (ND) is mainly used on 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.

ND snooping monitors ND packets on a network to filter unauthorized ND packets. It also monitors IPv6 hosts on a network and binds the monitored IPv6 hosts to interfaces to prevent IPv6 address from being used in unauthorized manner. ND snooping requires ND packets to be sent to the CPU. If ND packets are sent at a high rate, the CPU will be attacked. Therefore, ND attack defense 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 on a network.
Interface-based Rate Limiting and Attack Identification	Limit the rate according to the interface-based rate limit and identify interface attacks.
Configuring the Monitoring Period	Monitor host attackers in a specified period.
Configuring the Isolation Period	Isolate host attackers or interface attackers in a specified period.
Configuring Trusted Hosts	Trust a host. That is, the trusted host is not monitored.
Centralized Rate Limiting and Distribution	Classify and prioritize packets.

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 based on the source IP address, VLAN ID, and interface, or based on the link-layer source MAC address, VLAN ID, and interface. Each host has a rate limit and an attack threshold (also called alarm threshold). The rate limit must be smaller 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, logs them, and sends trap packets.

ARP scanning attacks may occur 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 occur.

When the NFPP-enabled device detects a specific type of attack packets of a service, it sends an alarm to the administrator. If the attack traffic persists, the NFPP-enabled device will not resend the alarm within 60 seconds after generating an alarm.

To prevent CPU resource consumption caused by frequent logging, the NFPP-enabled device writes attack detection logs to the buffer, obtains them from the buffer at a specified rate, and generates them. The NFPP-enabled device does not limit the rate of trap packets.

Only ARP attack defense and IP anti-scanning support anti-scanning.

1.3.2 Interface-based Rate Limiting and Attack Identification

Limit the rate of interface-based attack packets and identify the attacks.

Working Principle

Each interface has a rate limit and an attack threshold. The rate limit must be smaller than the attack threshold. If the packet rate exceeds the rate limit on an interface, the interface discards the packets. If the packet rate exceeds the attack threshold on an interface, the interface records the attacks in logs and sends trap packets.

1.3.3 Configuring the Monitoring Period

Configure the monitoring period for attackers.

Working Principle

Monitored hosts provide information about attackers in the current system. If the isolation period is 0 (that is, no isolation), the attack defense module automatically performs software monitoring on attackers in the configured

monitoring period. Within the monitoring period, you can view entries of a monitored host. If attack packets are received from this host before aging of the monitoring period, update the monitoring period of the host; otherwise, when the monitoring period is set to 0, entries of the monitored host will be deleted. When the isolation time is configured as a non-0 value, the attack defense module automatically isolates the host monitored by the software.

1.3.4 Configuring the Isolation Period

Configure the isolation period for attackers.

Working Principle

Isolation is performed based on the attack defense 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.

Isolation involves host-based and interface-based isolation. When an attacker is isolated, a policy will be configured in an ACL. When ACLs are exhausted and isolation fails, logs will be generated 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 configure the host to be trusted. This trusted host will be allowed to send packets of specified types to the CPU.

1.3.6 Centralized Rate Limiting and Distribution

Set the rate thresholds and percentages for management, routing, and protocol packets.

Working Principle

Services defined in the CPP are classified into three types: management, routing, and protocol packets. 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.

NFPP allows the administrator to flexibly assign bandwidth for three types of packets based on the actual network situation so that protocol and management packets can be first processed. Processing of protocol packets ensures proper running of the protocol, and processing of management packets helps the administrator perform proper management, thereby ensuring proper running of important device functions and improving attack defense capabilities of the device.

After packets are classified and rate-limited, all types of packets are centralized in a queue. When one type of service features a lower processing efficiency, packets of this service will be placed in the queue and may finally use up resources of the queue. NFPP allows the administrator to configure the percentages of these three types of packets in the queue. When the queue length occupied by one type of packets exceeds the product of the total queue length and the percentage of this type of packets, these packets are discarded. This effectively prevents one type of packets from exclusively occupying queue resources.

Packet Type	Service Type Defined in CPP
Protocol	tp-guard, dot1x, rldp, rerp, slow-packet, bpdu, 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 the definitions of service types, see *Configuring CPP*.

1.4 Configuration

Configuration	Description and Command	
Configuring ARP Attack Defense_Configuring_ARP_Guard	(Mandatory) It is used to configure global ARP attack defense.	
	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.
	arp-guard scan-threshold	Configures the global host-based scanning threshold.
	(Optional) It is used to configure ARP isolation and ARP attack defenseguard.	
	arp-guard isolate-period	Configures the global isolation period.
	arp-guard trusted-host	Configures trusted hosts.
	nfpp arp-guard enable	Enables attack detection for an interface.
	nfpp arp-guard policy	Configures the rate limit and attack threshold for an interface.
	nfpp arp-guard scan-threshold	Configures the stage-by-stage scanning threshold for an interface.
	nfpp arp-guard isolate-period	Configures the isolation period for an interface.
Configuring IP Anti-scanning_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 interface-based IP anti-scanning.	

Configuration	Description and Command	
	ip-guard isolate-period	Configures the global isolation period.
	ip-guard trusted-host	Configures trusted hosts.
	nfpp ip-guard enable	Enables attack detection for an interface.
	nfpp ip-guard policy	Configures the rate limit and attack threshold for an interface.
	nfpp ip-guard scan-threshold	Configures the stage-by-stage scanning threshold for an interface.
	nfpp ip-guard isolate-period	Configures the isolation period for an interface.
Configuring ICMP Attack Defense_Configuring_ICMP_Guard	(Mandatory) It is used to configure global ICMP attack defense.	
	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.
	(Optional) It is used to configure ICMP trusted hosts, ICMP isolation and interfaceport-based ICMP attack defenseguard.	
	icmp-guard isolate-period	Configures the global isolation period.
	icmp-guard trusted-host	Configures trusted hosts.
	nfpp icmp-guard enable	Enables attack detection for an interface.
	nfpp icmp-guard policy	Configures the rate limit and attack threshold for an interface.
	nfpp icmp-guard isolate-period	Configures the isolation period for a port.
Configuring DHCP Attack Defense_Configuring_DHCP_Guard	(Mandatory) It is used to configure the global DHCP attack defenseguard 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 interface-based DHCP attack defense.	
	dhcp-guard isolate-period	Configures the global isolation period.
	dhcp-guard trusted-host	Configures trusted hosts.
	nfpp dhcp-guard enable	Enables attack detection for an interface.
	nfpp dhcp-guard policy	Configures the rate limit and attack threshold for an interface.
	nfpp dhcp-guard isolate-period	Configures the isolation period for an interface.
Configuring DHCPv6	(Mandatory) It is used to configure global DHCPv6 attack defense.	

Configuration	Description and Command	
Attack Defense_Configuring_DHCPv6_Guard	**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 attack defense.	
	dhcpv6-guard isolate-period	Configures the global isolation period.
	dhcpv6-guard trusted-host	Configures trusted hosts.
	nfpp dhcpv6-guard enable	Enables attack detection for an interface.
	nfpp dhcpv6-guard policy	Configures the rate limit and attack threshold for an interface.
	nfpp dhcpv6-guard isolate-period	Configures the isolation period for an interface.
Configuring ND Attack Defense_Configuring_ND_Guard	⚠ (Mandatory) It is used to configure the global ND attack defenseguard 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 interface-based ND attack defense.	
	nd-guard trusted-host	Configures trusted hosts.
	nfpp nd-guard enable	Enables attack detection for an interface.
	nfpp nd-guard policy	Configures the rate limit and attack threshold for an interface.
Configuring Centralized Rate Limiting and Distribution_Configuring_Centralized_Rate	⚠ (Optional) It is used to set the rate thresholds and percentages for management, routing, and protocol packets.	
	cpu-protect sub-interface pps	Configures the maximum bandwidth for each type of packets.
	cpu-protect sub-interface percent	Configures the maximum percentage of each type of packets in the queue.
Configuring NFPP Log Information_Configuring_NFPP_Log	⚠ (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 configure 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 Attack Defense

Configuration Effect

- ARP attacks are identified based on hosts or physical interfaces. Host-based ARP attack identification can be based on the source IP address, VLAN ID, and interface, or based on the link-layer source MAC address, VLAN ID, and interface. 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 generates alarms and sends trap packets. In host-based attack identification, the system also isolates the attack source.
- ARP attack defense 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. Because attacks may be identified incorrectly, the hosts that may initiate ARP scanning are not isolated and are notified of the administrator for 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 precedence over that in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.
- ARP attack defense prevents only ARP DoS attacks to the device, but not ARP spoofing or ARP attacks on a network.

Configuration Step

↘ Enabling Attack Detection

- Mandatory.
- The AC supports the global configuration mode and interface configuration mode.
- If ARP attack defense is disabled, the system automatically clears monitored hosts, scanned hosts, and port isolation entries.

Command	**arp-guard enable**
Parameter Description	N/A
Defaults	ARP attack defense is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp arp-guard enable**
Parameter Description	N/A
Defaults	ARP attack defense is configured in global configuration mode, but not in interface configuration mode.

Command Mode	Interface configuration mode
Usage Guide	ARP attack defense configured in interface configuration mode takes precedence over that configured in global configuration mode.

Configuring the Isolation Period

- (Optional) Isolation is disabled by default.
- If the packet rate of attackers exceeds the rate limit, configure the isolation period for the device to directly discard packets and therefore save bandwidth resources.
- The AC supports the global configuration mode and interface configuration mode.
- If the isolation period is changed to 0, attackers on the corresponding interface are deleted, instead of being monitored by software.

Command	**arp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period, in seconds. It can be set to 0 or any value from 30 to 86400. **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 seconds. It can be set to 0 or any value from 30 to 86400.The value 0 indicates no isolation. **permanent**: Indicates permanent isolation.
Defaults	The default global isolation period is 0, that is, no isolation.
Command Mode	Interface configuration mode
Usage Guide	N/A

Configuring the Monitoring Period

- Mandatory.
- If the isolation period is configured, it is used as the attacker monitoring period, and the configured monitoring period does not take effect.
- The AC supports the global configuration mode.

Command	**arp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period, in seconds. The value ranges from 180 to 86400.
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.
- The AC supports the global configuration mode.
- 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 displays the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." The message notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system generates 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. The value range is from 1 to 4294967295.
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 attack defense 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
- The AC supports the global configuration mode and interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system generates 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 generates 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 generates the log "%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes precedence over source IP address-based rate limiting, while the latter takes precedence over interface-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 interface or based on the link-layer source MAC address, VLAN ID, and interface.

- 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 interface or based on the link-layer source MAC address, VLAN ID, and interface.
- In interface configuration mode, run the **nfpp arp-guard policy** {**per-src-ip | per-src-mac**} *rate-limit-pps attack-threshold-pps* command to configure rate limits and attack thresholds of hosts identified based on the source IP address, VLAN ID, and interface or based on the link-layer source MAC address, VLAN ID, and interface 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 interface. *pps*: Indicates the rate limit. The value range is from 1 to 9999.
Defaults	The default rate limit varies with the product model.
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 interface. *pps*: Indicates the attack threshold, in packets per second (pps). The value range is from 1 to 9999.
Defaults	The default attack threshold varies with the product model.
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 interface. *rate-limit-pps*: Indicates the rate limit. The value range is from 1 to 9999. *attack-threshold-pps*: Indicates the attack threshold. The value range is from 1 to 9999.
Defaults	By default, no rate limit and attack threshold are configured for an interface, 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.
- The AC supports the global configuration mode and interface configuration mode.

- The ARP scanning table stores only the latest 256 records. When the ARP scanning table is full, the latest record will overwrite the earliest record.
- ARP scanning attack may occur 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 count exceeds the scanning threshold.

Command	**arp-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold. The value range is from 1 to 9999.
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. The value range is from 1 to 9999.
Defaults	By default, no interface-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 attack defense, you can configure only a maximum of 500 IP addresses and MAC addresses not to be monitored.
- The AC supports the global configuration mode.
- 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 generates 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 generates 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 generates 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 generates 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 generates 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, configure the host to be trusted. The trusted host can send ARP packets to the CPU. In this case, the device does not rate-limit such packets or generate alarms.

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 matching the trusted host configuration) exceeds the attack threshold or scanning threshold, attack information is displayed.
- If the rate of attack packets matches the trusted host configuration, no information is displayed.

Configuration Example

CPU Protection Based on ARP Attack Defense

Scenario	● ARP host attacks exist in the system, and some hosts cannot properly establish ARP sessions. ● ARP scanning exists in the system, causing a high CPU usage. ● ARP packet traffic of some hosts is heavy in the system, and these packets need to be allowed.
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 configuration.

	`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 interfaces. In host-based IP attack identification, IP attacks are identified based on the source IP address, VLAN ID, and interface. 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 generates alarms 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. 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 precedence over that in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Step

Enabling Attack Detection

- Mandatory. Attack detection is enabled by default.
- The AC supports the global configuration mode and interface configuration mode.
- 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 precedence 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 CPP, configure the isolation period for the device to directly discard packets and therefore save bandwidth resources.
- The AC supports the global configuration mode and interface configuration mode.
- If the isolation period is changed to 0, attackers on the corresponding interface is deleted, instead of being monitored by software.

Command	**ip-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period, in seconds. It can be set to 0 or any value from 30 to 86400. **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 seconds. It can be set to 0 or any value from 30 to 86400. 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 used as the attacker monitoring period, and the configured monitoring period does not take effect.
- The AC supports the global configuration mode.

Command	**ip-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period, in seconds. The value ranges from 180 to 86400.
Defaults	The default monitoring period is 600 seconds.
Command Mode	NFPP configuration mode
Usage Guide	If the isolation period is changed to 0, attackers on the corresponding interface 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.
- The AC supports the global configuration mode.
- 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 displays the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." The message notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system generates 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. The value range is from 1 to 4294967295.
Defaults	The maximum number of monitored hosts is 1000 by default.
Command	NFPP configuration mode

Mode	
Usage Guide	N/A

Configuring the Attack Threshold

- Mandatory.
- The AC supports the global configuration mode and interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system generates 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 generates 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 generates the log "%NFPP_IP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes precedence over interface-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 attacks 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 an interface.

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 interface. *pps*: Indicates the rate limit. The value range is from 1 to 9999.
Defaults	**per-src-ip**: 20 pps. **per-port**: 1000 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 interface. *pps*: Indicates the attack threshold, in pps. The value range is from 1 to 9999.
Defaults	**per-src-ip**: 20 pps. **per-port**: 1500 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 interface. *rate-limit-pps*: Indicates the rate limit. The value range is from 1 to 9999. *attack-threshold-pps*: Indicates the attack threshold. The value range is from 1 to 9999.
Defaults	By default, no rate limit and attack threshed are configured for an interface, 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.
- The AC supports the global configuration mode and interface configuration mode.
- IP scanning attack may occur 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 count exceeds the scanning threshold.

Command	**ip-guard scan-threshold** *pkt-cnt*
Parameter Description	*pkt-cnt*: Indicates the scanning threshold. The value range is from 1 to 9999.
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. The value range is from 1 to 9999.
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.
- The AC supports the global configuration mode.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.

- If the table of trusted hosts is full, the system generates 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 generates 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 generates 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 generates 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 generates 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, configure the host to be trusted. The trusted host can send ARP packets to the CPU. In this case, the device does not rate-limit such packets or generate alarms.

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 matching the trusted host configuration) exceeds the attack threshold or scanning threshold, attack information is displayed.
- If the rate of attack packets matches the trusted host configuration, no information is displayed.

Configuration Example

CPU Protection Based on IP Attack Defense

Scenario	• IP host attacks exist in the system, and packets of some hosts cannot be properly routed or forwarded. • IP scanning exists in the system, causing a high CPU usage. • Traffic of some hosts is heavy in the system, and the traffic needs to be allowed.
Configuration Steps	• Configure the host-based attack threshold. • Configure the IP scanning threshold. • Set the isolation period to a non-zero value. • Configure trusted hosts.

	`Hostname# configure terminal`
	`Hostname(config)# nfpp`
	`Hostname(config-nfpp)#ip-guard rate-limit per-src-ip 20`
	`Hostname(config-nfpp)#ip-guard attack-threshold per-src-ip 30`

	Hostname(config-nfpp)#ip-guard isolate-period 180 Hostname(config-nfpp)#ip-guard trusted-host 192.168.201.46 255.255.255.255
Verification	● Run the **show nfpp ip-guard summary** command to display the configuration.
	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 Attack Defense

Configuration Effect

- ICMP attacks are identified based on hosts or interfaces. In host-based attack identification, ICMP attacks are identified based on the source IP address, VLAN ID, and interface. 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 generates alarms 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 precedence over that in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Step

Enabling Attack Detection

- (Mandatory) Attack detection is enabled by default.
- The AC supports the global configuration mode and interface configuration mode.
- If ICMP attack defense is disabled, the system automatically clears monitored hosts.

Command	**icmp-guard enable**
Parameter Description	N/A
Defaults	ICMP attack defense is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp icmp-guard enable**
Parameter Description	N/A
Defaults	ICMP attack defense is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	ICMP attack defense configured in interface configuration mode takes precedence over that in global configuration mode.

Configuring the Isolation Period

- Optional. Isolation is disabled by default.
- If the packet rate of attackers exceeds the rate limit of the CPP, configure the isolation period for the device to directly discard packets and therefore save bandwidth resources.
- The AC supports the global configuration mode and interface configuration mode.
- 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 seconds. It can be set to 0 or any value from 30 to 86400. 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 the global isolation period and interface-based isolation period (local isolation period). For an interface, if the interface-based isolation period is not configured, the global isolation period is used; otherwise, the interface-based isolation period is used.

Command	**nfpp icmp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period, in seconds. It can be set to 0 or any value from 30 to 86400. 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 used as the attacker monitoring period, and the configured monitoring period does not take effect.
- The AC supports the global configuration mode.

Command	**icmp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period, in seconds. The value ranges from 180 to 86400.
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 configures 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 on the corresponding interface 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.
- The AC supports the global configuration mode.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to be smaller than 1000. In this case, the system does not delete monitored hosts but displays the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." The message notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system generates 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	*number*: Indicates the maximum number of monitored hosts. The value range is from 1 to

Description	4294967295.
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 be smaller than 1000. In this case, the system does not delete monitored hosts but displays the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." The message notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system generates 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.
- The AC supports the global configuration mode and interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system generates 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 generates 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 generates the log "%NFPP_ICMP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source IP address-based rate limiting takes precedence over interface-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 attacks 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 an interface.

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 interface. *pps*: Indicates the rate limit. The value range is from 1 to 9999.
Defaults	For the AC, see the specification and limitation document. For the AP: **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 interface. *pps*: Indicates the attack threshold, in pps. The value range is from 1 to 9999.
Defaults	For the AC, see the specification and limitation document. For the AP: **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 interface. *rate-limit-pps*: Indicates the rate limit. The value range is from 1 to 9999. *attack-threshold-pps*: Indicates the attack threshold. The value range is from 1 to 9999.
Defaults	By default, no rate limit and attack threshed are configured for an interface, 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.
- The AC supports the global configuration mode.
- If any entry matching a trusted host (IP addresses are the same) exists in the table of monitored hosts, the system automatically deletes this entry.
- If the table of trusted hosts is full, the system generates 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 generates 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 generates 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 generates 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 generates 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, configure the host to be trusted. The trusted host can send ICMP packets to the CPU. In this case, the device does not rate-limit such packets or generate alarms. 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 matching the trusted host configuration) exceeds the attack threshold or scanning threshold, attack information is displayed.
- If the rate of attack packets matches the trusted host configuration, no information is displayed.

Configuration Example

CPU Protection Based on ICMP Attack Defense

Scenario	● ICMP host attacks exist in the system, and some hosts cannot ping devices. ● Traffic of some hosts is heavy in the system, and the traffic needs to be allowed.
Configuration Steps	● Configure the host-based attack threshold. ● Set the isolation period to a non-zero value. ● Configure trusted hosts.

	`Hostname# configure terminal`
	`Hostname(config)# nfpp`
	`Hostname(config-nfpp)#icmp-guard rate-limit per-src-ip 20`
	`Hostname(config-nfpp)#icmp-guard attack-threshold per-src-ip 30`
	`Hostname(config-nfpp)#icmp-guard isolate-period 180`
	`Hostname(config-nfpp)#icmp-guard trusted-host 192.168.201.46 255.255.255.255`

Verification	● Run the **show nfpp icmp-guard summary** command to display the configuration.

	`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 Attack Defense

Configuration Effect

DHCP attacks are identified based on hosts or interfaces. In host-based attack identification, DHCPv6 attacks are identified based on the link-layer source IP address, VLAN ID, and interface. 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 generates alarms 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 precedence over that in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Step

↘ Enabling Attack Detection

- Mandatory. Attack detection is enabled by default.
- The AC supports the global configuration mode and interface configuration mode.
- If DHCP attack defense is disabled, the system automatically clears monitored hosts.

Command	**dhcp-guard enable**
Parameter Description	N/A
Defaults	DHCP attack defense is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp dhcp-guard enable**
Parameter Description	N/A
Defaults	DHCP attack defense is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	DHCP attack defense configured in interface configuration mode takes precedence 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 CPP, configure the isolation period for the device to directly discard packets and therefore save bandwidth resources.
- The AC supports the global configuration mode and interface configuration mode.
- If the isolation period is changed to 0, attackers on the corresponding interface is deleted, instead of being monitored by software.

Command	**dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period, in seconds. It can be set to 0 or any value from 30 to 86400. 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 the global isolation period and port-based isolation period (local isolation period). For an interface, if the interface-based isolation period is not configured, the global isolation period is used; otherwise, the interface-based isolation period is used.

Command	**nfpp dhcp-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period, in seconds. It can be set to 0 or any value from 30 to 86400. 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 used as the attacker monitoring period, and the configured monitoring period does not take effect.
- The AC supports the global configuration mode.

Command	**dhcp-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period, in seconds. The value ranges from 180 to 86400.
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 on the corresponding interface 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.
- The AC supports the global configuration mode.
- If the number of monitored hosts exceeds 1000 (default value), the administrator can set the maximum number of monitored hosts to be smaller than 1000. In this case, the system does not delete monitored hosts but displays the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." The message notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system generates 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. The value range is from 1 to 4294967295.
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 be smaller than 1000. In this case, the system does not delete monitored hosts but displays the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." The message notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system generates 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.
- The AC supports the global configuration mode and interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system generates 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 generates 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 generates the log "%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes precedence 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 attacks 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 an interface.

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 interface. *pps*: Indicates the rate limit. The value range is from 1 to 9999.
Defaults	For the AC, The default rate limit varies with the product model. For the AP, the default rate limit for packets based on source MAC address is 5 pps, and the default rate limit for packets based on interfaces 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 interface. *pps*: Indicates the attack threshold, in pps. The value range is from 1 to 9999.
Defaults	For the AC, the default rate limit varies with the product model. For the AP, the default rate limit for packets based on source MAC address is 10 pps, and the default rate limit for packets based on interfaces 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	**per-src-mac:** Configures the rate limit and attack threshold for each source MAC address**.**

Description	**per-port:** Configures the rate limit and attack threshold for each interface. *rate-limit-pps*: Indicates the rate limit. The value range is from 1 to 9999. *attack-threshold-pps*: Indicates the attack threshold. The value range is from 1 to 9999.
Defaults	By default, no rate limit and attack threshed are configured for an interface, 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 attack defense, you can configure a maximum of 500 MAC addresses not to be monitored.
- The AC supports the global configuration mode.
- 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 generates 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 generates 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 generates 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 generates 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 generates 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, configure the host to be trusted. In this case, the device does not rate-limit such packets or generate alarms.

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 matching the trusted host configuration) exceeds the attack threshold or scanning threshold, attack information is displayed.
- If the rate of attack packets matches the trusted host configuration, no information is displayed.

Configuration Example

CPU Protection Based on DHCP Attack Defense

Scenario	● DHCP host attacks exist in the system, and some hosts fail to request IP addresses. ● DHCP traffic of some hosts is heavy in the system, and the traffic need to be allowed.
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 configuration.

	`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 Attack Defense

Configuration Effect

DHCPv6 attacks are identified based on hosts or interfaces. In host-based attack identification, DHCPv6 attacks are identified based on the link-layer source IP address, VLAN ID, and interface. 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 generates alarms 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 precedence over that in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Step

Enabling Attack Detection

- Mandatory. Attack detection is enabled by default.
- The AC supports the global configuration mode and interface configuration mode.
- If DHCPv6 attack defense is disabled, the system automatically clears monitored hosts.

Command	**dhcpv6-guard enable**
Parameter Description	N/A
Defaults	DHCPv6 attack defense is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	N/A

Command	**nfpp dhcpv6-guard enable**
Parameter Description	N/A
Defaults	DHCPv6 attack defense is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	DHCPv6 attack defense configured in interface configuration mode takes precedence 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 CPP, configure the isolation period for the device to directly discard packets and therefore save bandwidth resources.
- The AC supports the global configuration mode and interface configuration mode.
- If the isolation period is changed to 0, attackers on the corresponding interface is deleted, instead of being monitored by software.

Command	**dhcpv6-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period, in seconds. It can be set to 0 or any value from 30 to 86400. 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 the global isolation period and port-based isolation period (local isolation period). For an interface, if the interface-based isolation period is not configured, the global isolation period is used; otherwise, the interface-based isolation period is used.

Command	**nfpp dhcpv6-guard isolate-period** [*seconds* | **permanent**]
Parameter Description	*seconds*: Indicates the isolation period, in seconds. It can be set to 0 or any value from 30 to 86400. 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 used as the attacker monitoring period, and the configured monitoring period does not take effect.
- The AC supports the global configuration mode.

Command	**dhcpv6-guard monitor-period** *seconds*
Parameter Description	*seconds*: Indicates the monitoring period, in seconds. The value ranges from 180 to 86400.
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 on the corresponding interface 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.
- The AC supports the global configuration mode.
- 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 displays the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." The message notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted.
- If the table of monitored hosts is full, the system generates 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. The value range is from 1 to 4294967295.
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 displays the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." The message notifies the administrator that the configuration does not take effect and that some monitored hosts need to be deleted. If the table of monitored hosts is full, the system generates 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.
- The AC supports the global configuration mode and interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system generates 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 generates 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 generates the log "%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory." to notify the administrator.
- Source MAC address-based rate limiting takes precedence over interface-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 attacks 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 an interface.

Command	**dhcpv6-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 interface. *pps*: Indicates the rate limit. The value range is from 1 to 9999.
Defaults	For the AC, the default rate limit varies with the product model. For the AP, the default rate limit for packets based on source MAC address is 5 pps, and the default rate limit for packets based on interfaces is 150 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 interface. *rate-limit-pps*: Indicates the rate limit. The value range is from 1 to 9999. *attack-threshold-pps*: Indicates the attack threshold. The value range is from 1 to 9999.
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 attack defense, you can configure a maximum of 500 MAC addresses not to be monitored.
- The AC supports the global configuration mode.
- 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 generates 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 generates 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 generates 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 generates 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 generates 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, configure the host to be trusted. This trusted host can send DCHPv6 packets to the CPU. In this case, the device does not rate-limit such packets or generate alarms.

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 matching the trusted host configuration) exceeds the attack threshold or scanning threshold, attack information is displayed.
- If the rate of attack packets matches the trusted host configuration, no information is displayed.

Configuration Example

CPU Protection Based on DHCPv6 Attack Defense

Scenario	• DHCPv6 host attacks exist in the system, and DHCPv6 neighbor discovery fails on some hosts. • DHCPv6 traffic of some hosts is heavy in the system, and the traffic needs to be allowed.
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 configuration.

	`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 Attack Defense

Configuration Effect

- AR ND attack defense classifies ND packets into three types:

  (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: RA packets are used to advertise the gateway and prefix, while Redirect packets are used to advertise a better next hop.

- Only interface-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 generates alarms 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 precedence over that in global configuration mode.
- Isolation is disabled by default. If isolation is enabled, attackers will occupy entries of the security module.

Configuration Step

↘ Enabling Attack Detection

- Mandatory. Attack detection is enabled by default.
- The AC supports the global configuration mode and interface configuration mode.

Command	**nd-guard enable**
Parameter	-

Description	
Defaults	ND attack defense is enabled by default.
Command Mode	NFPP configuration mode
Usage Guide	-

Command	**nfpp nd-guard enable**
Parameter Description	-
Defaults	ND attack defense is configured in global configuration mode, but not in interface configuration mode.
Command Mode	Interface configuration mode
Usage Guide	ND attack defense configured in interface configuration mode takes precedence over that configured in global configuration mode.

Configuring the Attack Threshold

- Mandatory.
- The AC supports the global configuration mode and interface configuration mode.
- If the configured rate limit is greater than the attack threshold, the system generates 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 generates 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 generates 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 attacks 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 an interface.

Command	**nd-guard rate-limit per-port** [**ns-na**	**rs**	**ra-redirect**] *pps*
Parameter Description	**ns-na:** Indicates NS and NA packets. **rs:** Indicates RS packets. **ra-redirect:** Indicates RA and Redirect packets. *pps:* Indicates the rate limit. The value range is from 1 to 9999.
Defaults	For the AC, the default attack threshold varies with the product model. For the AP, the default attack threshold for NS, NA, RS, RA, and 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 NS and NA packets. **rs:** Indicates RS packets. **ra-redirect:** Indicates RA and Redirect packets. *pps*: Indicates the attack threshold, in pps. The value range is from 1 to 9999.
Defaults	For the AC, the default attack threshold varies with the product model. For the AP, the default attack threshold for NS, NA, RS, RA, and 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 NS and NA packets. **rs:** Indicates RS packets. **ra-redirect:** Indicates RA and Redirect packets. *rate-limit-pps*: Indicates the rate limit. The value range is from 1 to 9999. *attack-threshold-pps*: Indicates the attack threshold. The value range is from 1 to 9999.
Defaults	By default, no rate limit and attack threshed are configured for an interface, 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 interfaces into two types: untrusted interfaces (connecting the host) and trusted interfaces (connecting to the gateway). As the traffic volume on a trusted interface is greater than that on an untrusted interface, the rate limit for a trusted interface is higher than that for an untrusted interface. If ND snooping is enabled for a trusted interface, ND snooping sets the rate limit to 800 pps and the attack threshold to 900 pps for the three types of packets on the interface by advertising ND attack defense. ND attack defense 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 AC or AP.
- If the table of trusted hosts is full, the system generates 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 generates 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 generates 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 generates 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 generates 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, configure the host to be trusted. This trusted host can send ND packets to the CPU. In this case, the device does not rate-limit such packets or generate alarms.

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 matching the trusted host configuration) exceeds the attack threshold or scanning threshold, attack information is displayed.
- If the rate of attack packets matches the trusted host configuration, no information is displayed.

Configuration Example

CPU Protection Based on ND Attack Defense

Scenario	● ND host attacks exist in the system, and neighbor discovery fails on some hosts. ● ND traffic of some hosts is heavy in the system, and the traffic needs to be allowed.
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 configuration.

	`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

Configure centralized rate limiting and distribution so that management and protocol packets are first processed when the network is busy.

Notes

The valid percentage range of a type of packets must be equal to or smaller than 100% minus the percentage of the sum of the other two types.

Configuration Step

Configuring the Maximum Bandwidth for Each Type of Packets

- Mandatory. Management, routing, and protocol packets share the same default bandwidth. For details, see *Product Features*.
- The AC supports the global configuration mode.

Command	**cpu-protect sub-interface** { **manage** | **protocol** | **route** } **pps** *pps_value*
Parameter Description	**manage**: Specifies management packets. **protocol**: Specifies protocol packets. **route**: Specifies routing packets. *pps_value*: Indicates the rate limit. The value range is from 1 to 500000.
Defaults	For the AC, the default attack threshold varies with the product model. For the AP, the default rate limit of management, protocol, and routing packets is 3000 pps.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Maximum Percentage of Each Type of Packets in the Queue

- Mandatory. By default, management packets occupy 30% of the bandwidth, routing packets occupy 40%, and protocol packets occupy 25%.
- The AC supports the global configuration mode.

Command	**cpu-protect sub-interface** { **manage** | **protocol** | **route** } **percent** *percent_value*
Parameter Description	**manage**: Specifies management packets. **protocol**: Specifies protocol packets. **route**: Specifies routing packets. *percent_value*: Indicates the percentage of a type of packets in the queue. The value range is from 1 to 100.

Defaults	**manage**: 30% **protocol**: 25% **route**: 40%
Command Mode	Global configuration mode
Usage Guide	The valid percentage range of a type of packets must be equal to or smaller than 100% minus the percentage of the sum of the other two types.

Configuration Example

↘ Prioritizing Packets Sent to the CPU Through Centralized Distribution

Scenario	Various types of mass packets exist on a network and belong to different centralized types.
Configuration Steps	● Configure the maximum bandwidth for each type of packets. ● Configure the maximum percentage of each type of packets in the queue.

	`Hostname# configure terminal`
	`Hostname(config)# cpu-protect sub-interface manage pps 5000`
	`Hostname(config)# cpu-protect sub-interface manage percent 25`

Verification	Omitted.

1.4.8 Configuring NFPP Log Information

Configuration Effect

The NFPP-enabled device 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 generated in the log buffer, even if attacks are stopped.

Configuration Step

↘ 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.
- The AC supports the global configuration mode.

Command	**log-buffer entries** *number*
Parameter Description	*number*: Indicates the buffer size, which is expressed in the number of logs. The value range is from 0 to 1024.
Defaults	The default buffer size is 256.

Command Mode	NFPP configuration mode
Usage Guide	N/A

Configuring the System Message Generation Rate

- Mandatory.
- The system message generation rate depends on 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.
- The AC supports the global configuration mode.

Command	**log-buffer logs** *number_of_message* **interval** *length_in_seconds*
Parameter Description	*number_of_message*: Indicates the number of system messages. The value range is from 0 to 1024. The value 0 indicates that all logs are recorded in the log buffer and no system message is generated. *length_in_seconds*: Indicates the time segment length. The value range is from 0 to 86400 (1 day). The value 0 indicates that logs are not recorded in the log buffer but system messages are instantly generated. If ***number_of_message*** and ***length_in_seconds*** are 0, logs are not recorded in the log buffer but system messages are instantly generated. *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	N/A

Enabling Log Filtering

- Optional. Log filtering is disabled by default.
- Logs can be filtered based on an interface or VLAN.
- If log filtering is enabled, logs not meeting the filtering rule are discarded.
- The AC supports the global configuration mode.

Command	**logging vlan** *vlan-range*
Parameter Description	*vlan-range*: Records logs in a specified VLAN range, for example, 1-3,5 for example.
Defaults	All logs are recorded by default.
Command Mode	NFPP configuration mode
Usage Guide	This command is used to filter logs so that only logs in the specified VLAN range are recorded. For interface-based and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Command	**logging interface** *interface-id*
Parameter	*interface-id*: Records logs of a specified interface.

Description	
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 interface are recorded. For interface-based and VLAN-based log filtering, if either rule is met, logs are recorded in the log buffer.

Configuration Example

↘ CPU Protection Based on ND Attack Defense

Scenario	If there are too many attackers, log generation 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 configuration.

	`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

Command	Description
clear nfpp arp-guard scan	Clears the ARP attack defense scanning table.
clear nfpp arp-guard hosts	Clears monitored hosts in ARP attack defense.

Command	Description
clear nfpp ip-guard hosts	Clears monitored hosts in IP attack defense.
clear nfpp icmp-guard hosts	Clears monitored hosts in IMCP attack defense.
clear nfpp dhcp-guard hosts	Clears monitored hosts in DHCP attack defense.
clear nfpp dhcpv6-guard hosts	Clears monitored hosts in DHCPv6 attack defense.
clear nfpp log	Clears logs.

Displaying

Command	Description
show nfpp arp-guard summary	Displays configuration parameters of ARP attack defense.
show nfpp arp-guard hosts	Displays monitored hosts of ARP attack defense.
show nfpp arp-guard scan	Displays the ARP attack defense scanning table.
show nfpp arp-guard trusted-host	Displays trusted hosts in ARP attack defense.
show nfpp ip-guard summary	Displays configuration parameters of IP attack defense.
show nfpp ip-guard hosts	Displays monitored hosts in IP attack defense.
show nfpp ip-guard trusted-host	Displays trusted hosts in IP attack defense.
show nfpp icmp-guard summary	Displays configuration parameters of ICMP attack defense.
show nfpp icmp-guard hosts	Displays monitored hosts in ICMP attack defense.
show nfpp icmp-guard trusted-host	Displays trusted hosts in ARP attack defense.
show nfpp dhcp-guard summary	Displays configuration parameters of DHCP attack defense.
show nfpp dhcp-guard hosts	Displays monitored hosts in DHCP attack defense.
show nfpp dhcp-guard trusted-host	Displays trusted hosts in DHCP attack defense.
show nfpp dhcpv6-guard summary	Displays configuration parameters of DHCPv6 attack defense.
show nfpp dhcpv6-guard hosts	Displays monitored hosts in DHCPv6 attack defense.
show nfpp dhcpv6-guard trusted-host	Displays trusted hosts in DHCPv6 attack defense.
show nfpp nd-guard summary	Displays configuration parameters of ND attack defense.
show nfpp nd-guard trusted-host	Displays trusted hosts in ND attack defense.
show nfpp log summary	Displays NFPP logs.
show nfpp log buffer [**statistics**]	Displays the NFPP log buffer.

1 Configuring Password Policy

1.1 Overview

The password policy is provided for local authentication of the device, and is used to control users' login passwords and login status.

Protocols and Standards

N/A

1.2 Features

Basic Concepts

Minimum Password Length

An administrator can set the minimum length for user passwords according to system security requirements. If the input password 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 the password is cracked. 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. To ensure security, an administrator can enable the strong password detection function to ensure that the configured passwords are correctly configured. 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

Special Password Character Detection

Special characters include space, tilde (~), apostrophe (`), exclamation mark (!), at sign (@), number sign (#), dollar sign ($), percent (%), caret (^), ampersand (&), asterisk (*), parentheses (()), underscore (_), plus sign (+), hyphen (-), equal sign (=), braces ({}), vertical bar (|), brackets ([]), backslash (\), colon (:), quotation marks ("), semicolon (;), single quotation mark ('), angle brackets (<>), comma (,), period (.), and slash (/). If a password contains these special characters, the password is weak and may be easily cracked. To ensure security, an administrator can enable the special password character detection function to ensure that the configured passwords do not contain any special character. After the special password character detection function is enabled, a prompt will be displayed for passwords containing special characters.

Password Lifecycle

The password lifecycle defines the validity time of a user password. When the service time of a password exceeds the lifecycle, the user needs to change the password.

If the user inputs a password that has already expired during login, the system will display a message, 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 different, the system will ask the user to input the new password once again.

Limitation on Repeated Use of Passwords

When changing the password, a user will set a new password while the old password will be recorded as historical records. If the new password input by the user has been used previously, the system displays an error message and asks the user to specify another password.

The maximum number of password historical records per user can be configured. When the number of password historical records of a user is greater than the maximum number configured for this user, the new password historical record will overwrite the user's oldest password historical record.

Storage of Encrypted Passwords

An administrator can enable storage of encrypted passwords considering security. When an administrator runs the **show running-config** command to display the configuration or run the **write** command to save configuration files, various configured passwords are displayed in cipher text format. If the administrator disables storage of encrypted passwords next time, the passwords that use the cipher text format will not be restored to cleartext passwords.

1.3 Configuration

Configuration	Description and Command	
Configuring the Password Security Policy	⚠ (Optional configuration) It is used to configure a combination of parameters related to the password security policy.	
	password policy life-cycle	Configures the password lifecycle.
	password policy min-size	Configures the minimum length of user passwords.
	password policy no-repeat-times	Configures the number of times for repeated use of latest passwords.
	password policy strong	Enables the strong password detection function.
	service password-encryption	Enables storage of encrypted passwords.

1.3.1 Configuring the Password Security Policy

Configuration Effect

Provide a password security policy for local authentication of the device. You can configure different password security policies to implement password security management.

Notes

The configured password security policy is valid for global passwords (configured using **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 Step

Configuring the Password Lifecycle

- Optional.
- Perform this configuration on each device unless otherwise specified.

Configuring the Minimum Length of User Passwords

- Optional.
- Perform this configuration on each device unless otherwise specified.

Setting the Number of Times for Repeated Use of Latest Passwords

- Optional.
- Perform this configuration on each device unless otherwise specified.

Enabling the Strong Password Detection Function

- Optional.
- Perform this configuration on each device unless otherwise specified.

Enabling torage of Encrypted Passwords

- Optional.
- Perform this configuration on each device unless otherwise specified.

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 Lifecycle

Command Syntax	**password policy life-cycle** *days*
Parameter Description	*days*: Indicates the password lifecycle, in days. The value range is from 1 to 65535.
Command Mode	Global configuration mode
Usage Guide	The password lifecycle is used to define the validity period of user passwords. If the user logs in with a password whose service time already exceeds the lifecycle, a prompt is displayed, asking the user to change the password.

Configuring the Minimum Length of User Passwords

Command	**password policy min-size** *length*

Syntax	
Parameter Description	*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 Number of Times for Repeated Use of Latest Passwords

Command Syntax	**password policy no-repeat-times** *times*
Parameter Description	*times*: Indicates the number of times for repeated use of latest passwords. 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 recent times will be recorded as password historical records. If the new password input by the user has been used previously, the system displays an error prompt and the password change fails. You can configure the maximum number of password historical records per user. When the number of password historical records of a user is greater than the maximum number configured for the user, the new password historical record will overwrite the user's oldest password historical record.

Enabling the Strong Password Detection Function

Command Syntax	**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 Syntax	**service password-encryption**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Before storage of encrypted passwords is enabled, all passwords will be displayed and stored in cleartext format, unless the passwords are configured in cipher text format. You can enable storage of encrypted passwords considering security. When you run the **show running-config** command to

	display the configuration or run the **write** command to save configuration files, various configured passwords are displayed in cipher text format. If you disable storage of encrypted passwords next time, the passwords that use the cipher text format will not be restored to cleartext passwords.

Checking Configured Password Security Policy Information

Command Syntax	**show password policy**
Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, or 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 the configuration related to a password security policy.

Configuring Password Security Check on the Device

Typical Application	There are the following password security requirements on a network: 1. The passwords has a minimum of eight characters. 2. The password lifecycle is 90 days. 3. Passwords are stored and transmitted in cipher text format. 4. The number of times for repeated use of recent passwords is 3. 5. Passwords cannot be the same as user names, and cannot contain simple characters or digits only.

Configuration Steps	● Set the minimum length of passwords to 8.
	● Set the password lifecycle to 90 days.
	● Enable storage of encrypted passwords.
	● Set the number of times for repeated use of recent passwords 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 detection according to the password security policy.
	● Run the **show password policy** command to display 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 providing a pre-warning notification about password expiry is greater than the password lifecycle.

1.4 Monitoring

Displaying

Command	Function
show password policy	Displays configured password security policy information.

1 Configuring SSH

1.1 Overview

A Secure Shell (SSH) connection is similar to a Telnet connection except that all data transmitted over SSH is encrypted. When a user on an insecure network logs into a device remotely, SSH helps ensure information security and powerful authentication, protecting the device against attacks such as IP address spoofing and cleartext 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 an SSH server. In this way, the local device can securely log in to a remote device through SSH to implement management.

The device can work as either the SSH server or an SSH client, and supports SSHv1 and SSHv2. It supports IPv4 and IPv6 SSH.

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 Authentication	Use local line password authentication for SSH user authentication.
SSH AAA Authentication	Use the authentication, authorization and accounting (AAA) mode for SSH user authentication.
SSH Public Key Authentication	Use public key authentication for SSH user authentication.

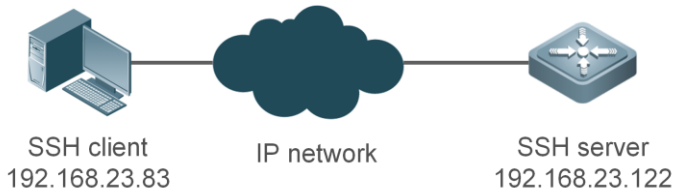
Application	Description
SSH File Transfer	Use Secure Copy (SCP) commands on the SSH client to exchange data with the SSH server.
SSH Client Application	Use the SSH client to securely log in to a remote device for management.

1.2.1 SSH Device Management

Scenario

To use SSH to manage devices, ensure that the SSH server is enabled. By default, the SSH server is disabled. The Telnet component that comes with the Windows system does not support SSH. Therefore, a third-party client software must be used. Well-compatible software includes PuTTY, Linux, and SecureCRT. PuTTY is used as an example to introduce the configuration of the SSH client. Figure 1-1 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, enter the host IP address of the SSH server and SSH port number 22, and select the connection type of SSH.
- On the **SSH** option tab of PuTTY, select preferred SSH protocol version 2.
- On the **SSH authentication** option tab of PuTTY, select the authentication method of **Attempt "keyboard-interactive" auth**.
- Click **Open** to connect to the SSH server.
- Enter the correct user name and password to access the terminal login interface.

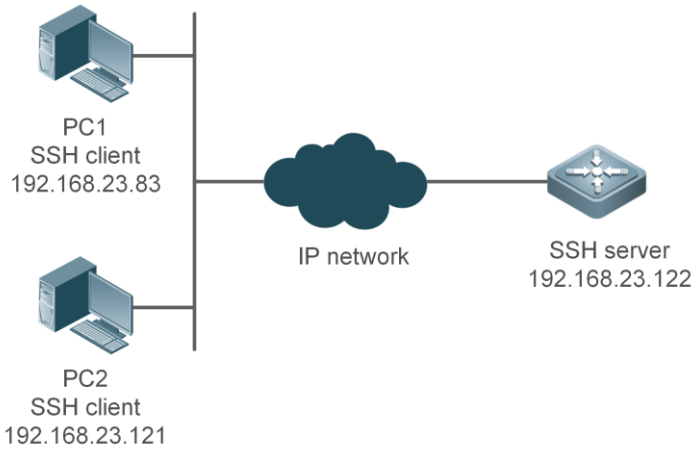
1.2.2 SSH Local Line Authentication

Scenario

SSH clients can use the local line password authentication mode, as shown in Figure 1-2. 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 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 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 cleartext with the password stored on the server, and returns a message about authentication success or failure. SSHv1 uses an RSA key, whereas SSHv2 adopts a Rivest-Shamir-Adleman (RSA) or Digital Signature Algorithm (DSA) key.

3 Configure the IP address of FastEthernet 0/1 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. PuTTY is used 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.

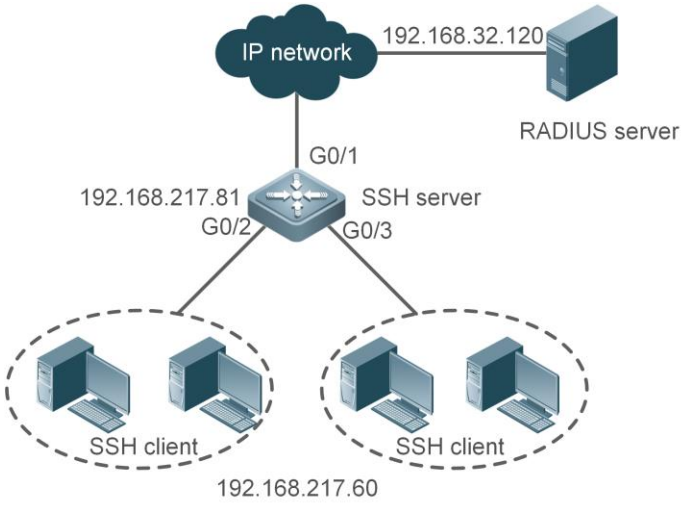
2 Set the IP address and connected port ID of the SSH server. As shown in the network topology, the IP address of the server is 192.168.23.122, and the port ID is 22. Click **Open** to start the connection. Because the current authentication mode does not require a user name, you can enter any user name, which cannot be empty. (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 1-3. To ensure security of data exchange, PCs function as the SSH clients and use SSH 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, local authentication is used.

Figure 1-3 Networking Topology of SSH AAA Authentication



Deployment

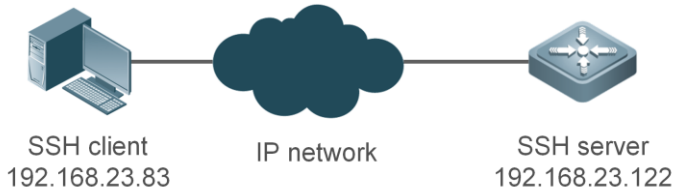
- Configure reachable routes from the SSH clients to the SSH server and from the SSH server to the RADIUS server.
- Configure the SSH server on the network device.
- Configure AAA parameters on the network device. When the AAA authentication mode is used, method lists are created to define identity authentication and types, and applied to a specified service or interface.

1.2.4 SSH Public Key Authentication

Scenario

SSH clients can use public keys for authentication, and the public key algorithm can be RSA or DSA, as shown in Figure 1-4. 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

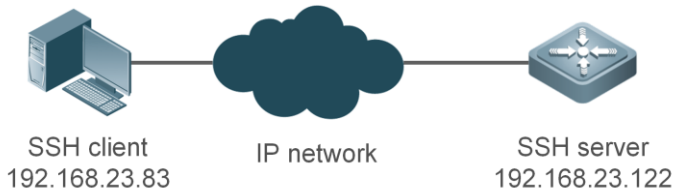
- To implement public key authentication for the client, configure the client to generate a key pair (RSA or DSA), configure the public key on the SSH server, and select the public key authentication mode.
- After the key is generated on the client, the SSH server will copy the file of the public key from the client to the flash memory 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 1-5.

Figure 1-5 Networking Topology of SSH File Transfer



Deployment

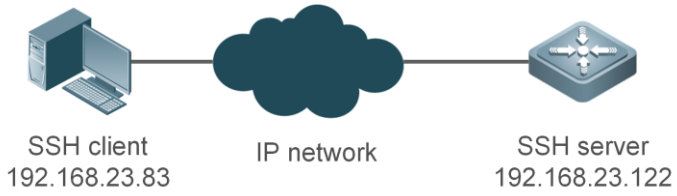
- Enable the SCP service on the server.
- On the client, use SCP commands to upload files to the server, or download files from the server.

1.2.6 SSH Client Application

Scenario

The SSH service is enabled on a remote SSH server, and the **ssh** command is used on the local client to set up an SSH connection with the server for secure data transmission, as shown in Figure 1-6.

Figure 1-6 Networking Topology of SSH Client Application



Deployment

- Enable the SSH service on the server.
- On the client, run the **ssh** command to set up an SSH connection with the server for secure data transmission.

1.3 Features

Basic Concepts

↘ User Authentication Mechanism

- Password authentication

During 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 successful or failed authentication.

- Public key authentication

During 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. The 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 not, the server directly sends an authentication failure message. If so, the server performs digital signature authentication on the client, and returns a message indicating successful or failed authentication.

Public key authentication is applicable only to SSHv2 clients.

SSH Communication

To ensure secure communication, interaction between an SSH server and an SSH client involves 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 algorithm negotiation are performed. The server and 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 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 is terminated and the session is ended.

Overview

Feature	Description
SSH Server	Enable the SSH server function on a network device for setting up a secure connection with 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, ensuring security.
SSH Client	The SSH client is used to set up a secure connection with a remote network device enabled with the SSH server.

1.3.1 SSH Server

Enable the SSH server function on a network device for setting up a secure connection with the SSH client. You can also disable the SSH server function to disconnect all SSH clients.

Working Principle

For details about the working principle of the SSH server, see "SSH Communication" In practice, after enabling the SSH server, you can configure the following parameters according to application requirements:

- Version: Configure the SSH version as SSHv1 or SSHv2 to connect SSH clients.
- Authentication timeout: The SSH server starts the timer after receiving a user connection request. The SSH server is disconnected from the client when the authentication succeeds or the authentication timeout is reached.
- Maximum re-authentication count: The SSH server starts authenticating the client after receiving its connection request. If authentication does not succeed after the maximum re-authentication count is reached, the system displays a message 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, that is, it can connect to SSHv1 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 SSHv1 or SSHv2 client can be connected to the SSH server.

Configuring the 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 this 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 Re-authentication Count

By default, the maximum re-authentication count is 3.

Run the **ip ssh authentication-retries** command to configure the maximum re-authentication count on the SSH server. Use the **no** form of this command to restore the default re-authentication count. If authentication still does not succeed when the maximum re-authentication count is reached, user authentication fails.

Specifying the SSH Encryption Mode

By default, the encryption mode supported by the SSH server is compatible. That is, the device supports Cipher Block Chaining (CBC), counter (CTR), and other encryption modes.

Run the **ip ssh cipher-mode** command to configure the encryption mode supported by the SSH server. Use the **no** form of this command to restore the default encryption mode supported by the SSH server.

Specifying the SSH Message Authentication Algorithm

By default, the message authentication algorithms supported by the SSH server are as follows:

(1) For SSHv1, no algorithm is supported.

(2) For SSHv2, MD5, SHA1, SHA1-96, MD5-96, SHA2-256, and SHA2-512 are supported.

Run the **ip ssh hmac-algorithm** command to configure the message authentication algorithm supported by the SSH server. Use the **no** form of the command to restore the default message authentication algorithm supported by the SSH server.

Configuring the DH Key Exchange Algorithm on the SSH Server

By default, Ruijie's SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 for key exchange, while the SSHv1 server dose not support any of them. Run the **ip ssh key-exchange** command to configure the Diffie-Hellman(DH) key exchange algorithm supported by the SSH server. Use the **no** form of this command to restore the default setting.

Setting a Monitoring Port ID for the SSH Server

The default port ID is 22.

Run the **ip ssh port** command to set a monitoring port ID for the SSH server. Use the **no ip ssh port** or **ip ssh port 22** command to restore the default setting.

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 this 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 client.

Working Principle

- SCP supports online file transfer. It runs on port 22 based on the Berkeley Software Distribution (BSD) Remote Copy Protocol (RCP), whereas RCP provides encryption and authentication functions based on SSH. 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 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, and 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 on a network device.

Configuring the Transmission Path for Files of the SCP Server

The default transmission path is **flash:/**.

Run the **ip scp server topdir {flash:/***path* **| flash2:/***path* **| usb0:/***path* **| usb1:/***path* **| sd0:/***path* **| sata0:/***path* **| tmp:/***path* **}** command to configure the transmission path to upload files to or download files from the SCP server.

1.3.3 SSH Client

The SSH client is used to set up a secure connection with a remote network device on which the SSH server runs.

Working Principle

For details about the working principle of the SSH client, see "SSH Communication"

Related Configuration

Specifying the Source Interface of the SSH Client

By default, the source address of SSH packets is queried based on the destination address.

Run the **ip ssh source-interface** *interface-name* command to specify the source interface of the SSH client.

Establishing a Session with the SSH Server

Run the **ssh** command to log in to a remote device that supports the SSH server.

Restoring an Established SSH Session

- Run the **ssh-session** *session-id* command to restore an established SSH session.

Disconnecting a Suspended SSH Session

- Run the **disconnect ssh-session** *session-id* command to disconnect a specified SSH session.

1.4 Configuration

Configuration	Description and Command	
Configuring the SSH Server	(Mandatory) It is used 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 re-authentication count.
	ip ssh cipher-mode { **cbc** | **ctr** | **others** | **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes192-cbc** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **blowfish-cbc** | **des-cbc** }	Specifies the SSH encryption mode.
	ip ssh hmac-algorithm { **md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** }	Specifies the SSH message authentication algorithm.
	ip ssh key-exchange { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** }	Configures the DH key exchange algorithm supported by the SSH server.
	ip ssh port *port*	Sets a monitoring port ID for 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.

Configuration	Description and Command	
	ip scp server topdir { **flash:/***path* | **flash2:/***path* | **usb0:/***path* | **usb1:/***path* | **sd0:/***path* | **sata0:/***path* | **tmp:/***path* }	Configures the transmission path for files of the SCP server.
Configuring the SSH Client	(Optional) It is used to set up a secure connection with a remote network device that supports the SSH server.	
	ip ssh source-interface *interface-name*	Specifies the source interface of the SSH client.
	ssh [**-v** { **1** | **2** }] [**-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** }] [**-l** *username*] [**-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** | **hmac-sha2-256** | **hmac-sha2-512** }] [**-p** *port-num*] { *ip-addr* | *hostname* } [**/source** { **ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name* }]	Establishes an encrypted session with a remote network device.

1.4.1 Configuring the SSH Server

Configuration Effect

- Enable the SSH server on a network device for setting up a secure connection with the SSH client. All interactive data is encrypted before being transmitted.
- 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 re-authentication count.
- You can specify the SSH encryption mode.
- You can specify the SSH message authentication algorithm.
- You can specify an ACL for filtering traffic on the SSH server.

Notes

- Before configuring a device as the SSH server, ensure that communication is smooth on the network that the device resides, and the administrator can access the device management interface to perform the configuration.
- The **no crypto key generate** command does not exist. You need to run the **crypto key zeroize** command to delete a key.
- The SSH module does not support hot standby. Therefore, for the device that supports hot standby on the supervisor modules, if no SSH key file exist on the new active module after failover, you must run the **crypto key generate** command to configure the device to re-generate a key before using SSH.

Configuration Step

Enabling the SSH Server

- Mandatory.
- By default, the SSH server is disabled. In global configuration mode, enable the SSH server and configure the device to generate an SSH key so that the SSH server status changes to ENABLE.

Specifying the SSH Version

- Optional.
- By default, the SSH server supports SSHv1 and SSHv2, that is, it can connect to SSHv1 or SSHv2 clients.

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 range is from 1 to 120, in seconds.

Configuring the Maximum Re-authentication Count

- Optional.
- Configure the maximum re-authentication count to prevent unauthorized behaviors such as malicious guessing. By default, the maximum re-authentication count is 3, that is, a user is allowed to enter the user name and password three times for authentication. You can configure the maximum re-authentication count as required. The value range is from 0 to 5.

Specifying the SSH Encryption Mode

- Optional.
- Specify the encryption mode supported by the SSH server. By default, the encryption mode supported by the SSH server is compatible. That is, the device supports CBC, CTR, and other encryption modes.

Specifying the SSH Message Authentication Algorithm

- Optional.
- Specify the message authentication algorithm supported by the SSH server. By default, the message authentication algorithms supported by the SSH server are as follows: (1) For SSHv1, no algorithm is supported. (2) For SSHv2, four algorithms, including MD5, SHA1, SHA1-96, and MD5-96, are supported.

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 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 re-authentication count of the SSH server.
- Run the **show crypto key mypubkey** command to display public information about 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 so, 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 status 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 an established SSH session. The value range is 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 SSH sessions 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 connection requests sent by SSHv1 clients. **2**: Indicates that the SSH server only receives 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 range is from 1 to 120, in seconds.
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 Re-authentication Count

Command	**ip ssh authentication-retries** *retry times*
Parameter Description	*retry times*: Indicates the maximum re-authentication count. The value range is from 0 to 5.
Command Mode	Global configuration mode
Usage Guide	Run the **no ip ssh authentication-retries** command to restore the default re-authentication count. The default value is 3.

Specifying the SSH Encryption Mode

Command	**ip ssh cipher-mode** { **cbc** | **ctr** | **others** | **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes192-cbc** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **blowfish-cbc** | **des-cbc** }
Parameter Description	**cbc**: Sets the encryption mode supported by the SSH server to CBC. Corresponding algorithms include DES-CBC, 3DES-CBC, AES-128-CBC, AES-192-CBC, AES-256-CBC, and Blowfish-CBC. **ctr**: Sets the encryption mode supported by the SSH server to CTR. Corresponding algorithms include AES128-CTR, AES192-CTR, and AES256-CTR.

	others: Sets the encryption mode supported by the SSH server to others. The corresponding algorithm is RC4.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the encryption mode supported by the SSH server. On Ruijie devices, the SSHv1 server supports DES-CBC, 3DES-CBC, and Blowfish-CBC encryption algorithms; 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 encryption algorithms. These algorithms can be grouped into three 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 have high security requirements can set the encryption mode supported by the SSH server to CTR to enhance security of the SSH server. If the complete set of CBC, CTR, and GCM is configured and their subsets are also configured, for example, if **ip ssh cipher cbc 3des-cbc** is configured, the configuration result indicates the CBC mode.

Specifying the SSH Message Authentication Algorithm Supported by the SSH Server

Command	**ip ssh hmac-algorithm** { **md5** | **md5-96** | **sha1** | **sha1-96** }
Parameter Description	**md5**: Indicates the MD5 algorithm supported by the SSH server. **md5-96**: Indicates the MD5-96 algorithm supported by the SSH server. **sha1**: Indicates the SHA1 algorithm supported by the SSH server. **sha1-96**: Indicates the SHA1-96 algorithm supported by the SSH server.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the message authentication algorithm supported by the SSH server. On Ruijie devices, the SSHv1 server does not support any message authentication algorithm; the SSHv2 server supports the MD5, SHA1, SHA1-96, and MD5-96 message authentication algorithms. You can select message authentication algorithms supported by the SSH server as required.

Configuring the DH Key Exchange Algorithm Supported by the SSH Server

Command	**ip ssh key-exchange** { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** }
Parameter Description	**dh_group_exchange_sha1**: Indicates diffie-hellman-group-exchange-sha1 for key exchange. The key has 2048 bytes, which cannot be edited. **dh_group14_sha1**: Indicates diffie-hellman-group14-sha1 for key exchange. The key has 2048 bytes. **dh_group1_sha1**: Indicates diffie-hellman-group1-sha1 for key exchange. The key has 1024 bytes.
Command Mode	Global configuration mode
Usage Guide	Use this command to configure a DH key exchange method on the SSH server. Ruijie's SSHv1 server does not support DH key exchange method, while the SSHv2 server supports diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, and diffie-hellman-group1-sha1 for key exchange.

Setting a Monitoring Port ID for the SSH Server

Command	**ip ssh port** *port*
Parameter Description	*port*: Indicates the monitoring port ID of the SSH server. The value range is from 1025 to 65535.
Command Mode	Global configuration mode
Usage Guide	Use the **no ip ssh port** or **ip ssh port 22** command to restore the default monitoring port ID of the SSH server.

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	This command is used to configure the RSA public key file associated with a user. For SSHv1 and SSHv2, only SSHv2 supports authentication based on the public key. This command associates the public key file on a 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	This command is used to configure the DSA key file associated with a user. For SSHv1 and SSHv2, only SSHv2 supports authentication based on the public key. This command associates the public key file on a 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 configure the SSH server to generate a RSA public key.

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 RSA key is generated successfully, the following information is displayed:
	`% Generating 512 bit RSA1 keys ...[ok]`
	`% Generating 512 bit RSA keys ...[ok]`
	● If the RSA key fails to be generated, 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 public information about the RSA key. If 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 supported by the SSH server.
SSH Server	Hostname(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1,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(config)#show ip ssh SSH Enable - version 2.0 SSH Port: 22 SSH Cipher Mode: cbc,ctr,others SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1,sha2-256,sha2-512 Authentication timeout: 100 secs Authentication retries: 3 SSH SCP Server: disabled

Configuring the Maximum Re-authentication Count

Configuration Steps	Run the **ip ssh authentication-retries** *retry times* command to set the maximum re-authentication count 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 re-authentication count.

SSH Server	`Hostname(config)#show ip ssh`
	`SSH Enable - version 2.0`
	`SSH Port: 22`
	`SSH Cipher Mode: cbc,ctr,others`
	`SSH HMAC Algorithm: md5-96,md5,sha1-96,sha1,sha2-256,sha2-512`
	`Authentication timeout: 120 secs`
	`Authentication retries: 2`
	`SSH SCP Server: disabled`

Specifying the SSH Encryption Mode

Configuration Steps	Run the **ip ssh cipher-mode** { **cbc** | **ctr** | **others** | **3des-cbc** | **aes128-cbc** | **aes128-ctr** | **aes192-cbc** | **aes192-ctr** | **aes256-cbc** | **aes256-ctr** | **blowfish-cbc** | **des-cbc** } command to set the encryption mode supported by the SSH server to CTR.
SSH Server	`Hostname#configure terminal` `Hostname(config)# ip ssh cipher-mode ctr`
Verification	Select the CTR encryption mode on the SSH client, and check whether you can successfully log in to the SSH server from the SSH client.

Specifying the SSH Message Authentication Algorithm

Configuration Steps	Run the **ip ssh hmac-algorithm** {**md5** | **md5-96** | **sha1** | **sha1-96** | **sha2-256** | **sha2-512** } command to set the message authentication algorithm supported by the SSH server to SHA1.
SSH Server	`Hostname#configure terminal` `Hostname(config)# ip ssh hmac-algorithmsha1`
Verification	Select the SHA1 message authentication algorithm on the SSH client, and check whether you can successfully log in to the SSH server from the SSH client.

Configuring the DH Key Exchange Algorithm Supported by 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 key exchange method on the SSH server.
SSH Server	`Hostname# configure terminal` `Hostname(config)# ip ssh key-exchange dh_group14_sha1`
Verification	Choose diffie-hellman-group14-sha1 on the client terminal and check whether you can log in successfully.

Setting a Monitoring Port ID for the SSH Server

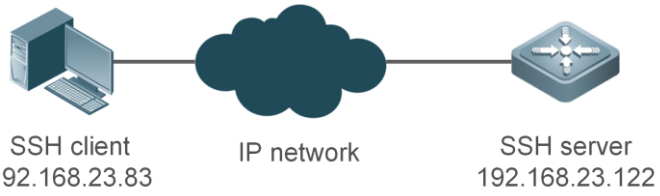
Command	**ip ssh port** *port*
Parameter Description	*port*: Indicates the monitoring port ID of the SSH server. The value range is from 1025 to 65535.
Command Mode	Global configuration mode
Usage Guide	Use the **no ip ssh port** or **ip ssh port 22** command to restore the default monitoring port ID of the

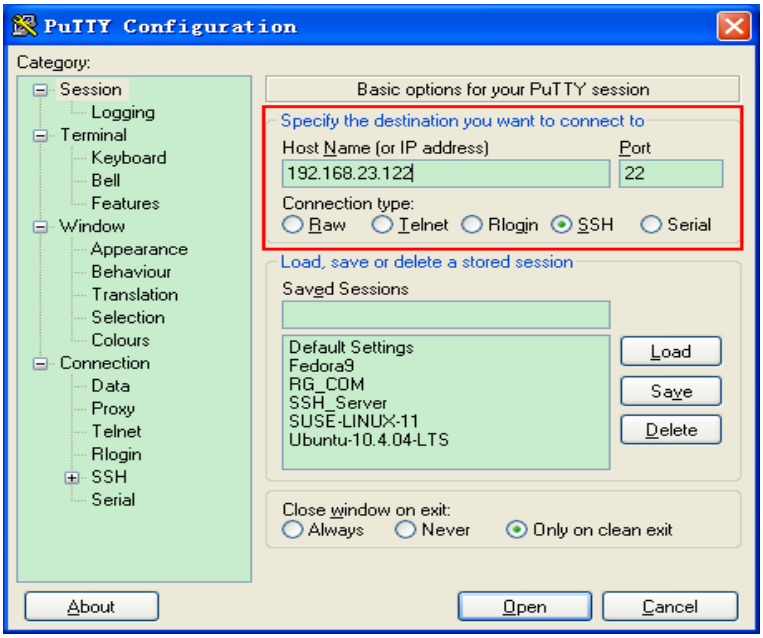
	SSH server.

Configuring Public Key Authentication

Configuration Steps	Run the **ip ssh peer** *username* **public-key** { **rsa** | **dsa** | **ecc**} *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 so, the public key file on the client is successfully associated with the user name, and public key authentication succeeds.

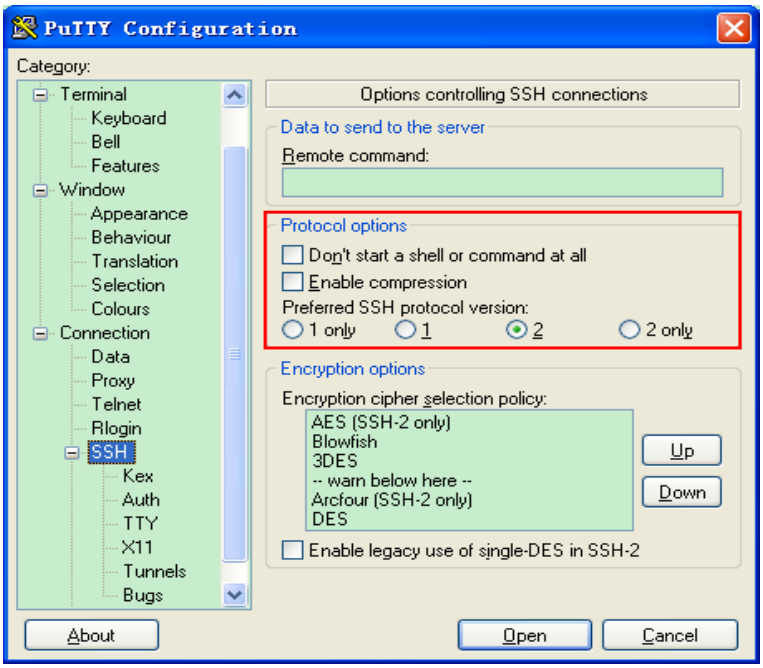
Configuring SSH Device Management

Scenario Figure1-6	 You can use SSH to manage devices only when the SSH server 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. Well-compatible client software includes PuTTY, Linux, and SecureCRT. PuTTY is used as an example to introduce the configuration of the SSH client.
Configuration Steps	• Start the PuTTY software. • On the **Session** option tab of PuTTY, enter 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. • Enter the correct user name and password to access the terminal login interface.
SSH Client	Figure 1-7



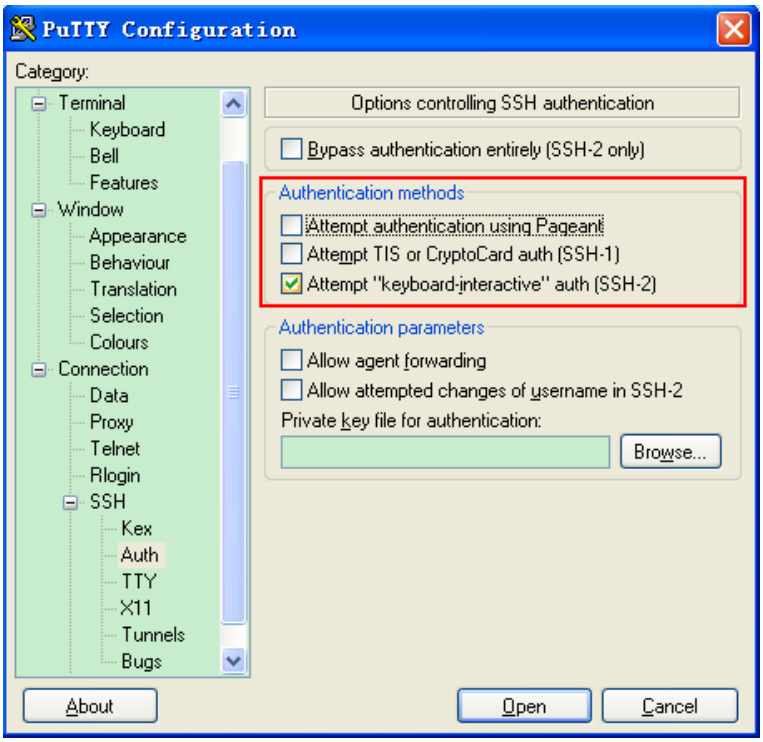
Host Name (or IP address) indicates the IP address of the host to be logged in. In this example, the IP address is **192.168.23.122**. **Port** indicates the port ID 22, that is, default listening port ID. The value of **Connection type** is **SSH**.

Figure 1-8



As shown in Figure 1-8, 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 1-8, select **Attempt "keyboard-interactive" auth** as the authentication method for authentication based on the user name and password.

Click **Open** to connect to the configured server host, as shown in Figure 1-10.

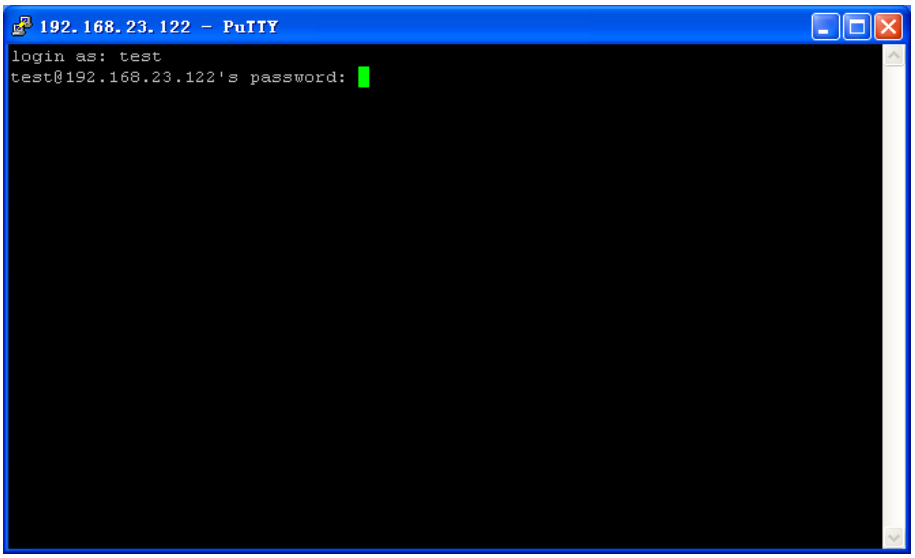
Figure 1-10



The **PuTTY Security Alert** box indicates that you are logging in to the client of the server at 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 1-11.

Figure 1-11



Enter the correct user name and password,. You can log in to the SSH terminal interface, as shown in Figure 1-12.

Figure 1-12

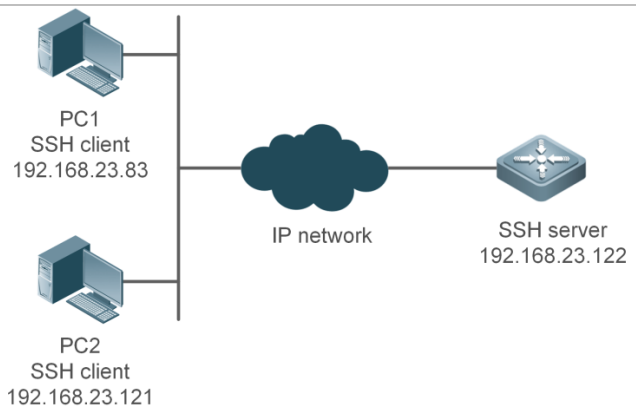


Verification	● Run the **show ip ssh** command to display the effective configuration on the SSH server. ● Run the **show ssh** command to display information about every SSH connection that has been established.

```
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

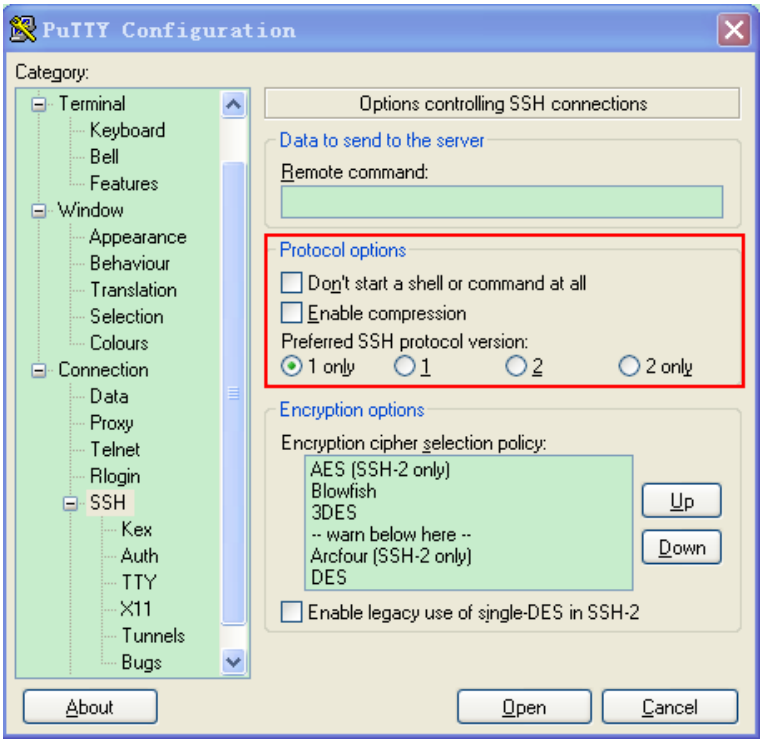
Scenario **Figure 1-13**	 SSH users can use the local line password for user authentication, as shown in Figure 1-13. To ensure security of data exchange, PC 1 and PC 2 function as SSH clients, and use SSH to log in to the network device where the SSH server is enabled. The requirements are as follows: ● 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 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 successful or failed authentication. SSHv1 uses the RSA key, whereas SSHv2 uses the RSA or DSA key. ● Configure the IP address of GigabitEthernet 0/1 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. PuTTY is used as an example to explain the method for configuring the SSH client. For details, see "Configuration Steps."

SSH Server	Before configuring the 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 is shown in Figure 1-14. The detailed procedure for configuring IP addresses and routes is 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-GigabitEthernet 0/1)#ip address 192.168.23.122
255.255.255.0
Hostname(config-if-GigabitEthernet 0/1)#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)

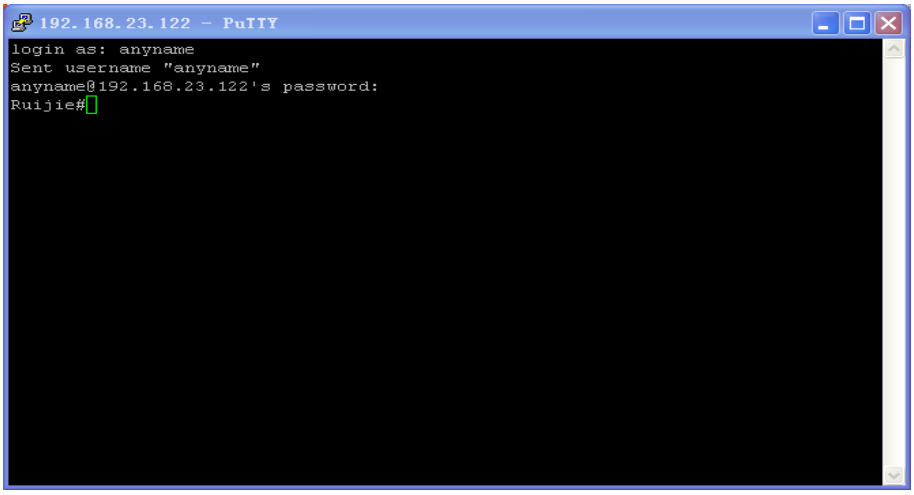
Figure 1-14



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, see Configuring SSH Device Management. Click **Open** to start the SSH server. Because the current authentication mode does not require a user name, you can enter any user name, but cannot leave the user name unspecified. In this example, the user name is **anyname**.

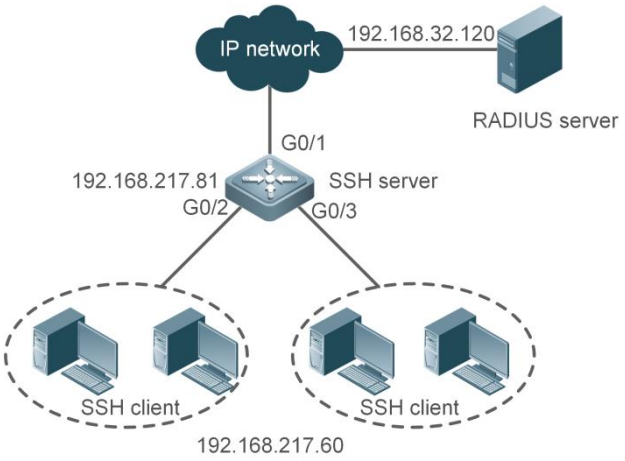
Verification

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

	● Verify that the SSH client configuration is correct.
SSH Server	Hostname#show running-config Building configuration... ! enable secret 5 1eyy2$xs28FDw4s2q0tx97 enable service ssh-server ! interface GigabitEthernet 0/1 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 1-15. 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 1-16. To ensure security of data exchange, the PC functions as the SSH client, and uses SSH 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. ● Perform AAA configuration 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 configuration.
- 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 with the SSH server. For details, see the previous example.

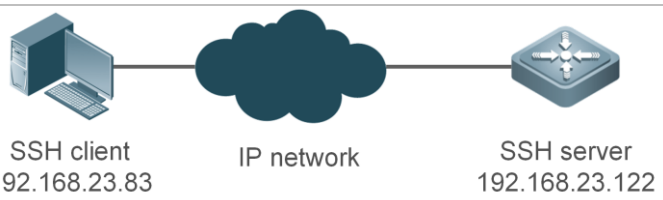
Enter the user name **user** and password **pass**. Verify that you can log in to the SSH server successfully.

```
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 1-17. SSH is configured on the client so that for setting up a secure connection with the SSH server.

Configuration Steps

- To implement public key authentication on the client, configure the device to 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.

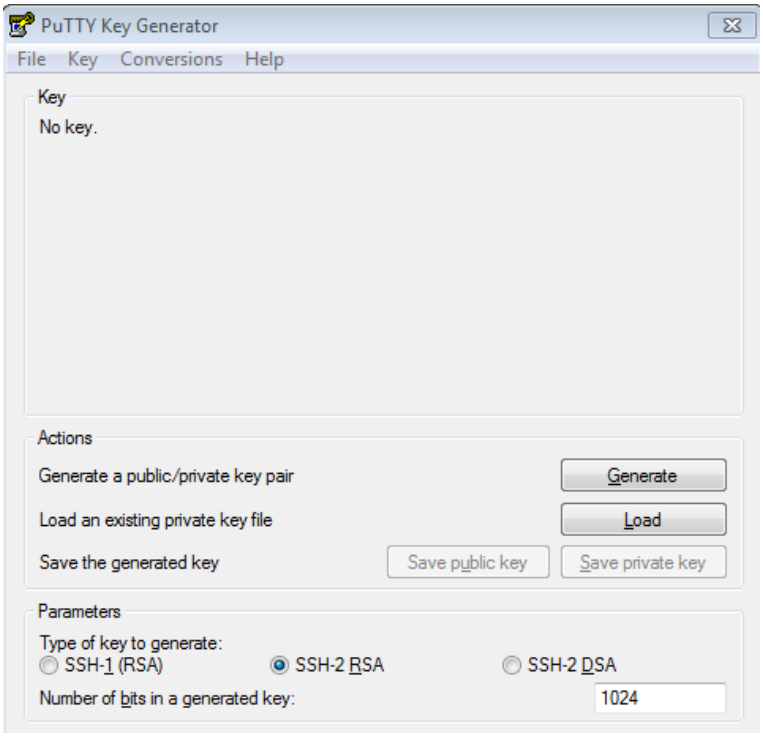
After the key pair is generated on the client, you must save and upload the public key file to the server and complete server-related settings before you can continue to configure the client and connect the client to the server.

- After the key is generated on the client, copy the public key file from the client to the flash memory 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

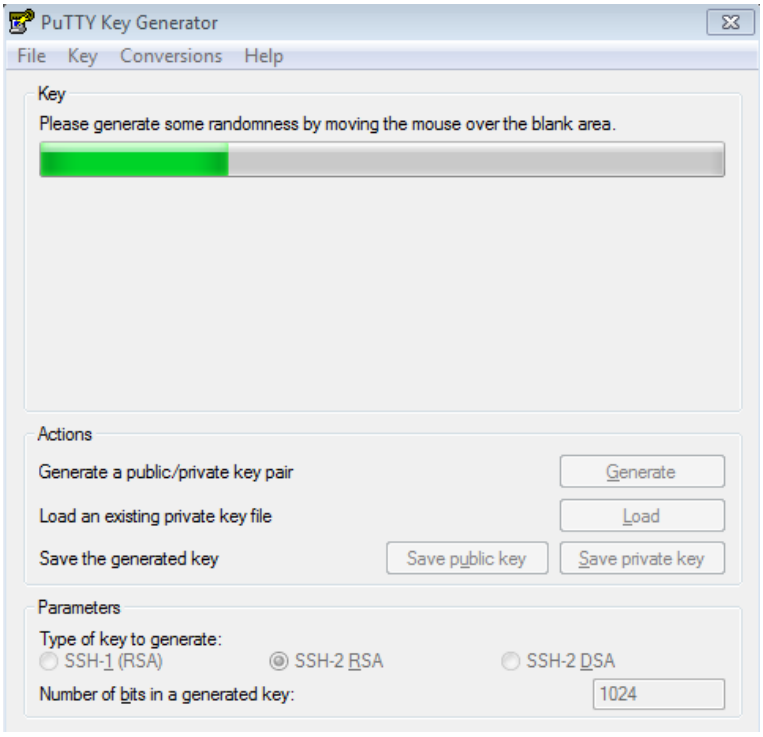
Run **puttygen.exe** on the client. Select **SSH-2 RSA** in the **Parameters** pane, and click **Generate** to generate a key, as shown in Figure 1-18.

Figure 1-18



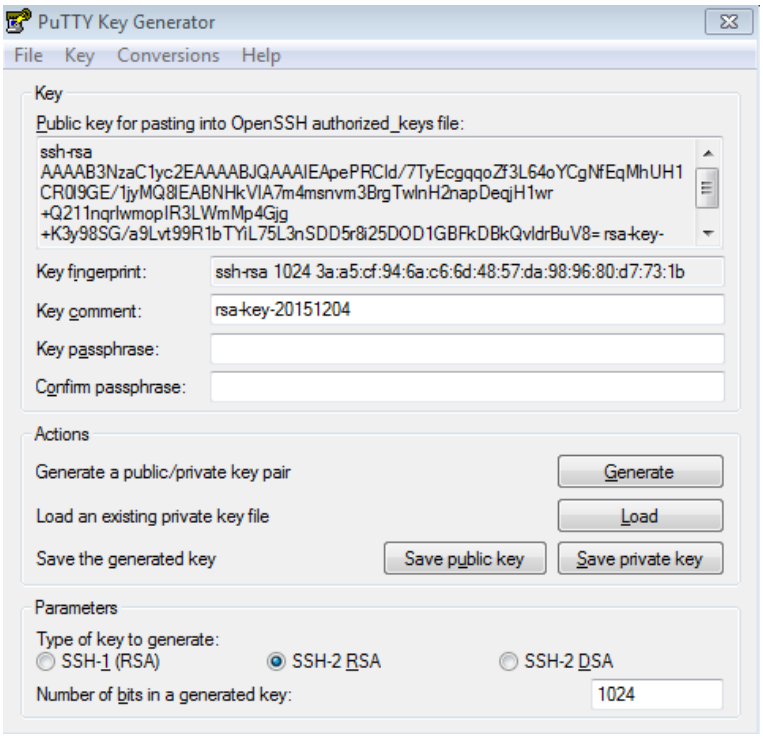
When a key is being generated, you need to constantly move the mouse over a blank area outside the green progress bar; otherwise, the progress bar does not move and key generation stops, as shown in Figure 1-19.

Figure 1-19



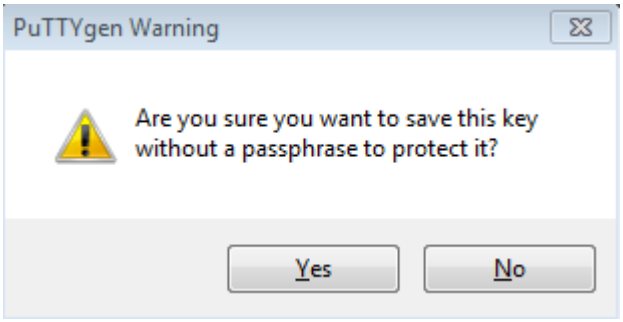
To ensure security of RSA public key authentication, the length of the generated RSA key pair must be equal to or larger than 768 bits. In this example, the length is set to 1024 bits.

Figure 1-20



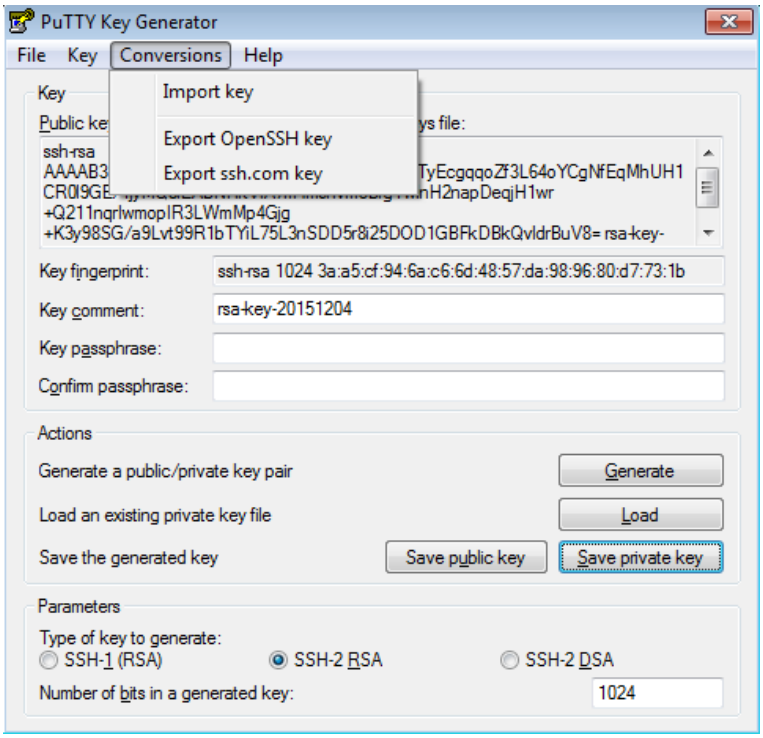
After the key pair is generated, click **Save public key**, enter the public key name **test_key.pub**, select the storage path, and click **Save**. Then click **Save private key**. The following dialog box is displayed. Select **Yes**, enter the public key name **test_private**, and click **Save**.

Figure 1-21



You must select the OpenSSH key file; otherwise, the key file cannot be used. **puttygen.exe** can be used to generate a key file in OpenSSH format, but the file cannot be directly used by the PuTTY client. You must use **puttygen.exe** to convert the private key to the PuTTY format. The public key file stored on the server uses the OpenSSH format and does not need to be converted, as shown in Figure 18-21.

Figure 1-22



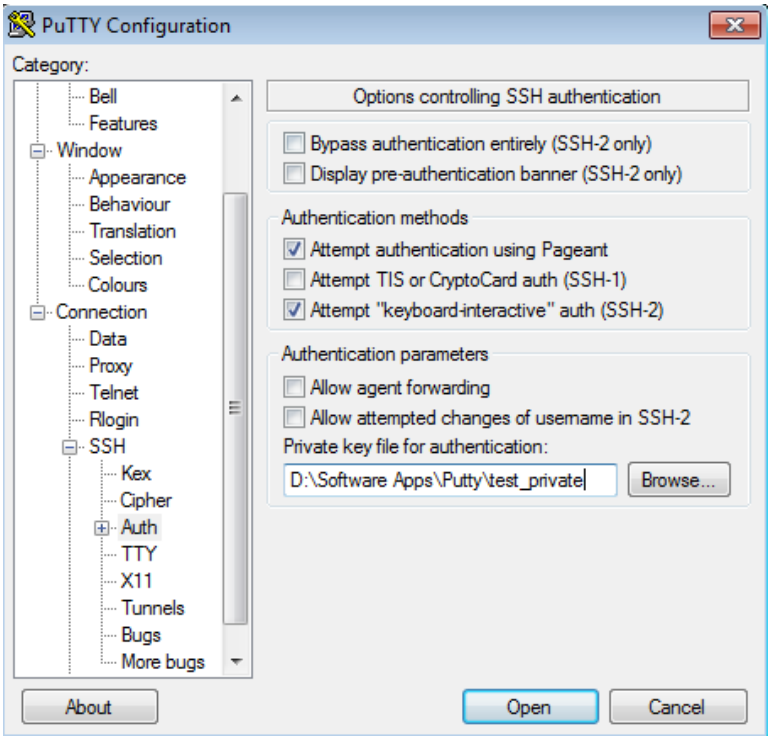
SSH Server

```
Hostname#configure terminal
Hostname(config)# ip ssh peer test public-key rsaflash:test_key.pub
```

Verification

- After completing basic configurations of the client and 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, ensuring security.

Notes

The SSH server must have been enabled.

Configuration Step

Enabling the SCP Server

- Mandatory.
- By default, the SCP server is disabled. Run the **ip scp server enable** command to enable the SCP server in global configuration mode.

Configuring the Transmission Path for Files of the SCP Server

- Optional.
- The default transmission path is **flash:/**. Run the **ip scp server topdir** { **flash:***/path* | **flash2:***/path* | **usb0:***/path* | **usb1:***/path* | **sd0:***/path* | **sata0:***/path* | **tmp:***/path* } command to configure the transmission path to upload files to or download files from the SCP server.

Verification

Run the **show ip ssh** command to check whether the SCP server 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.

Configuring the Transmission Path for Files of the SCP Server

Command	**ip scp server topdir** { **flash:***/path* | **flash2:***/path* | **usb0:***/path* | **usb1:***/path* | **sd0:***/path* | **sata0:***/path* | **tmp:***/path* }
Parameter	N/A

Description	
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the transmission path to upload files to or download files from the SCP server. Run the **no ip scp server topdir** command to restore the default transmission path.

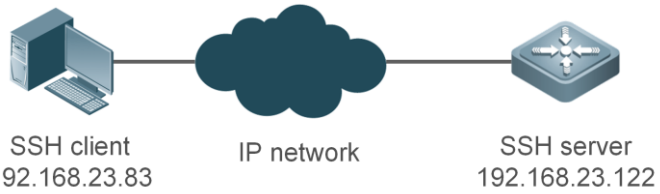
Configuration Example

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 is enabled.

	`Hostname(config)#show ipssh`
	`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 find 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 used, the system displays messages.
SSH Server	Hostname#configure terminal Hostname(config)# ip scp server enable
Verification	● File transmission example in 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

1.4.3 Configuring the SSH Client

Configuration Effect

On the network device that supports the SSH server, enable the SSH server, and specify the user authentication method and supported SSH versions. Then you can use the built-in SSH client of the device to set up a secure connection with the SSH server, implementing remote device management.

Notes

- The SSH server must have been configured on the remote device that supports the SSH server.
- The SSH client must communicate with the SSH server properly.

Configuration Step

↘ Specifying the Source Interface of the SSH Client

- Optional. This configuration must be performed on the SSH client.

↘ Establishing a Session with the SSH Server

- Optional. Use the **ssh** command on the client to set up a connection with a remote server.
- Before using this command, enable the SSH server and configure the SSH key and authentication mode on the server.

Restoring an Established SSH Session

- Optional. Run the related command to restore a disconnected session if necessary.

Disconnecting a Suspended SSH Session

- Optional. This configuration must be performed on the SSH client if you need to disconnect a specified SSH session.

Verification

Run the **show ssh-sessions** command to display information about established sessions of SSH clients.

Related Commands

Specifying the Source Interface of the SSH Client

Command	**ip ssh source-interface** *interface-name*
Parameter Description	*interface-name*: Specifies an interface, the IP address of which will be used as the source address of an SSH client session.
Command Mode	Global configuration mode
Usage Guide	This command is used to specify an interface, the IP address of which will be used as the global source address of an SSH client session. When the **ssh** command is used to connect to an SSH server, the global configuration will be used if the source interface or source address is not specified for this connection. Run the **no ip ssh source-interface** command to restore the default setting.

Establishing a Session with the SSH Server

Command	**ssh** [**-v** { **1** | **2** }] [**-c** { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** }] [**-l** *username*] [**-m** { **hmac-md5-96** | **hmac-md5-128** | **hmac-sha1-96** | **hmac-sha1-160** | **hmac-sha2-256** | **hmac-sha2-512** }] [**-p** *port-num*] { *ip-addr* | *hostname* } [**/source** { **ip** *A.B.C.D* | **ipv6** *X:X:X:X::X* | **interface** *interface-name* }]
Parameter Description	N/A
Command Mode	User EXEC mode
Usage Guide	The **ssh** command is used to set up a secure and encrypted connection from the local device (an SSH client) to another device (an SSH server) or any other server that supports SSHv1 or SSHv2. This connection provides a mechanism similar to the Telnet connection except that all data transmitted over this connection is encrypted. Based on authentication and encryption, the SSH client can set up a secure connection on an insecure network. ⚠ SSHv1 supports only DES (56-bit key) and 3DES (168-bit key) encryption algorithms. ⚠ SSHv2 supports the following Advanced Encryption Standards (AES) algorithms: ASE128-CBC, AES192-CBC, AES256-CBC, AES128-CTR, AES192-CTR, and AES256-CTR. ⚠ SSHv1 does not support the Hashed Message Authentication Code (HMAC). ⚠ If an SSH version is selected an a non-matched encryption or authentication algorithm is

	specified, the non-matched algorithm will be ignored when a connection is set up.

Recovering an Established SSH Client Session

Command	**ssh-session** *session-id*
Parameter Description	*session-id*: Indicates the ID of an established SSH client session.
Command Mode	User EXEC mode
Usage Guide	This command is used to restore the established SSH client session. When the **ssh** command is used to initiate an SSH client session, you can press **Ctrl+Shift+6+X** to temporarily exit the session. To restore this session, run the **ssh-session** command. In addition, if the session is already established, you can run the **show ssh-sessions** command to display information about the established session.

Disconnecting a Suspended SSH Session

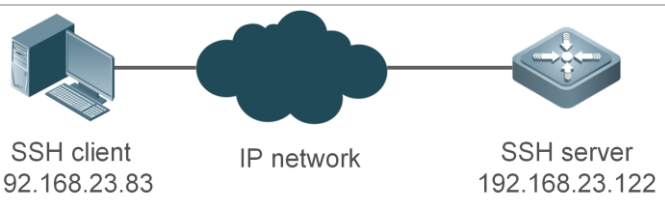
Command	**disconnect ssh-session** *session-id*
Parameter Description	*session-id*: Indicates the ID of a suspended SSH client session.
Command Mode	User EXEC mode
Usage Guide	You can specify an SSH client session ID to disconnect the specified SSH client session.

Configuration Example

Specifying the Source Interface of the SSH Client

Configuration Steps	Run the **ip ssh source-interface** *interface-name* command to specify an interface, the IP address of which will be used as the global source address of an SSH client session.
	`Hostname#configure terminal` `Hostname(config)#ipsshsource-interface gigabitethernet 0/1`
Verification	N/A

Establishing a Session with the SSH Server

Scenario **Figure 1-25**	 The SSH server function is enabled on the server. The **ssh** command is used on the client to set up a secure connection with the server.
Configuration Steps	● Enable the SSH server on the server. ● Configure the SSH key on the server. ● Configure the authentication mode of the SSH server, and use the local line authentication

	mode for Line 0 to Line 4. ● Configure the IP address of Gi 0/1 of the SSH server. The client will use this address as the source address to connect to the SSH server. ● Configure the SSH client and specify the source address of the SSH client. By default, the SSH server supports two SSH versions: SSHv1 and SSHv2. With this key, the SSH server decrypts the encrypted password received from the SSH client, compares the decrypted cleartext with the password stored on the server, and returns a message indicating successful or failed authentication. SSHv1 uses an RSA key, whereas SSHv2 uses an RSA or DSA key. The authentication mode used by the SSH server is local line authentication. The local user name is **admin**, and the password is 123456. The SSH client is connected to the SSH server based on this IP address. The routes from the SSH clients to the SSH server are reachable. Configure the IP address of Gi 0/1 of the SSH server. The client will use this address as the source address to connect to the SSH server.

SSH Server	`Hostname#configure terminal`
	`Hostname(config)#enable service ssh-server`
	`Hostname(config)#crypto key generate rsa`
	`% You already have RSA keys.`
	`% Do you really want to replace them? [yes/no]:`
	`Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a few minutes.`
	`How many bits in the modulus [512]:`
	`% Generating 512 bit RSA1 keys ...[ok]`
	`% Generating 512 bit RSA keys ...[ok]`
	`Hostname(config)#line vty 0 4`
	`Hostname(config-line)#login local`
	`Hostname(config-line)#exit`
	`Hostname(config)#username admin password 123456`
	`Hostname(config)#username admin privilege 15`
	`Hostname(config-line)#exit`
	`Hostname(config)#interface gigabitethernet 0/1`
	`Hostname(config-if-GigabitEthernet0/1)#ip address 192.168.23.122 255.255.255.0`
	`Hostname(config-if-GigabitEthernet0/1)#exit`

SSH Client	`Hostname(config)#interface gigabitethernet 0/1`
	`Hostname(config-if-GigabitEthernet0/1)#ip address 192.168.23.83 255.255.255.0`
	`Hostname(config-if-GigabitEthernet0/1)#exit`
	`Hostname(config)# ip ssh source-interface gigabitEthernet 0/1`

Verification	• Run the **show running-config| include username** and **show ip ssh** commands to check whether the SSH server configuration is correct. • On the SSH client, set up a connection with a remote SSH server. After the connection is set up, enter the correct password **123456**. The SSH server operation interface is displayed. Check the login user on the console of the SSH client.
	`Hostname(config)#sh running-config	include username` `username admin password admin` `username admin privilege 15` `Hostname(config)#sh running-config	begin line` `line con 0` `line vty 0 4` `login local` `!` `!` `end`
	• Check whether the SSH client configuration is correct.

	`Hostname#ssh -l admin 192.168.23.122`
	`%Trying 192.168.23.122, 22,...open`
	`admin@192.168.23.122's password:`
	`Hostname#`
	`Hostname#sh users`
	`Line User Host(s) Idle Location`
	`0 con 0 idle 00:00:00`
	`* 1 vty 0 admin idle 00:00:36 192.168.217.20`

1.5 Monitoring

Displaying

Description	Command
show ipssh	Displays the effective SSH server configuration.
show ssh	Displays the established SSH connection.
show crypto key mypubkey	Displays public information about the SSH public key.
show ssh-sessions	Displays the established SSH client session.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug ssh	Debugs SSH sessions.
debug ssh client	Debugs SSH client sessions.

Configuring Reliability

1. Configuring VRRP
2. Configuring Supervisor Module Redundancy
3. Configuring WLAN Hot Standby
4. Configuring Virtual AC
5. Configuring RIPT
6. Configuring Track

1 Configuring VRRP

1.1 Overview

The Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant routing protocol.

VRRP adopts the active/standby design to ensure that when the master fails, the backup routing device can seamlessly take over functions without affecting internal and external data communication, and without the need to modify internal network parameters. Multiple routing devices in a VRRP group are mapped to a single virtual router. VRRP ensures that only one routing device at a time represents the virtual router for packet transmission. Hosts send packets to this virtual router, and the router forwarding the packets is seleced as the master. If the master becomes unable to function due to any reason, one backup device is selected to replace the original master. VRRP makes it appear to hosts on a LAN that only one router device is being used, and even in the event of failure of the current first-hop router being used, connectivity can be maintained.

- VRRP is applicable to LANs where redundancy of routing egresses is required.

Protocols and Standards

- RFC 2338: Virtual Router Redundancy Protocol
- RFC 3768: Virtual Router Redundancy Protocol (VRRP)
- RFC 5798: Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6

1.2 Applications

Application	Description
Routing Redundancy	Configure routing devices on a LAN as one VRRP group to achieve routing redundancy.
Load Balancing	Configure routing devices on a LAN as multiple VRRP groups to achieve traffic load balancing.

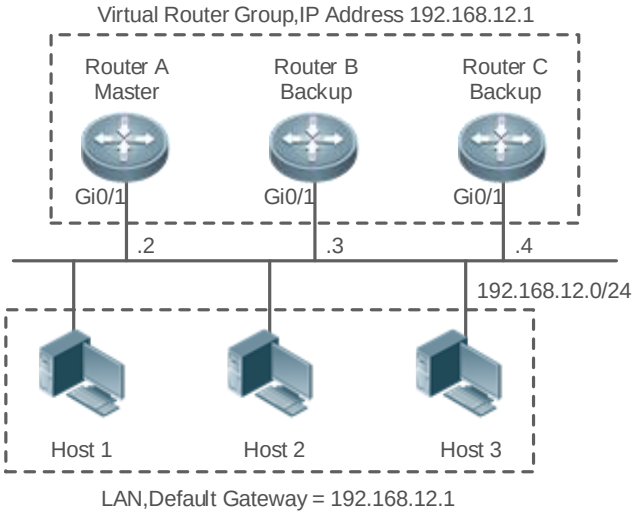
1.2.1 Routing Redundancy

Scenario

Configure a VRRP group on routers of a LAN, where hosts use the virtual IP address of the group as the default gateway address.

- Packets from Host 1, Host 2 and Host 3 to other networks are forwarded by the elected master (Router A in Figure 1-1).
- If Router A fails, the master will be re-elected between Router B and Router C to forward packets, achieving simple routing redundancy.

Figure 1-1



Deployment

- Router A, Router B and Router C are connected to the LAN through Ethernet interfaces.
- On Router A, Router B, and Router C, VRRP is configured on Ethernet interfaces connected to the LAN.
- These Ethernet interfaces are in the same VRRP group whose virtual IP address is 192.168.12.1.
- The gateway address for Host 1, Host 2, and Host 3 is the IP address of the VRRP group, namely, 192.168.12.1.

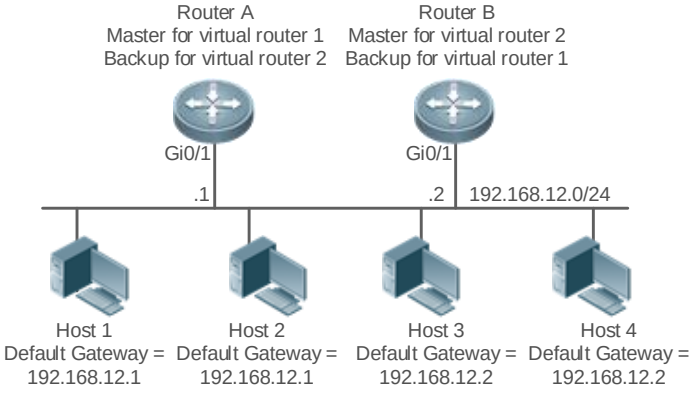
1.2.2 Load Balancing

Scenario

Configure multiple VRRP groups on routers of a LAN. Hosts on the LAN use virtual IP addresses of the groups as their gateways, and each router backs up for other routers in different groups.

- Packets from Host 1 and Host 2 to other networks with the default gateway address as the virtual IP address of virtual router 1 are forwarded by the master of virtual router 1 (Router A in Figure 1-2).
- Packets from Host 3 and Host 4 to other networks with the default gateway address as the virtual IP address of virtual router 2 are forwarded by the master of virtual router 2 (Router B in Figure 1-2).
- Routing redundancy is achieved on Router A and Router B, and LAN traffic is shared to achieve load balancing.

Figure 1-2



Deployment

- Router A and Router B are connected to the LAN through Ethernet interfaces.
- On Router A and Router B, two virtual routers are configured on the Ethernet interfaces connected to the LAN.
- Router A uses the IP address 192.168.12.1 of Ethernet interface Gi0/1 as the IP address of virtual router 1. For virtual router 1, Router A becomes the master and Router B becomes the backup.
- Router B uses the IP address 192.168.12.2 of Ethernet interface Gi0/1 as the IP address of virtual router 2. For virtual router 2, Router B becomes the master and Router A becomes the backup.
- On the LAN, Host 1 and Host 2 use the IP address 192.168.12.1 of virtual router 1 as the default gateway address, while Host 3 and Host 4 use the IP address 192.168.12.2 of virtual router 2 as the default gateway address.

1.3 Features

Basic Concepts

Virtual Router

A virtual router, also called a VRRP group, is regarded as a default gateway for hosts on a LAN, which involves the Virtual Router Identifier (VRID) and a set of virtual IP addresses.

Virtual IP Address

The virtual IP address is the IP address of a virtual router. A virtual router can be configured with one or more IP addresses.

IP Address Owner

If a VRRP group has the virtual IP address as that of an Ethernet interface on one router, the router is regarded as the virtual IP address owner. In such case, the router priority is 255. If the corresponding Ethernet interface is available, the VRRP group will be in master state automatically. The IP address owner receives and processes the packets with the destination IP address as that of the virtual router.

Virtual MAC Address

The virtual MAC address of a VRRP group is an IEEE 802 MAC address, in the format of 00-00-5E-00-01-{VRID} with the first five octets assigned and the last two as a group VRID. A VRRP group responds to an Address Resolution Protocol (ARP) request packet with its virtual MAC address but not the actual MAC address.

Master Router

In a VRRP group, only the master responds to ARP request packets and forwards IP packets. If the router is the IP address owner, it becomes the master router.

Backup Router

In a VRRP group, backup routers only monitor the state of the master but do not respond to ARP request packets or forward IP packets. When the master fails, backup routers will compete for the master role.

Preemption Mode

If a VRRP group runs in preemption mode, a backup router with a higher priority will replace the master with a lower priority.

Overview

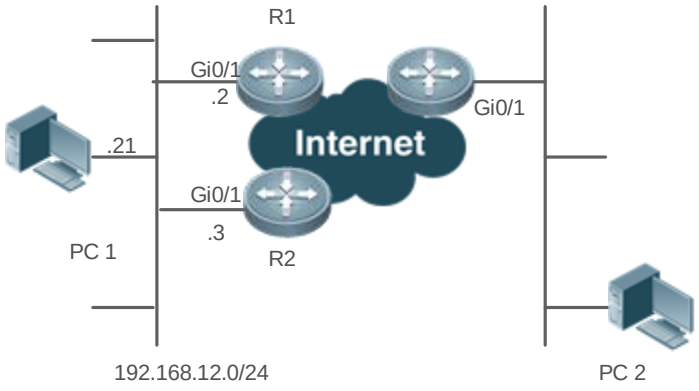
Feature	Description
VRRP	VRRP achieves redundancy for default gateways of terminals on a multi-access media (for example, Ethernet). It enables a backup router to forward packets when the master router is Down, providing transparent switching and enhancing the network service quality.

1.3.1 VRRP

When the master router is faulty, VRRP achieves migration of functions from the master router to a backup without affecting internal and external data communication or changing the LAN configuration.

Working Principle

Figure 1-3 Working Principle of VRRP



Working Mode of VRRP

RFC 2338, RFC 3768, and RFC 5798 define the format and operating mechanism of VRRP packets. Multicast VRRP packets are sent periodically with specified destination addresses by the master router to advertise normal operation or for master election. VRRP allows a router on a LAN to automatically replace the master who forwards IP packets when the master fails. This helps achieve hot standby and fault tolerance of IP-based routing as well as ensure communication continuity and reliability for hosts on the LAN. A VRRP group achieves redundancy through multiple routers. However, only one router acts as the master to forward packets while the others are backup routers. Switching in a VRRP group is completely transparent to hosts on a LAN.

Master Election Process

RFC standards define the master election process as follows:

- VRRP provides a simple mechanism for master election. First, routers in a VRRP group compare the VRRP priorities configured on connected interfaces. The router with the highest priority is elected as the master. If the priorities are the same, they compare the primary IP addresses. The router with the largest IP address is elected as the master.
- After the master router is elected, the other routers become backup routers (and enter the backup state) and monitor the state of the master router through VRRP packets the master router sends. If the master router is

operational, it regularly sends VRRP multicast packets known as Advertisement packets to notify the backup routers of its status. If the backup routers do not receive such packets within a given period of time, all of them will enter the master state. In such case, master election is repeated. In this way, a router with the highest priority will be elected as a new master, achieving VRRP backup.

Once the master router of a VRRP group is elected, it is responsible for forwarding packets for hosts on a LAN.

Communication Process

Figure 1-3 Working Principle of VRRP shows the VRRP communication process. R1 and R2 are connected to the LAN segment 192.168.12.0/24 through the VRRP-enabled Ethernet interfaces Gi0/1. Hosts on the LAN use the virtual IP address of the VRRP group as the default gateway address. Only the virtual router is recognized by the hosts. The master router in the group, however, is unknown. For example, when PC 1 plan to communicate with PC 2, PC 1 sends packets to the default gateway with the virtual IP address. The master router in the group receives the packets and forwards them to PC 2. In this process, PC 1 only detects the virtual router but not R1 or R2. The master router in the group is elected between R1 and R2. When the master fails, it will be replaced automatically by the other router.

Related Configuration

Enabling VRRP

By default, VRRP is disabled on an interface.

In interface configuration mode, run the **vrrp** *group* **ip** *ipaddress* [**secondary**] or **vrrp** *group* **ipv6** *ipv6-address* command to set the VRID and virtual IP address to enable VRRP.

VRRP must be enabled on an interface.

Configuring the IPv4 VRRP Authentication String

By default, VRRP is in non-authentication mode.

Run the **vrrp group authentication** *string* command to set an authentication string in MD5 authentication mode or a cleartext password for an IPv4 VRRP group. In cleartext authentication mode, a password contains up to 8 bytes.

Members of a VRRP group can communicate with each other only when they use the same authentication mode. In cleartext authentication mode, all routers in a VRRP group should have the same authentication password. The cleartext authentication password cannot guarantee security but only prevents or prompts VRRP configuration errors.

Configuring the VRRP Advertisement Interval

By default, the advertisement interval of the master router is 1 second.

Run the **vrrp** [**ipv6**] *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* } command to change the interval.

When the VRRP learning timer is not configured, the same advertisement interval should be set for a VRRP group. Otherwise, routers in backup state will discard received VRRP packets.

Configuring the VRRP Preemption Mode

By default, a VRRP group operates in preemption mode.

To enable the preemption mode for a VRRP group, run the **vrrp** [**ipv6**] *group* **preempt** [**delay** *seconds*] command. The value of **delay** *seconds* is 0 by default.

If a VRRP group works in preemption mode, a router will become the mater of the group when it finds that its priority is higher than that of the master. If a VRRP group operates in non-preemption mode, a router will not become the master even when it finds that its priority is higher than that of the master. When the VRRP group uses the IP address of an Ethernet interface, the device that the Ethernet interface belongs to has the highest priority and automatically becomes the master in the group. The optional parameter **delay** *seconds* defines the delay before a backup VRRP router declares its master role.

Enabling the IPv6 VRRP Accept Mode

By default, the Accept mode is disabled for an IPv6 VRRP group.

To enable the Accept mode, run the **vrrp ipv6** *group* **accept_mode** command.

When the Accept mode is enabled, an IPv6 VRRP virtual router in master state receives and processes packets destined for the virtual router IP address; when the Accept mode is disabled, the virtual router discards such packets except Neighbor Advertisement (NA) packets and Neighbor Solicitation (NS) packets. Besides, an IPv6 VRRP master in owner state receives and processes packets destined for the virtual router IP address by default regardless of whether the Accept mode is configured.

Configuring the VRRP Router Priority

By default, router priorities in a VRRP group are all 100.

To adjust the priority, run the **vrrp** [**ipv6**] *group* **priority** *level* command.

If a router in preemption mode has the group's virtual IP address and the highest priority, it becomes the master, while the other routers with lower priorities in the group become backup (or monitoring) routers.

Configuring the VRRP Tracked Interface

By default, no interface is tracked by a VRRP group.

To configure such an interface, run the **vrrp** *group* **track** { *interface-type interface-number* | **bfd** *interface-type interface-number ipv4-addess* } [*priority*] or **vrrp ipv6** ***group*** **track** *interface-type interface-number* [*priority*] command.

After an interface to be monitored by a VRRP group is configured, the router priority will be adjusted dynamically based on the interface status. Once the interface becomes unavailable, the priority of the router in the group will be reduced by a set value, and another functional router with a higher priority in this group will become the master.

To trace the link layer protocol status of an interface, configure the **link** parameter. Otherwise, the network layer protocol status of the interface is traced.

Configuring the VRRP Tracked IP Address

By default, no IP address is tracked by a VRRP group.

To configure such an address, run the **vrrp** *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*] or **vrrp ipv6** *group* **track** { *ipv6-global-address* | { *ipv6-linklocal-address interface-type interface-number* } } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*] command.

After an IP address to be monitored by a VRRP group is configured, the router priority will be adjusted dynamically based on address accessibility. Once the address is inaccessible (the **ping** command fails), the priority of the router in the group will be reduced by a set value, and another router with a higher priority in this group will become the master.

Configuring the VRRP Learning Timer

By default, the learning timer is disabled for a VRRP group.

To enable it, run the **vrrp** [**ipv6**] *group* **timers learn** command.

After the learning timer is configured, a VRRP backup router learns the advertisement interval of NA packets from the master. The backup router calculates the interval for determining a failure of the master based on the learning timer but not the local advertisement interval. This command ensures that advertisement intervals between backup routers and the master are synchronized.

Configuring the Description for a VRRP Group

By default, no description is configured for a VRRP group.

To configure such a string, run the **vrrp** [**ipv6**] *group* **description** *text* command.

The description helps distinguish a VRRP group. A description has up to 80 bytes. If the description has more than 80 bytes, the system displays the message about incorrect configuration.

Configuring the Delay for a VRRP Group

By default, no delay is configured for a VRRP group.

To configure the delay for a VRRP Group, run the **vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* } command. The delay range of two types is from 0 to 60, in seconds.

The command configures the delay of starting a VRRP group on an interface. There are two types of VRRP delay: delay after system startup and delay after an interface becomes active. You may configure them respectively or simultaneously. After the delay is configured for a VRRP group on an interface, the VRRP group does not start when the system starts up or the interface becomes active. Instead, the VRRP group starts after the delay, ensuring that the non-preemption configuration is effective. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP group will be started immediately. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface.

Configuring the IPv4 VRRP Version

By default, IPv4 adopts the VRRPv2 standard.

To specify the version for IPv4 VRRP, run the **vrrp** *group* **version** { **2** | **3** } command.

When the parameter value is set to 2, VRRPv2 is adopted; when the parameter value is set to 3, VRRPv3 is adopted.

Specifying a Sub-VLAN of a Super-VLAN to Receive the IPv4 VRRP Packets

By default, IPv4 VRRP packets are sent to the first Up interface of a sub-VLAN in a super-VLAN.

To specify the first Up interface of a sub-VLAN in a super-VLAN to receive IPv4 VRRP packets, run the **vrrp detection-vlan first-subvlan** command; to specify a sub-VLAN, run the **vrrp detection-vlan** *subvlan-id* command. If VRRP and VRRP Plus are enabled simultaneously on an interface of a super-VLAN, VRRP packets are sent to all Up interfaces of the sub-VLANs in the super-VLAN.

You can configure the IPv4 VRRP protocol packets to be sent only to the first Up interface of a sub-VLAN or a specified sub-VLAN in a super-VLAN. This reduces the number of VRRP protocol packets, and prevents device performance and network bandwidth from being affected. In this case, routers constituting an IPv4 VRRP group should be interconnected within the first Up interface of a sub-VLAN or a specified sub-VLAN of the super-VLAN.

1.4 Configuration

Configuration	Description and Command	
Configuring IPv4 VRRP	(Mandatory) It is used to enable IPv4 VRRP.	
	vrrp *group* **ip** *ipaddress* [**secondary**]	Enables IPv4 VRRP.
	(Optional) It is used to configure IPv4 VRRP parameters.	
	vrrp *group* **authentication** *string*	Configures the IPv4 VRRP authentication string.
	vrrp *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* } [**multiplier** *interval*]	Configures the IPv4 VRRP advertisement interval.
	vrrp *group* **preempt** [**delay** *seconds*]	Configures the IPv4 VRRP preemption mode.
	vrrp *group* **priority** *level*	Configures the IPv4 VRRP router priority.
	vrrp *group* **track** *interface-type interface-number* [*priority*]	Configures the IPv4 VRRP tracked interface.
	vrrp *group* **track** *ip-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	Configures the IPv4 VRRP tracked IP address.
	vrrp *group* **timers learn**	Configures the IPv4 VRRP learning timer.
	vrrp *group* **description** *text*	Configures the IPv4 VRRP group description.
	vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }	Configures the IPv4 VRRP delay.
	vrrp *group* **version** { **2** | **3** }	Configures the IPv4 VRRP version.
	vrrp detection-vlan { **first-subvlan** | *subvlan-id* }	Configures the IPv4 VRRP protocol packets to be sent only to the first Up interface of a sub-VLAN or a specified sub-VLAN in the super-VLAN.
Configuring IPv6 VRRP	(Mandatory) It is used to enable IPv6 VRRP.	
	vrrp *group* **ipv6** *ipv6-address*	Enables IPv6 VRRP in interface configuration mode.
	(Optional) It is used to configure IPv6 VRRP parameters.	
	vrrp ipv6 *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }	Configures the IPv6 advertisement interval.
	vrrp ipv6 *group* **preempt** [**delay** *seconds*]	Configures the IPv6 VRRP preemption mode.
	vrrp ipv6 *group* **accept_mode**	Enables the Accept mode for an IPv6 VRRP group.

Configuration	Description and Command	
	vrrp ipv6 *group* **priority** *level*	Configures the IPv6 VRRP router priority.
	vrrp ipv6 *group* **track** *interface-type interface-number* [**link**] [*interface–priority*]	Configures the IPv6 VRRP tracked interface.
	vrrp ipv6 *group* **track** { *ipv6-global-address* | { *ipv6-linklocal-address interface-type interface-number* } } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]	Configures the IPv6 VRRP tracked IP address.
	vrrp ipv6 *group* **timers learn**	Configures the IPv6 VRRP learning timer.
	vrrp ipv6 *group* **description** *text*	Configures the IPv6 VRRP group description.
	vrrp delay { **minimum** *min-seconds* | **reload** *reload-seconds* }	Configures the IPv6 VRRP delay.
Configuring VRRP and MSTP	The configuration is the same as IPv4 VRRP configuration.	

1.4.1 Configuring IPv4 VRRP

Configuration Effect

- Configure a VRRP group on an interface of a specific LAN segment by setting the VRID and virtual IP address.
- Configure multiple VRRP groups on an interface to achieve load balancing and offer more stable and reliable network services.
- Configure the VRRP tracked interfaces to monitor failures, change interface priorities, and realize failover dynamically.

Notes

- To achieve VRRP, routers in a VRRP group should be configured with the same virtual IPv4 address.
- To achieve backup between multiple IPv4 VRRP groups, configure multiple IPv4 VRRP groups with the same VRRP configuration on different interfaces and configure different priorities for the groups so that they back up each other.
- Enable VRRP on Layer 3 interfaces.

Configuration Steps

Enabling IPv4 VRRP

By default, IPv4 VRRP is disabled on an interface. You can enable it as needed.

Configuring the IPv4 VRRP Authentication String

By default, VRRP is in non-authentication mode. You can enable cleartext authentication as needed.

Configuring the IPv4 VRRP Advertisement Interval

By default, the master router sends advertisement packets every 1s. You can modify the interval as needed.

Configuring the IPv4 VRRP Preemption Mode

By default, a VRRP group operates in preemption mode without a delay.

Configuring the IPv4 VRRP Router Priority

The default router priority for a VRRP group is 100. You can modify the priority as needed.

Configuring the IPv4 VRRP Tracked Interface

By default, an IPv4 VRRP group does not monitor any interface and the value of priority change is 10. To detect faults through interface monitoring, perform this configuration.

Configuring the IPv4 VRRP Learning Timer

By default, the learning timer is disabled for a VRRP group. Enable this function if backup routers need to learn the master's advertisement interval.

Configuring the Description for an IPv4 VRRP Group

By default, no description is configured for a VRRP group. To help distinguish VRRP groups, configure descriptions.

Configuring the IPv4 VRRP Delay

By default, the IPv4 VRRP delay is not configured. To guarantee an effective non-preemption mode, configure the delay.

Configuring the IPv4 VRRP Version

By default, IPv4 adopts the VRRPv2 standard. To change it, use the corresponding command.

Setting the Sending Mode of IPv4 VRRP Packets in a Super-VLAN

By default, IPv4 VRRP packets are only sent to the first Up interface of a sub-VLAN in a super-VLAN. However, it is possible to configure them to be sent to a specific sub-VLAN in the super-VLAN.

Verification

Run the **show vrrp** command to verify the configuration.

Related Commands

Enabling IPv4 VRRP

Command	**vrrp** *group* **ip** *ipaddress* [**secondary**]
Parameter Description	*group*: Indicates the VRID of a VRRP group. The value range depends on product models. *ipaddress*: Indicates the IP address of a VRRP group. **secondary**: Indicates the secondary IP address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	If no virtual IP address is specified, routers cannot join a VRRP group. If no secondary IP address is applied, the configured IP address will be the primary IP address of a VRRP group.

Configuring the IPv4 VRRP Authentication String

Command	**vrrp** *group* **authentication** *string*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *string*: Indicates the authentication string of a VRRP group (a cleartext password consists of 8 bytes at most).
Command Mode	Interface configuration mode
Usage Guide	In a VRRP group, the same authentication password should be configured for routers. The cleartext authentication password cannot guarantee security but only prevents or prompts VRRP configuration errors. This command is only applicable to VRRPv2 but not VRRPv3. Authentication is abolished for VRRPv3 (IPv4 VRRP and IPv6 VRRP) packets. If VRRPv2 is chosen for an IPv4 VRRP group, the command is effective; if VRRPv3 is chosen, the command is ineffective.

Configuring the IPv4 VRRP Advertisement Interval

Command	**vrrp** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group, in seconds. ***csec*** *centisecond-interval:* Indicates the interval for the master router in a VRRP group to send VRRP packets. It is an integer from 50 to 99, in centiseconds. No default value is provided. The command is only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is 1s.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority, and other information. As defined by RFC standards, if an IPv4 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40s. Therefore, if the interval is larger than 40s, the maximum interval of 40s will be applied, though the configuration is effective.

Configuring the IPv4 VRRP Preemption Mode

Command	**vrrp** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the master router to declare its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in preemption mode, a router with a higher priority will replace the master with a lower priority. If a VRRP group runs in non-preemption mode, a router with the priority higher than that of the master remains backup. When the VRRP group uses the IP address of an Ethernet interface, the device to which the Ethernet interface belongs has the highest priority and automatically becomes the master in the group.

Configuring the IPv4 VRRP Router Priority

Command	**vrrp** *group* **priority** *level*

Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of an interface in a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the VRRP router priority.

Configuring the IPv4 VRRP Tracked Interface

Command	**vrrp** *group* **track** *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the step of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer 3 logical interface, for example, a routed interface, an SVI, a loopback interface, or a tunnel interface. The priority of the router that has the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

Configuring the IPv4 VRRP Tracked IP Address

Command	**vrrp** *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv4-addres*: Indicates the IPv4 address to be tracked. ***interval*** *interval-value*: Indicates the probe interval, in seconds. The default value is 3s. ***timeout*** *timeout-value*: Indicates the probe timeout interval of waiting for response, in seconds. If no response is received within the timeout interval, the device considers that the destination is inaccessible. The default value is 1s. **retry** *retry-value*: Indicates the probe retry count. If no response is received after the probe retry count, the device considers that the destination is inaccessible. The default value is 3. *priority*: Indicates the step of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv4 address for an IPv4 VRRP group. If a VRRP group owns the IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

Configuring the IPv4 VRRP Learning Timer

Command	**vrrp** *group* **timers learn**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode

Usage Guide	After the learning timer is configured, a VRRP backup router learns the advertisement interval of NA packets from the master. The backup router calculates the interval for determining a failure of the master based on the learning timer but not the local advertisement interval. This command ensures that advertisement intervals between backup routers and the master are synchronized.

Configuring the Description for an IPv4 VRRP Group

Command	**vrrp** *group* **description** *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	The description helps distinguish a VRRP group. A description has up to 80 bytes. If the description has more than 80 bytes, the system displays the message about incorrect configuration.

Configuring the IPv4 VRRP Delay

Command	**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group does not start when the system starts up or the interface becomes active. Instead, the VRRP group starts after the delay, ensuring that the non-preemption configuration is effective. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP group will be started immediately. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface. The value range of the delay of two types is from 0 to 60, in seconds.

Configuring the IPv4 VRRP Version

Command	**vrrp** *group* **version** { **2** | **3** }
Parameter Description	**2**: Indicates VRRPv2. **3**: Indicates VRRPv3.
Command Mode	Interface configuration mode
Usage Guide	Considering compatibility between VRRPv2 and VRRPv3, specify a standard for IPv4 VRRP based on the actual network condition. VRRPv2 is defined in RFC 3768 and VRRPv3 in RFC 5798. This command is only applicable to IPv4 VRRP.

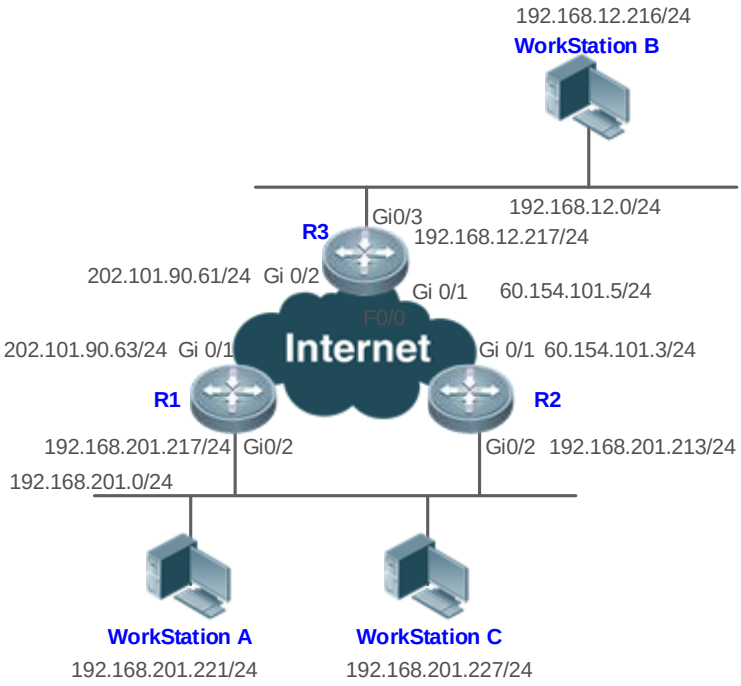
Specifying a Sub-VLAN of a Super-VLAN to Receive IPv4 VRRP Packets

Command	**vrrp detection-vlan** { **first-subvlan** | *subvlan-id* }
Parameter Description	**first-subvlan**: Sends IPv4 VRRP packets only to the first Up interface of a sub-VLAN in a super-VLAN. *subvlan-id*: Sends packets to a specified sub-VLAN.
Command Mode	Interface configuration mode

Usage Guide	This command is used to specify a sub-VLAN of a super-VLAN to receive the IPv4 VRRP packets. IPv4 VRRP packets are sent in a super-VLAN using the following three methods. Packets are sent to the first Up interface of a sub-VLAN in a super-VLAN, or to a specified sub-VLAN interface in a super-VLAN, or to all the sub-VLAN interfaces in a super-VLAN. If VRRP and VRRP Plus are enabled simultaneously on a super-VLAN interface, VRRP packets are sent to all Up interfaces of sub-VLANs in the super-VLAN. This command is configured on a VLAN interface and effective only to super-VLAN interfaces.

Configuration Example

↘ Configuring an IPv4 VRRP Group and Tracked Interface

Scenario **Figure 1-4**	
Configuration Steps	● Configure a VRRP group between R1 and R2. The cluster of WorkStation A and WorkStation C (192.168.201.0/24) uses the virtual IP address 192.168.201.1 of the VRRP group as the gateway address to communicate with WorkStation B (192.168.12.0 /24). ● Configure GigabitEthernet 0/1 on R1 as the tracked interface. ● Configure routing functions on R3.

R3	`R3#configure terminal`
	`R3(config)#interface GigabitEthernet 0/3`
	`R3(config-if-GigabitEthernet 0/3)#no switchport`
	`R3(config-if-GigabitEthernet 0/3)#ip address 192.168.12.217 255.255.255.0`
	`R3(config-if-GigabitEthernet 0/3)#exit`
	`R3(config)#interface GigabitEthernet 0/1`
	`R3(config-if-GigabitEthernet 0/1)#no switchport`
	`R3(config-if-GigabitEthernet 0/1)#ip address 60.154.101.5 255.255.255.0`
	`R3(config-if-GigabitEthernet 0/1)#exit`
	`R3(config)#interface GigabitEthernet 0/2`
	`R3(config-if-GigabitEthernet 0/2)#no switchport`

	R3(config-if-GigabitEthernet 0/2)#ip address 202.101.90.61 255.255.255.0 R3(config-if-GigabitEthernet 0/2)#exit R3(config)#router ospf R3(config-router)#network 202.101.90.0 0.0.0.255 area 10 R3(config-router)#network 192.168.12.0 0.0.0.255 area 10 R3(config-router)#network 60.154.101.0 0.0.0.255 area 10
R1	R1#configure terminal R1(config)#interface GigabitEthernet 0/2 R1(config-if-GigabitEthernet 0/2)#ip address 192.168.201.217 255.255.255.0 R1(config-if-GigabitEthernet 0/2)#vrrp 1 priority 120 R1(config-if-GigabitEthernet 0/2)#vrrp 1 timers advertise 3 R1(config-if-GigabitEthernet 0/2)#vrrp 1 ip 192.168.201.1 R1(config-if-GigabitEthernet 0/2)#vrrp 1 track GigabitEthernet 0/1 30 R1(config-if-GigabitEthernet 0/2)#exit R1(config)#interface GigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)#ip address 202.101.90.63 255.255.255.0 R1(config-if-GigabitEthernet 0/1)#exit R1(config)#router ospf R1(config-router)#network 202.101.90.0 0.0.0.255 area 10 R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
R2	R2#configure terminal R2(config)#interface GigabitEthernet 0/2 R2(config-if-GigabitEthernet 0/2)#ip address 192.168.201.213 255.255.255.0 R2(config-if-GigabitEthernet 0/2)#vrrp 1 ip 192.168.201.1 R2(config-if-GigabitEthernet 0/2)#vrrp 1 timers advertise 3 R2(config-if-GigabitEthernet 0/2)#exit R2(config)#interface GigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)#no switchport R2(config-if-GigabitEthernet 0/1)#ip address 60.154.101.3 255.255.255.0 R2(config-if-GigabitEthernet 0/1)#exit R2(config)#router ospf R2(config-router)#network 60.154.101.0 0.0.0.255 area 10 R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
Verification	Run the **show vrrp** command to verify the configuration. ● Check whether R1 used as the master reduces its VRRP priority from 30 to 90 when GigabitEthernet0/1 connected to the Wide Area Network (WAN) is unavailable. If so, R2 becomes the master. ● Check whether R1 changes its VRRP priority from 30 to 120 when GigabitEthernet 0/1 connected to the WAN recovers. If so, R1 is re-elected as the master.
R1	R1#show vrrp GigabitEthernet 0/2 - Group 1 State is Master Virtual IP address is 192.168.201.1 configured

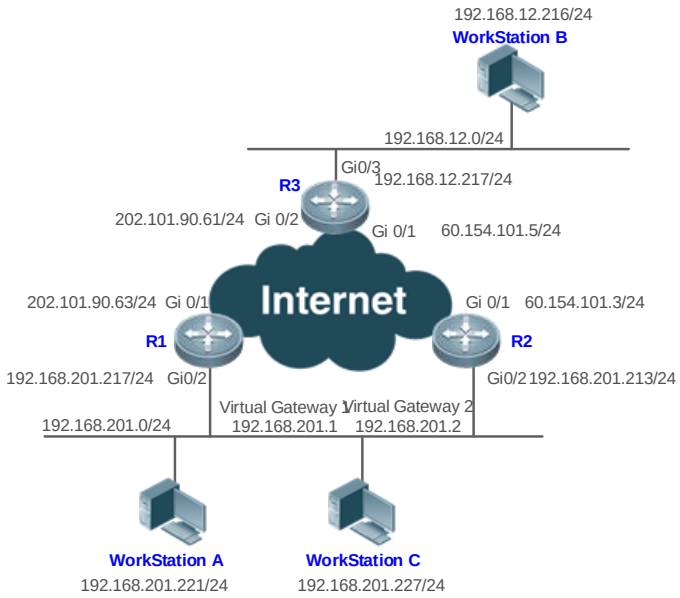
	Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.217 (local), priority is 120 Master Down interval is 10.59 sec Tracking state of 1 interface, 1 up: up GigabitEthernet 0/1 priority decrement=30
R2	R2#show vrrp GigabitEthernet 0/2 - Group 1 State is Backup Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.217 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec

Common Errors

- Different virtual IP addresses are configured on routers in a VRRP group, resulting in multiple master routers in the group.
- Different VRRP advertisement intervals are configured on routers in a VRRP group and the learning timer is not configured, resulting in multiple master routers in the group.
- Different VRRP versions are configured on routers in a VRRP group, resulting in multiple master routers in the group.
- For VRRPv2, Ethernet interfaces of the routers in a VRRP group are all in cleartext authentication mode but use inconsistent authentication strings, resulting in multiple master routers in the group.

Configuration Example

Configuring Multiple IPv4 VRRP Groups

Scenario **Figure 1-5**	
Configuration Steps	● The user workstation cluster (192.168.201.0/24) uses the VRRP group constituted by R1 and R2. The gateway for partial workstations (WorkStation A for example) points to the virtual IP address 192.168.201.1 of VRRP group 1, while that for other partial workstations (WorkStation C for example) points to the virtual IP address 192.168.201.2 of VRRP group 2. IPv4 multicast routing is enabled on all devices. ● R1 acts as the master router in VRRP group 2 and as a backup router in VRRP group 1. ● R2 acts as a backup router in VRRP group 2 and as the master router in VRRP group 1.

R3	`R3#configure terminal`
	`R3(config)#interface GigabitEthernet 0/3`
	`R3(config-if-GigabitEthernet 0/3)#no switchport`
	`R3(config-if-GigabitEthernet 0/3)#ip address 192.168.12.217 255.255.255.0`
	`R3(config-if-GigabitEthernet 0/3)#exit`
	`R3(config)#interface GigabitEthernet 0/1`
	`R3(config-if-GigabitEthernet 0/1)#no switchport`
	`R3(config-if-GigabitEthernet 0/1)#ip address 60.154.101.5 255.255.255.0`
	`R3(config-if-GigabitEthernet 0/1)#exit`
	`R3(config)#interface GigabitEthernet 0/2`
	`R3(config-if-GigabitEthernet 0/2)#no switchport`
	`R3(config-if-GigabitEthernet 0/2)#ip address 202.101.90.61 255.255.255.0`
	`R3(config-if-GigabitEthernet 0/2)#exit`
	`R3(config)#router ospf`
	`R3(config-router)#network 202.101.90.0 0.0.0.255 area 10`
	`R3(config-router)#network 192.168.12.0 0.0.0.255 area 10`
	`R3(config-router)#network 60.154.101.0 0.0.0.255 area 10`

R1	`R1#configure terminal`
	`R1(config)#interface GigabitEthernet 0/2`
	`R1(config-if-GigabitEthernet 0/2)#ip address 192.168.201.217 255.255.255.0`
	`R1(config-if-GigabitEthernet 0/2)#vrrp 1 timers advertise 3`

	R1(config-if-GigabitEthernet 0/2)#vrrp 1 ip 192.168.201.1 R1(config-if-GigabitEthernet 0/2)#vrrp 2 priority 120 R1(config-if-GigabitEthernet 0/2)#vrrp 2 timers advertise 3 R1(config-if-GigabitEthernet 0/2)#vrrp 2 ip 192.168.201.2 R1(config-if-GigabitEthernet 0/2)#vrrp 2 track GigabitEthernet 0/1 30 R1(config-if-GigabitEthernet 0/2)#exit R1(config)#interface GigabitEthernet 0/1 R1(config-if-GigabitEthernet 0/1)#ip address 202.101.90.63 255.255.255.0 R1(config-if-GigabitEthernet 0/1)#exit R1(config)#router ospf R1(config-router)#network 202.101.90.0 0.0.0.255 area 10 R1(config-router)#network 192.168.201.0 0.0.0.255 area 10
R2	R2#configure terminal R2(config)#interface GigabitEthernet 0/2 R2(config-if-GigabitEthernet 0/2)#ip address 192.168.201.213 255.255.255.0 R2(config-if-GigabitEthernet 0/2)#vrrp 1 ip 192.168.201.1 R2(config-if-GigabitEthernet 0/2)#vrrp 1 timers advertise 3 R2(config-if-GigabitEthernet 0/2)#vrrp 1 priority 120 R2(config-if-GigabitEthernet 0/2)#vrrp 2 ip 192.168.201.2 R2(config-if-GigabitEthernet 0/2)#vrrp 2 timers advertise 3 R2(config-if-GigabitEthernet 0/2)#exit R2(config)#interface GigabitEthernet 0/1 R2(config-if-GigabitEthernet 0/1)#ip address 60.154.101.3 255.255.255.0 R2(config-if-GigabitEthernet 0/1)#exit R2(config)#router ospf R2(config-router)#network 60.154.101.0 0.0.0.255 area 10 R2(config-router)#network 192.168.201.0 0.0.0.255 area 10
Verification	Run the **show vrrp** command to verify the configuration. ● Check whether R1 used as the master router in the group 2 reduces its VRRP group priority from 30 to 90 when it finds that GigabitEthernet 0/1 connected to a WAN is unavailable. If so, R2 in VRRP group 2 becomes the master router. ● Check whether R1 increases its VRRP group priority from 30 to 120 when it finds that GigabitEthernet 0/1 connected to a WAN becomes available again. If so, R1 becomes the master router again in VRRP group 2.
R1	R1#show vrrp GigabitEthernet 0/2 - Group 1 State is Backup Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100

	Master Router is 192.168.201.213 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec GigabitEthernet 0/2 - Group 2 State is Master Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.217 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec Tracking state of 1 interface, 1 up: up GigabitEthernet 0/1 priority decrement=30
R2	R2#show vrrp GigabitEthernet 0/2 - Group 1 State is Master Virtual IP address is 192.168.201.1 configured Virtual MAC address is 0000.5e00.0101 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 120 Master Router is 192.168.201.213 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec GigabitEthernet 0/2 - Group 2 State is Backup Virtual IP address is 192.168.201.2 configured Virtual MAC address is 0000.5e00.0102 Advertisement interval is 3 sec Preemption is enabled min delay is 0 sec Priority is 100 Master Router is 192.168.201.217 , priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec

Common Errors

- Different virtual IP addresses are configured on routers in a VRRP group, resulting in multiple master routers in the group.

- Different VRRP advertisement intervals are configured on routers in a VRRP group and the learning timer is not configured, resulting in multiple master routers in the group.
- Different VRRP versions are configured on routers in a VRRP group, resulting in multiple master routers in the group.
- For VRRPv2, the Ethernet interfaces of routers in a VRRP group are all in cleartext authentication mode but use inconsistent authentication strings, resulting in multiple master routers in the group.

1.4.2 Configuring IPv6 VRRP

Configuration Effect

- Configure an IPv6 VRRP group on an interface of a specific LAN segment by setting the VRID and virtual IPv6 address.
- Configure multiple IPv6 VRRP groups on an interface to achieve load balancing and achieve more stable and reliable network services.
- Configure the VRRP tracked interfaces to monitor failures, change interface priorities, and realize failover dynamically.

Notes

- To achieve VRRP, routers in a VRRP group should be configured with the same virtual IPv6 address.
- To achieve backup for multiple IPv6 VRRP groups, configure multiple IPv6 VRRP groups with identical VRRP configuration on an interface and configure different priorities for them so that they back up each other.
- VRRP must be enabled on Layer 3 interfaces.
- To use the IPv6 VRRP function on an N18000 with a CB line card inserted, enable the IPv6 VRRP function in global configuration mode first.

Configuration Steps

↘ Enabling IPv6 VRRP in Interface Configuration Mode

By default, IPv6 VRRP is not enabled on an interface. You can enable it as needed.

↘ Configuring the IPv6 VRRP Advertisement Interval

By default, the master router sends advertisement packets every 1s. You can modify the interval as needed.

↘ Configuring the IPv6 VRRP Preemption Mode

By default, a VRRP group operates in preemption mode without a delay.

↘ Enabling the Accept Mode for an IPv6 VRRP Group

By default, the Accept mode is disabled for an IPv6 VRRP group. To configure an IPv6 VRRP group in master state to receive and process packets with the destination IP address as that of the virtual router, enable the Accept mode.

↘ Configuring the IPv6 VRRP Router Priority

The default router priority for a VRRP group is 100. You can modify the priority as needed.

Configuring the IPv6 VRRP Tracked Interface

By default, no tracked interface is configured. You can modify the interval as needed.

Configuring the IPv6 VRRP Tracked IP Address

By default, no tracked IPv6 address is configured and the value of priority change is 10. You can configure this function as needed.

Configures the IPv6 VRRP Learning Timer

By default, the learning timer is disabled for a VRRP group. Enable this function if the backup routers need to learn the master's advertisement interval.

Configuring the Description for an IPv6 VRRP Group

By default, no description is configured for a VRRP group. To help distinguish VRRP groups, configure descriptions.

Configuring the IPv4 VRRP Delay

By default, the IPv6 VRRP delay is not configured. To guarantee an effective non-preemption mode, configure the delay.

Verification

Run the **show vrrp** command to verify the configuration.

Related Commands

Enabling IPv6 VRRP

Command	**vrrp** *group* **ipv6** *ipv6-address*
Parameter Description	*group*: Indicates the VRID of a VRRP group. The value range depends on product models. *ipv6-address*: Indicates the IPv6 address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	IPv6 and IPv4 VRRP groups share a VRID range from 1 to 255. One VRID is applicable to an IPv4 VRRP group and an IPv6 VRRP group simultaneously. The first configured address should be a link-local address, which can be deleted only after other virtual addresses.

Configuring the IPv6 VRRP Advertisement Interval

Command	**vrrp ipv6** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group, in seconds. ***csec*** *centisecond-interval:* Indicates the interval for the master router in a VRRP group to send VRRP packets. It is an integer from 50 to 99, in centiseconds. No default value is provided. The command is only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is 1s.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority, and other information.

	As defined by RFC standards, if an IPv4 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40s. Therefore, if the interval is larger than 40s, the maximum interval of 40s will be applied, though the configuration is effective.

Configuring the Preemption Mode

Command	**vrrp ipv6** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the master router to declare its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in preemption mode, a router with a higher priority will replace the master with a lower priority. If a VRRP group runs in non-preemption mode, a router with the priority higher than that of the master remains backup. When the VRRP group uses the IP address of an Ethernet interface, the device to which the Ethernet interface belongs has the highest priority and automatically becomes the master in the group.

Enabling the Accept Mode for an IPv6 VRRP Group

Command	**vrrp ipv6** *group* **accept_mode**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	By default, an IPv6 VRRP group in master state is not permitted to receive packets with the destination IPv6 address as that of the VRRP group. However, it receives NA and NS packets regardless of whether the Accept mode is configured. Besides, the IP address owner in master state receives and processes the packets with the destination IPv6 address as that of the VRRP group regardless of whether the Accept mode is configured.

Configuring the IPv6 VRRP Router Priority

Command	**vrrp ipv6** *group* **priority** *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of a VRRP router.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the VRRP router priority.

Configuring the IPv6 VRRP Tracked Interface

Command	**vrrp ipv6** *group* **track** *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the step of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command	Interface configuration mode

Mode	
Usage Guide	A tracked interface must be a routable Layer 3 logical interface, for example, a routed interface, an SVI, a loopback interface, or a tunnel interface. The priority of the router that has the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

Configuring the IPv6 VRRP Tracked IP Address

Command	**vrrp ipv6** *group* **track** { *ipv6-global-address* | *ipv6-linklocal-address interface-type interface-number* } [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv6-global-addres*: Indicates the IPv6 global unicast address. *ipv6-linklocal-address*: Indicates the IPv6 link-local address. *interface-type interface-number*: Indicates the interface to be tracked. ***interval*** *interval-value*: Indicates the probe interval, in seconds. The default value is 3s. ***timeout*** *timeout-value*: Indicates the probe timeout interval of waiting for response, in seconds. If no response is received within the timeout interval, the device considers that the destination is inaccessible. The default value is 1s. **retry** *retry-value*: Indicates the probe retry count. If no response is received after the probe retry count, the device considers that the destination is inaccessible. The default value is 3. *priority*: Indicates the step of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv6 address for an IPv6 VRRP group. If the host IP address being tracked is a link-local address, specify a network interface. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

Configures the IPv6 VRRP Learning Timer

Command	**vrrp ipv6** *group* **timers learn**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	After the learning timer is configured, a VRRP backup router learns the advertisement interval of NA packets from the master. The backup router calculates the interval for determining a failure of the master based on the learning timer but not the local advertisement interval. This command ensures that advertisement intervals between backup routers and the master are synchronized.

Configuring the Description for an IPv6 VRRP Group

Command	**vrrp ipv6** *group* **description** *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command	Interface configuration mode

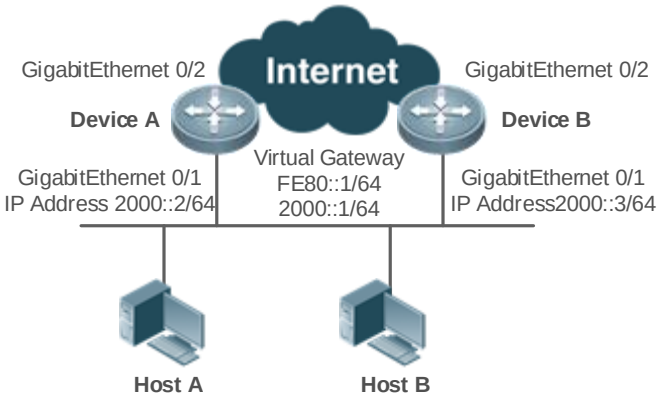
Mode	
Usage Guide	The description helps distinguish a VRRP group. A description has up to 80 bytes. If the description has more than 80 bytes, the system displays the message about incorrect configuration.

Configuring the IPv4 VRRP Delay

Command	**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode
Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group does not start when the system starts up or the interface becomes active. Instead, the VRRP group starts after the delay, ensuring that the non-preemption configuration is effective. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP group will be started immediately. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface. The value range of the delay of two types is from 0 to 60, in seconds.

Configuration Example

Configuring an IPv6 VRRP Group and Tracked Interface

Scenario **Figure 1-6**	
Configuration Steps	● Host A and Host B access the Internet resources through the default gateway address 2000::1/64. ● Device A and Device B belong to IPv6 VRRP group 1, and their virtual addresses are 2000::1/64 and FE80::1 respectively. ● Device A tracks GigabitEthernet 0/2 connected to the Internet. When GigabitEthernet 0/2 is unavailable, Device A reduces its priority and Device B acts as a gateway.

DeviceA	`Device A#configure terminal`
	`Device A(config)#interface GigabitEthernet 0/1`
	`Device A(config-if-GigabitEthernet 0/1)#no switchport`
	`Device A(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64`
	`Device A(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1`
	`Device A(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1`
	`Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120`

	Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 track GigabitEthernet 0/2 50 Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
DeviceB	Device B#configure terminal Device B(config)#interface GigabitEthernet 0/1 Device B(config-if-GigabitEthernet 0/1)#no switchport Device B(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64 Device B(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 Device B(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode
Verification	Run the **show ipv6 vrrp** command to verify the configuration. ● Check whether Device A used as the master router reduces its VRRP group priority from 50 to 70 when it finds that GigabitEthernet 0/2 connected to a WAN is unavailable. If so, Device B becomes the master. ● Check whether Device A increases its VRRP group priority from 50 to 120 when it finds that GigabitEthernet 0/2 connected to a WAN becomes available again. If so, Device A becomes the master again.
DeviceA	Device A#show ipv6 vrrp 1 GigabitEthernet 0/1 - Group 1 State is Master Virtual IPv6 address is as follows: FE80::1 2000::1 Virtual MAC address is 0000.5e00.0201 Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 120 Master Router is FE80::1234 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec Tracking state of 1 interface, 1 up: up GigabitEthernet 0/2 priority decrement=50
DeviceB	Device B#show ipv6 vrrp 1 GigabitEthernet 0/1 - Group 1 State is Backup Virtual IPv6 address is as follow: FE80::1 2000::1

```
Virtual MAC address is 0000.5e00.0201
Advertisement interval is 3 sec
Accept_Mode is enabled
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is FE80::1234, priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 10.82 sec
```

Common Errors

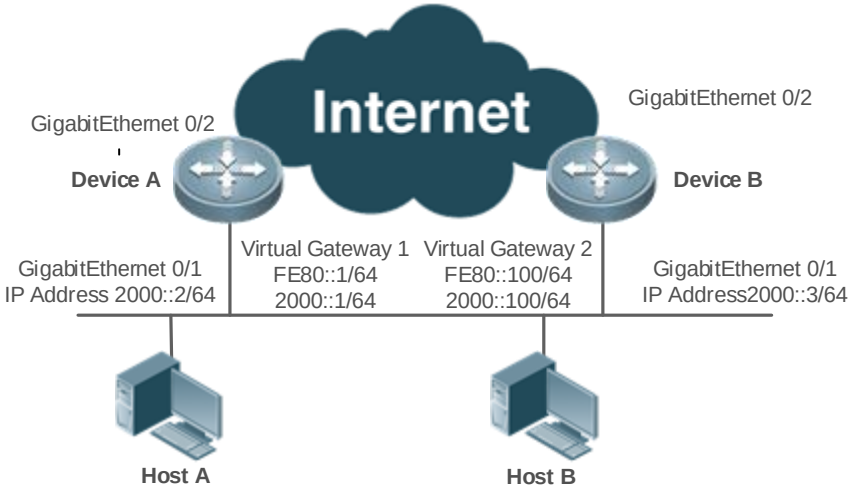
- Different virtual IP addresses are configured on routers in a VRRP group, resulting in multiple master routers in the group.
- Different VRRP advertisement intervals are configured on routers in a VRRP group and the learning timer is not configured, resulting in multiple master routers in the group.

Configuration Example

Configuring Multiple IPv6 VRRP Groups

Scenario

Figure 1-7



Configuration Steps

- Host A and Host B access the Internet resources through gateway addresses of 2000::1/64 and 2000::100/64 respectively.
- Device A and Device B belong to IPv6 VRRP group 1, and their virtual addresses are 2000::1/64 and FE80::1 respectively.
- Device A and Device B belong to IPv6 VRRP group 2 of a virtual IPv6 router, and their virtual addresses are 2000::100/64 and FE80::100 respectively.
- Device A and Device B act as gateways and forward flows. They back up to each other.

DeviceA

```
Device A#configure terminal
Device A(config)#interface GigabitEthernet 0/1
Device A(config-if-GigabitEthernet 0/1)#no switchport
Device A(config-if-GigabitEthernet 0/1)#ipv6 address 2000::2/64
```

	Device A(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 Device A(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1 Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 120 Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode Device A(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100 Device A(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100 Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 100 Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3 Device A(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode
DeviceB	Device B#configure terminal Device B(config)#interface GigabitEthernet 0/1 Device B(config-if-GigabitEthernet 0/1)#no switchport Device B(config-if-GigabitEthernet 0/1)#ipv6 address 2000::3/64 Device B(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 FE80::1 Device B(config-if-GigabitEthernet 0/1)#vrrp 1 ipv6 2000::1 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 priority 100 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 timers advertise 3 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 1 accept_mode Device B(config-if-GigabitEthernet 0/1)#vrrp 2 ipv6 FE80::100 Device B(config-if-GigabitEthernet 0/1)# vrrp 2 ipv6 2000::100 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 priority 120 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 timers advertise 3 Device B(config-if-GigabitEthernet 0/1)#vrrp ipv6 2 accept_mode
Verification	● Run the **show ipv6 vrrp** command to verify the configuration.
DeviceA	Device A#show ipv6 vrrp GigabitEthernet 0/1 - Group 1 State is Master Virtual IPv6 address is as follows: FE80::1 2000::1 Virtual MAC address is 0000.5e00.0201 Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 120 Master Router is FE80::1234 (local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec GigabitEthernet 0/1 - Group 2 State is Backup Virtual IPv6 address is as follows:

	FE80::100 2000::100 Virtual MAC address is 0000.5e00.0202 Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 100 Master Router is FE80::5678, priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec
DeviceB	Device B#show ipv6 vrrp GigabitEthernet 0/1 - Group 1 State is Backup Virtual IPv6 address is as follow: FE80::1 2000::1 Virtual MAC address is 0000.5e00.0201 Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 100 Master Router is FE80::1234, priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.82 sec GigabitEthernet 0/1 - Group 2 State is Master Virtual IPv6 address is as follows: FE80::100 2000::100 Virtual MAC address is 0000.5e00.0202 Advertisement interval is 3 sec Accept_Mode is enabled Preemption is enabled min delay is 0 sec Priority is 120 Master Router is FE80::5678(local), priority is 120 Master Advertisement interval is 3 sec Master Down interval is 10.59 sec

Common Errors

- Different virtual IP addresses are configured on routers in a VRRP group, resulting in multiple master routers in the group.

- Different VRRP advertisement intervals are configured on routers in a VRRP group and the learning timer is not configured, resulting in multiple master routers in the group.

1.4.3 Configuring VRRP and MSTP

Configuration Effect

VRRP and MSTP can be configured simultaneously, achieving link-level and gateway-level backup and improving network robustness.

Notes

- Configure routers in a VRRP group with the same virtual IPv4 address.
- Enable VRRP on a Layer 3 interface.

Configuration Steps

↘ Enabling IPv4 VRRP

By default, IPv4 VRRP is not enabled on an interface. You can enable it as needed.

↘ Configuring the IPv4 VRRP Authentication String

By default, VRRP is in a non-authentication mode. To enable cleartext password authentication for VRRP, perform this configuration.

↘ Configuring the IPv4 VRRP Advertisement Interval

By default, the master router sends advertisement packets every 1s. You can modify the interval as needed.

↘ Configuring the IPv4 VRRP Preemption Mode

By default, VRRP groups work in preemption mode without a delay.

↘ Configuring the IPv4 VRRP Router Priority

The default router priority for a VRRP group is 100. You can modify the priority as needed.

↘ Configuring the IPv4 VRRP Tracked Interface

By default, an IPv4 VRRP group does not monitor any interface. To detect faults through interface monitoring, perform this configuration.

↘ Configuring the IPv4 VRRP Learning Timer

By default, the learning timer is disabled for a VRRP group. Enable this function if backup routers need to learn the master's advertisement interval.

↘ Configuring the Description for an IPv4 VRRP Group

By default, no description is configured for a VRRP group. To help distinguish VRRP groups, configure descriptions.

↘ Configuring the IPv4 VRRP Delay

By default, the IPv4 VRRP delay is not configured. To guarantee an effective non-preemption mode, configure the delay.

Configuring the IPv4 VRRP Version

By default, IPv4 adopts the VRRPv2 standard. To change it, use the corresponding command.

Specifying a Sub-VLAN of a Super-VLAN to Receive the IPv4 VRRP Packets

By default, IPv4 VRRP packets are only sent to the first Up interface of a sub-VLAN in a super-VLAN. However, it is possible to configure them to be sent to a specific sub-VLAN in the super-VLAN.

Verification

Run the **show vrrp** command to verify the configuration.

Related Commands

Enabling IPv4 VRRP

Command	**vrrp** *group* **ip** *ipaddress* [**secondary**]
Parameter Description	*group*: Indicates the VRID of a VRRP group. The value range depends on product models. *ipaddrss*: Indicates the IP address of a VRRP group. **secondary**: Indicates the secondary IP address of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	If no virtual IP address is specified, routers cannot join a VRRP group. If no secondary IP address is applied, the configured IP address will be the primary IP address of a VRRP group.

Configuring the IPv4 VRRP Authentication String

Command	**vrrp** *group* **authentication** *string*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *string*: Indicates the authentication string of a VRRP group (a cleartext password consists of 8 bytes at most).
Command Mode	Interface configuration mode
Usage Guide	In a VRRP group, the same authentication password should be configured for routers. The cleartext authentication password cannot guarantee security but only prevents or prompts VRRP configuration errors. This command is only applicable to VRRPv2 but not VRRPv3. Authentication is abolished for VRRPv3 (IPv4 VRRP and IPv6 VRRP) packets. If VRRPv2 is chosen for an IPv4 VRRP group, the command is effective; if VRRPv3 is chosen, the command is ineffective.

Configuring the IPv4 VRRP Advertisement Interval

Command	**vrrp** *group* **timers advertise** { *advertise-interval* | **csec** *centisecond-interval* }
Parameter Description	*group*: Indicates the VRID of a VRRP group. *advertise-interval*: Indicates the advertisement interval of a VRRP group, in seconds. ***csec*** *centisecond-interval:* Indicates the interval for the master router in a VRRP group to send VRRP packets. It is an integer from 50 to 99, in centiseconds. No default value is provided. The command is

	only effective for VRRPv3 packets. If it is configured for VRRPv2 packets, the default interval is 1s.
Command Mode	Interface configuration mode
Usage Guide	If a router is elected as the master in a VRRP group, it sends VRRP advertisement packets at the set interval to announce its VRRP state, priority, and other information. As defined by RFC standards, if an IPv4 VRRP group adopts VRRPv3 for sending multicast packets, the maximum advertisement interval is 40s. Therefore, if the interval is larger than 40s, the maximum interval of 40s will be applied, though the configuration is effective.

Configuring the IPv4 VRRP Preemption Mode

Command	**vrrp** *group* **preempt** [**delay** *seconds*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. **delay** *seconds*: Indicates the preemption delay for the master router to declare its status. The default value is 0 second.
Command Mode	Interface configuration mode
Usage Guide	If a VRRP group runs in preemption mode, a router with a higher priority will replace the master with a lower priority. If a VRRP group runs in non-preemption mode, a router with the priority higher than that of the master remains backup. When the VRRP group uses the IP address of an Ethernet interface, the device to which the Ethernet interface belongs has the highest priority and automatically becomes the master in the group.

Configuring the IPv4 VRRP Router Priority

Command	**vrrp** *group* **priority** *level*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *level*: Indicates the priority of an interface in a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	This command is used to manually configure the priority of a VRRP group.

Configuring the IPv4 VRRP Tracked Interface

Command	**vrrp** *group* **track** *interface-type interface-number* [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *interface-type interface-number*: Indicates the interface to be tracked. *priority*: Indicates the step of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	A tracked interface must be a routable Layer 3 logical interface, for example, a routed interface, an SVI, a loopback interface, or a tunnel interface. The priority of the router that has the virtual IP address associated with a VRRP group must be 255, and no tracked interface can be configured on it.

Configuring the IPv4 VRRP Tracked IP Address

Command	**vrrp** *group* **track** *ipv4-address* [**interval** *interval-value*] [**timeout** *timeout-value*] [**retry** *retry-value*] [*priority*]
Parameter Description	*group*: Indicates the VRID of a VRRP group. *ipv4-addres*: Indicates the IPv4 address to be tracked. ***interval*** *interval-value*: Indicates the probe interval, in seconds. The default value is 3s. ***timeout*** *timeout-value*: Indicates the probe timeout interval of waiting for response, in seconds. If no response is received within the timeout interval, the device considers that the destination is inaccessible. The default value is 1s. **retry** *retry-value*: Indicates the probe retry count. If no response is received after the probe retry count, the device considers that the destination is inaccessible. The default value is 3. *priority*: Indicates the step of VRRP priority change when the state of a monitored interface changes. The default value is 10.
Command Mode	Interface configuration mode
Usage Guide	To monitor a host, specify its IPv4 address for an IPv4 VRRP group. If a VRRP group owns the actual IP address of an Ethernet interface, the group priority is 255, and no monitored IP address can be configured.

Configuring the IPv4 VRRP Learning Timer

Command	**vrrp** *group* **timers learn**
Parameter Description	*group*: Indicates the VRID of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	After the learning timer is configured, a VRRP backup router learns the advertisement interval of NA packets from the master. The backup router calculates the interval for determining a failure of the master based on the learning timer but not the local advertisement interval. This command ensures that advertisement intervals between backup routers and the master are synchronized.

Configuring the Description for an IPv4 VRRP Group

Command	**vrrp** *group* **description** *text*
Parameter Description	*group*: Indicates the VRID of a VRRP group. *text*: Indicates the description of a VRRP group.
Command Mode	Interface configuration mode
Usage Guide	The description helps distinguish a VRRP group. A description has up to 80 bytes. If the description has more than 80 bytes, the system displays the message about incorrect configuration.

Configuring the IPv4 VRRP Delay

Command	**vrrp delay** { **minimum** *min-seconds* | **reload** *reload-seconds* }
Parameter Description	**minimum** *min-seconds*: Indicates the VRRP delay after an interface state changes. **reload** *reload-seconds*: Indicates the VRRP delay after the system starts.
Command Mode	Interface configuration mode

Usage Guide	After the delay is configured for a VRRP group on an interface, the VRRP group does not start when the system starts up or the interface becomes active. Instead, the VRRP group starts after the delay, ensuring that the non-preemption configuration is effective. If the interface receives a VRRP packet during the delay, the delay will be canceled and the VRRP group will be started immediately. This configuration will be effective for both IPv4 and IPv6 VRRP groups of an interface. The value range of the delay of two types is from 0 to 60, in seconds.

Configuring the IPv4 VRRP Version

Command	**vrrp** *group* **version** { **2** | **3** }
Parameter Description	**2**: Indicates VRRPv2. **3**: Indicates VRRPv3.
Command Mode	Interface configuration mode
Usage Guide	Considering compatibility between VRRPv2 and VRRPv3, specify a standard for IPv4 VRRP based on the actual network condition. VRRPv2 is defined in RFC 3768 and VRRPv3 in RFC 5798. This command is only applicable to IPv4 VRRP.

Specifying a Sub-VLAN of a Super-VLAN to Receive IPv4 VRRP Packets

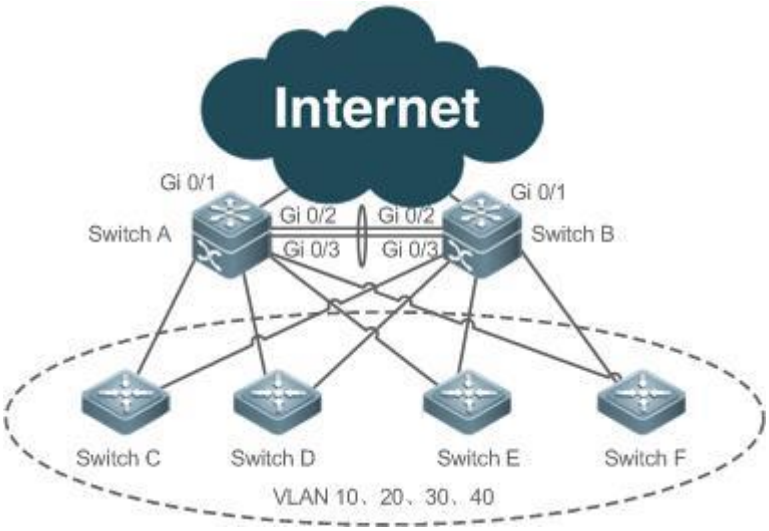
Command	**vrrp detection-vlan** { **first-subvlan** | *subvlan-id* }
Parameter Description	**first-subvlan**: Sends IPv4 VRRP packets only to the first Up interface of a sub-VLAN in a super-VLAN. *subvlan-id*: Sends packets to a specified sub-VLAN.
Command Mode	Interface configuration mode
Usage Guide	This command is used to specify a sub-VLAN of a super-VLAN to receive the IPv4 VRRP packets. IPv4 VRRP packets are sent in a super-VLAN using the following three methods. Packets are sent to the first Up interface of a sub-VLAN in a super-VLAN, or to a specified sub-VLAN interface in a super-VLAN, or to all the sub-VLAN interfaces in a super-VLAN. If VRRP and VRRP Plus are enabled simultaneously on a super-VLAN interface, VRRP packets are sent to all Up interfaces of sub-VLANs in the super-VLAN. This command is configured on a VLAN interface and effective only to super-VLAN interfaces.

Configuration Example

Configuring VRRP and MSTP

Scenario

Figure 1-8



Configuration Steps

- Configure MSTP on switches A, B, C, D, E and F. Configure VLAN-MSTI mapping (mapping VLAN 10 and VLAN 20 to MSTI 1, VLAN 30 and VLAN 40 to MSTI 2, and the rest VLANs to MSTI 0), and configure gateways (Switch A and Switch B in this example) as the root bridges of corresponding MSTIs.
- Add the SVIs of all VLANs to corresponding VRRP groups, and configure gateways as the master and backup routers for corresponding VRRP groups.

Gateway	VLAN ID	SVI	VRRP Group	Virtual IP Address	State
Switch A	10	192.168.10.2	VRRP group 10	192.168.10.1	Master
Switch B		192.168.10.3			Backup
Switch A	20	192.168.20.2	VRRP group 20	192.168.20.1	Master
Switch B		192.168.20.3			Backup
Switch A	30	192.168.30.2	VRRP group 30	192.168.30.1	Backup
Switch B		192.168.30.3			Master
Switch A	40	192.168.40.2	VRRP group 40	192.168.40.1	Backup
Switch B		192.168.40.3			Master

- Configure the uplink interface (Gi 0/1 of Switch A and Switch B) of master routers as a monitored interface of the master router.
- Create VLANs. Create VLAN 10, VLAN 20, VLAN 30, and VLAN 40 on Switch A and Switch B.
- Configure MST regions. Map VLAN 10 and VLAN 20 to MSTI 1, VLAN 30 and VLAN 40 to

	MSTI 2, and the rest VLANs to MSTI 0. ● Configure Switch A as the root bridge for MST 0 and MST 1, and Switch B as the root bridge for MST 2. ● Enable MSTP. ● Configure SVIs of all the VLANs, add the SVIs to corresponding VRRP groups, and configure virtual IP addresses for the groups. ● Configure master routers and backup routers for all the groups. ● Configure uplink interfaces of master routers as monitored ports of VRRP groups. Monitored interfaces must be Layer 3 interfaces. ● Configure Internet interfaces of core routers as aggregate interfaces.

SwitchA	`//Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 on Switch A.`
	`SwitchA#configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`SwitchA(config)#vlan range 10,20,30,40`
	`SwitchA(config-vlan-range)#exit`
	`//Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0.`
	`SwitchA(config)#spanning-tree mst configuration`
	`SwitchA(config-mst)#instance 1 vlan 10,20`
	`%Warning:you must create vlans before configuring instance-vlan relationship`
	`SwitchA(config-mst)#instance 2 vlan 30,40`
	`%Warning:you must create vlans before configuring instance-vlan relationship`
	`SwitchA(config-mst)#exit`
	`//On Switch A, configure the priority of MST 0 and MST 1 as 4096, and that of MST 2 as 8192.`
	`SwitchA(config)#spanning-tree mst 0 priority 4096`
	`SwitchA(config)#spanning-tree mst 1 priority 4096`
	`SwitchA(config)#spanning-tree mst 2 priority 8192`
	`//Enabling MSTP`
	`SwitchA(config)#spanning-tree`
	`Enable spanning-tree.`
	`//Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups.`
	`SwitchA(config)#interface vlan 10`
	`SwitchA(config-if-VLAN 10)#ip address 192.168.10.2 255.255.255.0`
	`SwitchA(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1`
	`SwitchA(config-if-VLAN 10)#exit`
	`SwitchA(config)#interface vlan 20`
	`SwitchA(config-if-VLAN 20)#ip address 192.168.20.2 255.255.255.0`
	`SwitchA(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1`
	`SwitchA(config-if-VLAN 20)#exit`
	`SwitchA(config)#interface vlan 30`
	`SwitchA(config-if-VLAN 30)#ip address 192.168.30.2 255.255.255.0`
	`SwitchA(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1`

	SwitchA(config-if-VLAN 30)#exit
	SwitchA(config)#interface vlan 40
	SwitchA(config-if-VLAN 40)#ip address 192.168.40.2 255.255.255.0
	SwitchA(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
	SwitchA(config-if-VLAN 40)#exit
	//Increase the priority of the VRRP 10 and VRRP 20 of Switch A to 120.
	SwitchA(config)#interface vlan 10
	SwitchA(config-if-VLAN 10)#vrrp 10 priority 120
	SwitchA(config-if-VLAN 10)#exit
	SwitchA(config)#interface vlan 20
	SwitchA(config-if-VLAN 20)#vrrp 20 priority 120
	SwitchA(config-if-VLAN 20)#exit
	//Configure the Gi 0/1 port of Switch A as Route Port and its IP address as10.10.1.1/24.
	SwitchA(config)#interface gigabitEthernet 0/1
	SwitchA(config-if-GigabitEthernet 0/1)#no switchport
	SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.10.1.1 255.255.255.0
	SwitchA(config-if-GigabitEthernet 0/1)#exit
	//Configure the Gi 0/1 port of Switch A as a monitored port for VRRP 10 and VRRP 20, and a Priority decrement of 30.
	SwitchA(config)#interface vlan 10
	SwitchA(config-if-VLAN 10)#vrrp 10 track gigabitEthernet 0/1 30
	SwitchA(config-if-VLAN 10)#exit
	SwitchA(config)#interface vlan 20
	SwitchA(config-if-VLAN 20)#vrrp 20 track gigabitEthernet 0/1 30
	SwitchA(config-if-VLAN 20)#exit
	//Configure ports Gi 0/2 and Gi 0/3 as AP ports, which are Trunk ports.
	SwitchA#configure terminal
	Enter configuration commands, one per line. End with CNTL/Z.
	SwitchA(config)#interface range gigabitEthernet 0/2-3
	SwitchA(config-if-range)#port-group 1
	SwitchA(config)#interface aggregateport 1
	SwitchA(config-if-AggregatePort 1)#switchport mode trunk

SwitchB	//Create VLAN 10, VLAN 20, VLAN 30 and VLAN 40 on Switch B.
	SwitchB#configure terminal
	Enter configuration commands, one per line. End with CNTL/Z.
	SwitchB(config)#vlan range 10,20,30,40
	SwitchB(config-vlan-range)#exit
	//Map VLAN 10 and VLAN 20 to Instance 1, VLAN 30 and VLAN 40 to Instance 2, and the rest VLANs to Instance 0.
	SwitchB(config)#spanning-tree mst configuration
	SwitchB(config-mst)#instance 1 vlan 10,20
	%Warning:you must create vlans before configuring instance-vlan relationship
	SwitchB(config-mst)#instance 2 vlan 30,40

```
%Warning:you must create vlans before configuring instance-vlan relationship
SwitchB(config-mst)#exit
//On Switch B, configure the priority of MST 2 as 4096, and that of MST 0 and MST 1 as 8192.
SwitchB(config)#spanning-tree mst 2 priority 4096
SwitchB(config)#spanning-tree mst 0 priority 8192
SwitchB(config)#spanning-tree mst 1 priority 8192
//Enabling MSTP
SwitchB(config)#spanning-tree
Enable spanning-tree.
//Configure SVIs of all the VLANs, add the SVIs to corresponding backup groups, and configure virtual IP addresses for the groups.
SwitchB(config)#interface vlan 10
SwitchB(config-if-VLAN 10)#ip address 192.168.10.3 255.255.255.0
SwitchB(config-if-VLAN 10)#vrrp 10 ip 192.168.10.1
SwitchB(config-if-VLAN 10)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if-VLAN 20)#ip address 192.168.20.3 255.255.255.0
SwitchB(config-if-VLAN 20)#vrrp 20 ip 192.168.20.1
SwitchB(config-if-VLAN 20)#exit
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#ip address 192.168.30.3 255.255.255.0
SwitchB(config-if-VLAN 30)#vrrp 30 ip 192.168.30.1
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#ip address 192.168.40.3 255.255.255.0
SwitchB(config-if-VLAN 40)#vrrp 40 ip 192.168.40.1
SwitchB(config-if-VLAN 40)#exit
//Increase the priority of VRRP 30 and VRRP 40 of Switch B to 120.
SwitchB(config)#interface vlan 30
SwitchB(config-if-VLAN 30)#vrrp 30 priority 120
SwitchB(config-if-VLAN 30)#exit
SwitchB(config)#interface vlan 40
SwitchB(config-if-VLAN 40)#vrrp 40 priority 120
SwitchB(config-if-VLAN 40)#exit
//Configure the Gi 0/1 port of Switch B as Route Port and its IP address as 10.10.1.1/24.
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#no switchport
SwitchB(config-if-GigabitEthernet 0/1)#ip address 10.10.2.1 255.255.255.0
SwitchB(config-if-GigabitEthernet 0/1)#exit
//Configure the Gi 0/1 port of Switch B as a monitored port for VRRP 30 and VRRP 40, and the Interface-Priority as 30.
SwitchB(config)#interface vlan 30
```

	SwitchB(config-if-VLAN 30)#vrrp 30 track gigabitEthernet 0/1 30 SwitchB(config-if-VLAN 30)#exit SwitchB(config)#interface vlan 40 SwitchB(config-if-VLAN 40)#vrrp 40 track gigabitEthernet 0/1 30 SwitchB(config-if-VLAN 40)#exit //Configure ports Gi 0/2 and Gi 0/3 as AP ports, which are Trunk ports. SwitchB #configure terminal Enter configuration commands, one per line. End with CNTL/Z. SwitchB (config)#interface range gigabitEthernet 0/2-3 SwitchB (config-if-range)#port-group 1 SwitchB (config)#interface aggregateport 1 SwitchB (config-if-AggregatePort 1)#switchport mode trunk
Verification	
Switch A	Check the configuration. SwitchA#show running-config ! vlan 10 ! vlan 20 ! vlan 30 ! vlan 40 ! spanning-tree spanning-tree mst configuration instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094 instance 1 vlan 10, 20 instance 2 vlan 30, 40 spanning-tree mst 0 priority 4096 spanning-tree mst 1 priority 4096 spanning-tree mst 2 priority 8192 interface GigabitEthernet 0/1 no switchport no ip proxy-arp ip address 10.10.1.1 255.255.255.0 ! interface GigabitEthernet 0/2 port-group 1 ! interface GigabitEthernet 0/3 port-group 1 ! interface AggregatePort 1

	switchport mode trunk
	!
	interface VLAN 10
	no ip proxy-arp
	ip address 192.168.10.2 255.255.255.0
	vrrp 10 priority 120
	vrrp 10 ip 192.168.10.1
	vrrp 10 track GigabitEthernet 0/1 30
	!
	interface VLAN 20
	no ip proxy-arp
	ip address 192.168.20.2 255.255.255.0
	vrrp 20 priority 120
	vrrp 20 ip 192.168.20.1
	vrrp 20 track GigabitEthernet 0/1 30
	!
	interface VLAN 30
	no ip proxy-arp
	ip address 192.168.30.2 255.255.255.0
	vrrp 30 ip 192.168.30.1
	!
	interface VLAN 40
	no ip proxy-arp
	ip address 192.168.40.2 255.255.255.0
	vrrp 40 ip 192.168.40.1
	//Check VRRP status.
	SwitchA#show vrrp brief
	Interface Grp Pri timer Own Pre State Master addr Group addr
	VLAN 10 10 120 3 - P Master 192.168.10.2 192.168.10.1
	VLAN 20 20 120 3 - P Master 192.168.20.2 192.168.20.1
	VLAN 30 30 100 3 - P Backup 192.168.30.3 192.168.30.1
	VLAN 40 40 100 3 - P Backup 192.168.40.3 192.168.40.1
	//Disconnect the uplink of Switch A, and check VRRP status.
	SwitchA#show vrrp brief
	Interface Grp Pri timer Own Pre State Master addr Group addr
	VLAN 10 10 90 3 - P Backup 192.168.10.3 192.168.10.1
	VLAN 20 20 90 3 - P Backup 192.168.20.3 192.168.20.1
	VLAN 30 30 100 3 - P Backup 192.168.30.3 192.168.30.1
	VLAN 40 40 100 3 - P Backup 192.168.40.3 192.168.40.1

Switch B	//Check the configuration. SwitchB#show running-config ! vlan 10 !

```
vlan 20
!
vlan 30
!
vlan 40
!
spanning-tree
spanning-tree mst configuration
 instance 0 vlan 1-9, 11-19, 21-29, 31-39, 41-4094
 instance 1 vlan 10, 20
 instance 2 vlan 30, 40
spanning-tree mst 0 priority 8192
spanning-tree mst 1 priority 8192
spanning-tree mst 2 priority 4096
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.10.2.1 255.255.255.0
!
interface GigabitEthernet 0/2
 port-group 1!
interface GigabitEthernet 0/3
 port-group 1
!
interface AggregatePort 1
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.3 255.255.255.0
 vrrp 10 ip 192.168.10.1
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.3 255.255.255.0
 vrrp 20 ip 192.168.20.1
!
interface VLAN 30
 no ip proxy-arp
 ip address 192.168.30.3 255.255.255.0
 vrrp 30 priority 120
 vrrp 30 ip 192.168.30.1
 vrrp 30 track GigabitEthernet 0/1 30
!
```

```
interface VLAN 40
 no ip proxy-arp
 ip address 192.168.40.3 255.255.255.0
 vrrp 40 priority 120
 vrrp 40 ip 192.168.40.1
 vrrp 40 track GigabitEthernet 0/1 30
//Check VRRP status.
SwitchB#show vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
VLAN 10 10 100 3 - P Backup 192.168.10.2 192.168.10.1
VLAN 20 20 100 3 - P Backup 192.168.20.2 192.168.20.1
VLAN 30 30 120 3 - P Master 192.168.30.3 192.168.30.1
VLAN 40 40 120 3 - P Master 192.168.40.3 192.168.40.1
//Disconnect the uplink of Switch B, and check VRRP status.
SwitchB#show vrrp brief
Interface Grp Pri timer Own Pre State Master addr Group addr
VLAN 10 10 100 3 - P Master 192.168.10.3 192.168.10.1
VLAN 20 20 100 3 - P Master 192.168.20.3 192.168.20.1
VLAN 30 30 120 3 - P Master 192.168.30.3 192.168.30.1
VLAN 40 40 120 3 - P Master 192.168.40.3 192.168.40.1
```

Common Errors

- Different virtual IP addresses are configured on routers in a VRRP group, resulting in multiple master routers in the group.
- Different VRRP advertisement intervals are configured on routers in a VRRP group and the learning timer is not configured, resulting in multiple master routers in the group.
- Different VRRP versions are configured on routers in a VRRP group, resulting in multiple master routers in the group.
- For VRRPv2, Ethernet interfaces of routers in a VRRP group are all in cleartext authentication mode and use inconsistent authentication strings, resulting in multiple master routers in the group.

1.5 Monitoring

Displaying

Command	Description
show [**ipv6**] **vrrp** [**brief** | *group*]	Displays brief or detailed information about IPv4/IPv6 VRRP.
show [**ipv6**] **vrrp interface** *type number* [**brief**]	Displays information about an IPv4/IPv6 VRRP group on a specified interface.
show vrrp [**brief** | *group*]	Displays brief or detailed information about IPv4 VRRP.
show vrrp interface *type number* [**brief**]	Displays information about an IPv4 VRRP group on a specified interface.

show vrrp packet statistics [*interface-type interface-number*]	Displays statistics on VRRP packets.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug [**ipv6**] **vrrp**	Debugs VRRP errors, events, packets, and status.
debug [**ipv6**] **vrrp errors**	Debugs VRRP errors.
debug [**ipv6**] **vrrp events**	Debugs VRRP events.
debug vrrp packets [**acl** *acl-id* **|** [**icmp | protocol**] **interface** *type number* [*group*]] **debug ipv6 vrrp packets** [**acl** *acl-name* **|** [**icmp | protocol**] **interface** *type number* [*group*]]	Debugs VRRP packets.
debug [**ipv6**] **vrrp state**	Debugs the VRRP status.

1 Configuring Supervisor Module Redundancy

1.1 Overview

Supervisor module redundancy is a mechanism that adopts real-time backup (also called hot standby) of the service running status of supervisor modules to improve device availability.

In a network device where the control plane is separated from the forwarding plane, the control plane runs on a supervisor module and the forwarding plane runs on line cards. The control plane information of the active supervisor module is backed up to the standby supervisor module in real time during device running. When the active supervisor module is shut down as expected (for example, due to software upgrade) or unexpectedly (for example, due to software or hardware exception), the device can automatically and rapidly switch to the standby supervisor module without user configuration loss, thereby ensuring normal operation of the network. The forwarding plane continues with packet forwarding during switching. Forwarding is not stopped and no link flapping occurs during restart of the control plane.

The supervisor module redundancy technology brings the following benefits to network services:

1 Improving network availability

The supervisor module redundancy technology sustains data forwarding and status information about user sessions during switching.

2 Preventing neighbors from detecting link flapping

The forwarding plane is not restarted during switching. Therefore, neighbors cannot detect the status change of a link from Down to Up.

3 Preventing route flapping

The forwarding plane sustains forwarding communication during switching, and the control plane rapidly constructs a new forwarding table. This process prevents route flapping.

4 Preventing loss of user sessions

User sessions that are created prior to switching are not lost because the session status is synchronized in real time.

1.2 Applications

Application	Description
Redundancy of Supervisor Modules	On a core switch where two supervisor modules are installed, the redundancy technology can improve network stability and system availability.

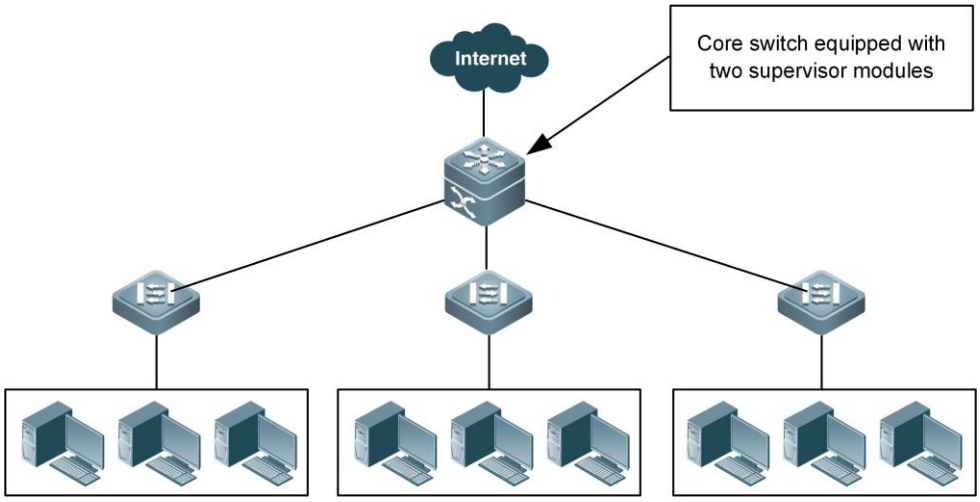
1.2.1 Redundancy of Supervisor Modules

Scenario

In Figure 1-1, in this network topology, if the core switch malfunctions, networks connected to the core switch may break down. To improve the network stability, two supervisor modules need to be configured on the core switch to implement redundancy. The active supervisor module manages the entire system and the standby supervisor module backs up

information about service running status of the active supervisor module in real time. When manual switching is performed or forcible switching is performed due to a failure on the active supervisor module, the standby supervisor module immediately takes over functions of the active supervisor module. The forwarding plane can proceed with data forwarding and the system availability is enhanced.

Figure 1-1



Deployment

For modular devices, the system is equipped with the active/standby backup mechanism. The system supports plug-and-play as long as active and standby supervisor modules conform to redundancy conditions.

For fixed devices, each device is equivalent to one supervisor module and one line card. The virtual switching unit (VSU) composed of multiple fixed devices also has the active and standby backup mechanism.

1.3 Features

Basic Concepts

Active and Standby Supervisor Modules

On a device where two supervisor modules are installed, the system elects one supervisor module as the active supervisor module. The other supervisor module functions as the backup supervisor module. When the active supervisor module malfunctions or proactively requests switching, the standby supervisor module takes over functions of the active supervisor module and becomes the new active supervisor module, which is called the standby supervisor module. Typically, the standby supervisor module does not participate in device management but monitors the running status of the active supervisor module.

Globally Active Supervisor Module, Globally Standby Supervisor Module, Globally Candidate Supervisor Module

In a VSU composed of two or more modular devices, each device has two supervisor modules, with the active supervisor module managing the entire chassis and the standby supervisor module functioning as a backup. For a VSU, there are two or more supervisor modules. One active supervisor module is elected out of the supervisor modules to manage the entire VSU, one standby supervisor module is elected as the backup of the VSU, and other supervisor modules are used as candidate supervisor modules. A candidate supervisor module replaces the active or standby

supervisor module and runs as the active or standby supervisor module when the original active or standby supervisor module malfunctions. In most cases, candidate supervisor modules do not participate in backup. To differentiate active and standby supervisor modules in a chassis from those in a VSU, the active, standby, and candidate supervisor modules in a VSU are called globally active, standby, and candidate supervisor modules respectively. The redundancy mechanism of supervisor modules takes effect on the globally active and standby supervisor module. Therefore, the active and standby supervisor modules in the VSU are globally ones.

In a VSU composed of two or more fixed devices, each fixed device is equivalent to one supervisor module and one line card. The system elects one device as the globally active supervisor module and one device as the globally standby supervisor module, and other devices serve as globally candidate supervisor modules.

↘ Prerequisites for Redundancy of Supervisor Modules

In a device system, hardware and software of all supervisor modules must be compatible so that supervisor modules in redundancy mode function properly.

Batch synchronization is required between the active and standby supervisor modules during startup so that the two supervisor modules are in the same state. Redundancy of supervisor modules is ineffective prior to synchronization.

↘ Redundancy Status of Supervisor Modules

The active supervisor module experiences the following status changes during active/standby backup:

- alone: In this state, only one supervisor module is running in the system, or active/standby switching is not complete, and redundancy is not established between the new active and standby supervisor modules.
- batch: In this state, redundancy is established between the active and standby supervisor modules and batch backup is being performed.
- realtime: The active supervisor module enters this state after the batch backup between active and standby supervisor modules is complete. Real-time backup is performed between the active and standby supervisor modules, and manual switching can be performed only in this state.

Overview

Feature	Description
Election of Active and Standby Supervisor Modules	The device can automatically select active and standby supervisor modules based on the status of the system. Manual selection is also supported.
Information Synchronization of Supervisor Modules	For supervisor modules in redundancy mode, the active supervisor module synchronizes status information and configuration files to the standby supervisor module in real time.

1.3.1 Election of Active and Standby Supervisor Modules

Working Principle

↘ Automatically Selecting Active and Standby Supervisor Modules for Modular Devices

You can install or remove supervisor modules during device running. The device, based on the current condition of the system, automatically selects an engine for running, without affecting normal data switching. The following cases may occur and the active supervisor module is selected accordingly:

- If only one supervisor module is installed during device startup, the device selects this supervisor module as the active supervisor module regardless of whether it is installed into the M1 slot or M2 slot.
- If two supervisor modules are installed during device startup, the supervisor module in the M1 slot is selected as the active supervisor module and the supervisor module in the M2 slot is selected as the standby supervisor module to serve as a backup by default, and relevant prompts are output.
- If one supervisor module is installed during device startup and another supervisor module is installed during device running, the supervisor module that is inserted later is used as the standby supervisor module to serve as a backup regardless of whether it is inserted into the M1 slot or M2 slot, and relevant prompts are output.
- Assume that two supervisor modules are installed during device startup and one supervisor module is removed during device running (or one supervisor module malfunctions). If the removed supervisor module is the standby supervisor module prior to removal (or failure), only a prompt is displayed after removal (or malfunction), indicating that the standby supervisor module is removed (or fails to run). If the removed supervisor module is the active supervisor module prior to removal (or failure), the other supervisor module becomes the active supervisor module and relevant prompts are output.

↘ Manually Selecting Active and Standby Supervisor Modules

You can manually select active and standby supervisor modules, which are selected as follows:

- In standalone mode, you can manually perform active/standby switching. The supervisor modules take effect after reset.
- In VSU mode, you can manually perform active/standby switching to make the globally standby supervisor module become the globally active supervisor module. If a VSU has only two supervisor modules, the original globally active supervisor module becomes the new globally standby supervisor module after reset. If there are more than two supervisor modules, one globally candidate supervisor module is elected as the new globally standby supervisor module and the original globally active supervisor module becomes a globally candidate supervisor module after reset.

Related Configuration

↘ Manually Performing Active/Standby Switching

- By default, the device can automatically select the active supervisor module.
- In standalone and VSU modes, you can run the **redundancy forceswitch** command to perform manual switching.

1.3.2 Information Synchronization of Supervisor Modules

Working Principle

- Status synchronization

The active supervisor module synchronizes its running status to the standby supervisor module in real time so that the standby supervisor module can take over functions of the active supervisor module at any time, without causing any obvious changes.

- Configuration synchronization

There are two system configuration files during device running: running-config and startup-config. running-config is a system configuration file dynamically generated during running and changes with the service configuration.

startup-config is a system configuration file imported during device startup. You can run the **write** command to write running-config into startup-config or run the **copy** command to perform the copy operation.

For some functions that are not directly related to non-stop forwarding, synchronization of system configuration files can ensure consistent user configuration during switching.

In the case of redundancy of dual supervisor modules, the active supervisor module periodically synchronizes startup-config and running-config files to the standby supervisor module and all candidate supervisor modules. Configuration synchronization is also triggered in the following operations:

1. The running-config file is synchronized when the device switches from the global configuration mode to privileged EXEC mode.
2. The startup-config file is synchronized when the **write** or **copy** command is executed to save the configuration.
3. Information configured over the Simple Network Management Protocol (SNMP) is not automatically synchronized and the synchronization of the running-config file needs to be triggered by running commands on the CLI.

Related Configuration

- By default, the startup-config and running-config files are automatically synchronized once per hour.

1.4 Configuration

Configuration	Description and Command	
Configuring Manual Active/Standby Switching	Optional.	
	show redundancy states	Displays the hot standby status.
	redundancy forceswitch	Manually performs active/standby switching.
Resetting Supervisor Modules	Optional.	
	redundancy reload	Resets the standby supervisor module or resets both the active and standby supervisor modules.

1.4.1 Configuring Manual Active/Standby Switching

Configuration Effect

The original active supervisor module is reset and the standby supervisor module becomes the new active supervisor module.

If there are more than two supervisor modules in the system, the original standby supervisor module becomes the active supervisor module, one supervisor module is elected out of candidate supervisor modules to serve as the new standby supervisor module, and the original active supervisor module becomes a candidate supervisor module after reset.

Notes

To ensure that data forwarding is not affected during switching, batch synchronization needs to be first performed between the active and standby supervisor modules so that the two supervisor modules are in the same state. That is, manual switching can be performed only when redundancy of supervisor modules is in real-time backup state. In

addition, to ensure synchronization of complete configuration files, service modules temporarily forbid manual active/standby switching during synchronization. Therefore, the following conditions need to be met simultaneously for manual switching:

- Manual active/standby switching is performed on the active supervisor module and a standby supervisor module is available.

Configuration Steps

- Optional.
- Perform the configuration on the active supervisor module.

Verification

Run the **show redundancy states** command to check whether the active and standby supervisor modules are switched.

Related Commands

Checking the Hot Standby Status

Command	**show redundancy states**
Parameter Description	N/A
Command Mode	Privileged EXEC mode or global configuration mode
Usage Guide	N/A

Manually Performing Active/Standby Switching

Command	**redundancy forceswitch**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Common Errors

N/A

1.4.2 Resetting Supervisor Modules

Configuration Effect

Resetting only the standby supervisor module does not affect data forwarding, and forwarding is not interrupted or user session information is not lost during reset of the standby supervisor module.

In standalone mode, running the **redundancy reload shelf** command will cause simultaneous reset of all supervisor modules and line cards in the chassis. In VSU mode, the device of a specified ID is reset when this command is

executed. If there are two or more devices in the system and the device to be reset is the device where the globally active supervisor module resides, the system performs active/standby switching.

Notes

In VSU mode, if the supervisor modules of the system do not enter the real-time backup state, resetting the device where the globally active supervisor module resides will cause the reset of the entire VSU.

Configuration Steps

Optional. Perform the reset when the supervisor modules or device runs abnormally.

Related Commands

Command	**redundancy reload** { **peer** | **shelf** [*switchid*] }
Parameter Description	**peer**: Resets only the standby supervisor module. **shelf** [*switchid*]: Indicates that the active and standby supervisor modules are set in standalone mode, and the ID of the device to be reset needs to be specified in VSU mode.
Command Mode	Privileged EXEC mode
Usage Guide	In standalone mode, **redundancy reload shelf** is used to reset the device. In VSU mode, **redundancy reload shelf** *switchid* is used to reset the device of a specified device ID.

Configuration Example

Resetting a Device in VSU Mode

Configuration Steps	In privileged EXEC mode of the globally active supervisor module, reset the device with the ID of 2.

	`Hostname# redundancy reload shelf 2`
	`This operation will reload the device 2. Are you sure to continue? [N/y] y`
	`Preparing to reload device 2!`

Verification	Check whether the relevant supervisor module or device is restarted.

1.5 Monitoring

Displaying

Command	Description
show redundancy states	Displays the redundancy status of dual supervisor modules.

1 Configuring WLAN Hot Standby

1.1 Overview

Wireless LAN (LAN) hot standby is a wireless dual-host hot standby function.

The WLAN hot standby function enables switchover over the Control and Provisioning of Wireless Access Points (CAPWAP) tunnels between access controllers (ACs) and access points (APs) within several milliseconds when the AC is unreachable or faulty, thus ensuring uninterrupted services for associated stations (STAs) to the maximum extent.

Working modes of WLAN hot standby include the active/standby (A/S) mode and the active/active (A/A) mode.

WLAN hot standby is applicable to a reliability-sensitive wireless network.

Protocols and Standards

N/A

1.2 Applications

Application	Description
1+1 A/S Networking	Two ACs are deployed. AC-1 and AC-2 are configured as hot standby ACs working in A/S mode.
1+1 A/A Networking	Two ACs are deployed. AC-1 and AC-2 are configured as hot standby ACs working in A/A mode.
N+1 A/S Networking	N+1 ACs are deployed and configured as hot standby ACs working in A/S mode.
Hierarchical AC Networking	A special N+1 networking mode is adopted in hierarchical AC scenarios.

1.2.1 1+1 A/S Networking

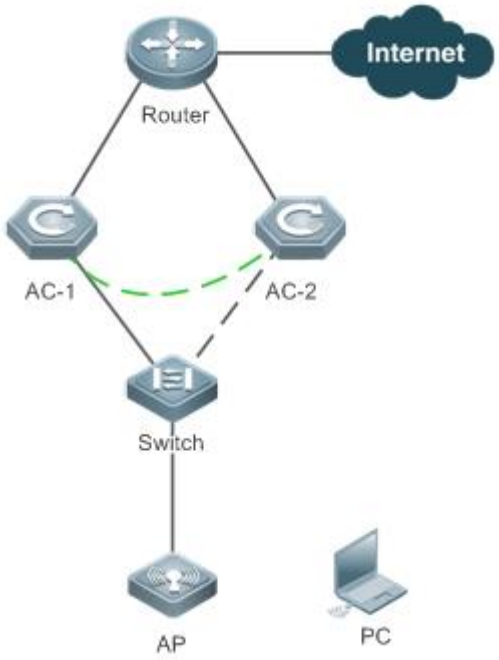
Scenario

On a wireless network, two ACs are deployed. One AC works as the active AC and provides services to external entities. The other AC works as the standby AC and receives data synchronized from the active AC.

When the active AC is unreachable due to some reasons (for example, the AC is upgraded and restarted or the power supply of the equipment room is interrupted), the standby AC can take over services from the active AC to ensure that the wireless network is not affected.

As shown in Figure 1-1, when AC-1 is unreachable but the switch and other devices work normally, AC-2 takes over services from AC-1. The wireless network is not affected and can still provide wireless services normally.

Figure 1-1



Remarks	The router functions as the gateway of STAs. The switch is an aggregation device that functions as the gateway of APs.

Deployment

- Enable the WLAN hot standby function on AC-1 and AC-2, and configure a hot standby instance.
- Add the AP group to which the AP belongs to the WLAN hot standby instance.

1.2.2 1+1 A/A Networking

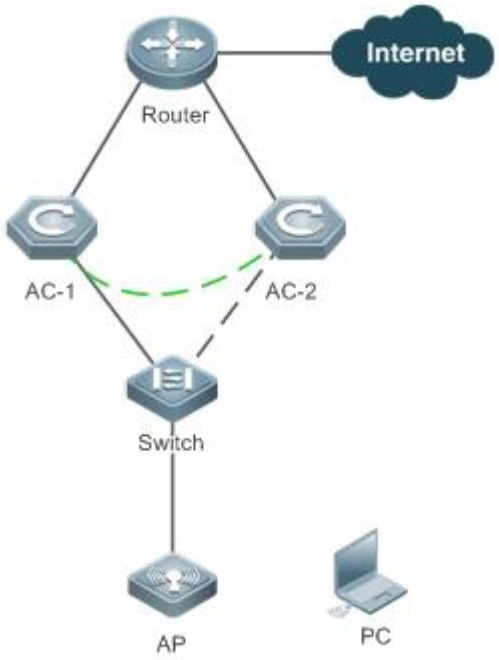
Scenario

On a wireless network, two ACs are deployed. Both ACs work as the active ACs and provide services to external entities. Both ACs work as the standby AC of the peer AC and receive data synchronized from the peer AC.

When one AC is unreachable due to some reasons (for example, the AC is upgraded and restarted or the power supply of the equipment room is interrupted), the other AC can take over services from the unreachable AC to ensure that the wireless network is not affected.

As shown in Figure 1-2, when AC-1 is unreachable but the switch and other devices work normally, AC-2 takes over services from AC-1. The wireless network is not affected and can still provide wireless services normally.

Figure 1-2



Remarks	The router functions as the gateway of STAs. The switch is an aggregation device that functions as the gateway of APs.

Deployment

- Enable the WLAN hot standby function on AC-1 and AC-2, and configure two hot standby instances.
- Add the AP group to which the AP belongs evenly to the two WLAN hot standby instances.

1.2.3 N+1 A/S Networking

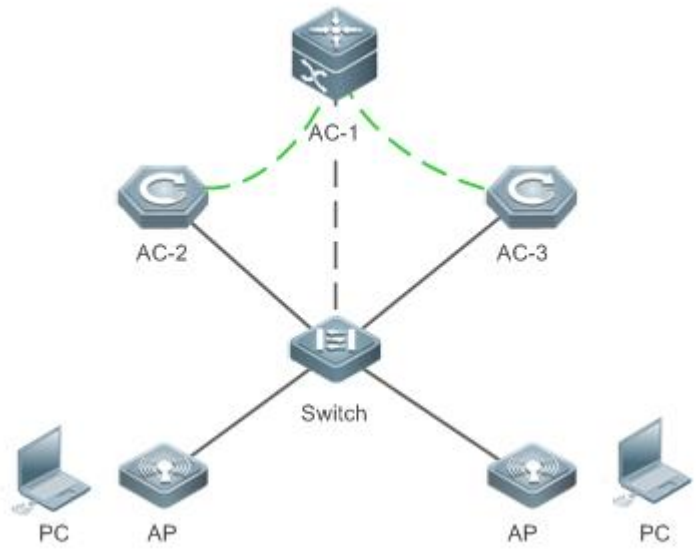
Scenario

On the wireless network, N+1 ACs are deployed. *N* ACs work as the active ACs and provide services to external entities. The other AC works as the standby AC and receives data synchronized from the active ACs.

When one active AC is unreachable (for example, the AC is upgraded and restarted or the power supply of the equipment room is interrupted), the standby AC can take over services from the active AC to ensure that the wireless network is not affected.

As shown in Figure 1-3, when AC-2 is unreachable but the switch, APs, and other devices work normally, AC-1 takes over services from AC-2. The wireless network is not affected and can still provide wireless services normally.

Figure 1-3



Remarks	The router functions as the gateway of STAs. The switch is an aggregation device that functions as the gateway of APs.

⚠ The N+1 A/S networking mode is not compatible with the 1+1 A/A networking mode.

Deployment

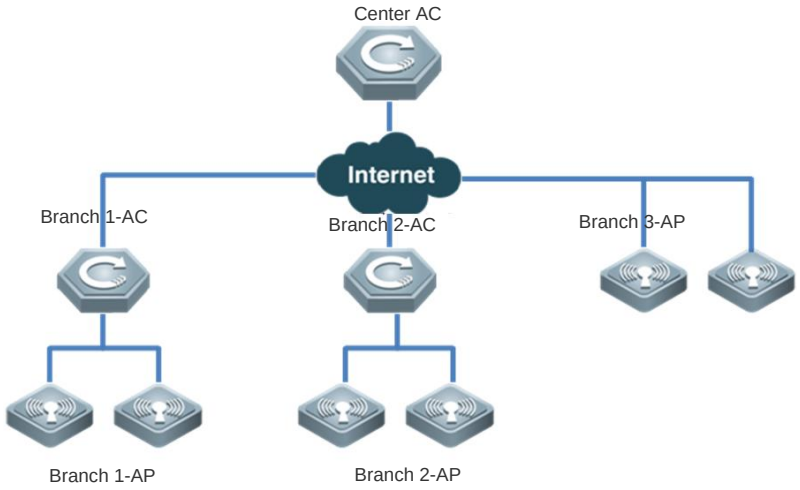
- Enable the WLAN hot standby function on AC-1, and configure two hot standby instances. Enable the WLAN hot standby function on AC-2 and AC-3, and configure a hot standby instance respectively on AC-2 and AC-3.
- Add the AP group to which the AP belongs to the WLAN hot standby instance.

1.2.4 Hierarchical AC Networking

Scenario

Hierarchical AC is a centralized management and distributed forwarding model. In this model, ACs are classified into the center AC and branch ACs. A high-performance AC is deployed at the center, and low-end ACs are deployed at braches. The following figure shows the model.

Figure 1-1



Deployment

- Enable the WLAN hot standby function and configure two hot standby instances on the center AC. Enable the WLAN hot standby function and configure one hot standby instance on Branch 1-AC and Branch 2-AC.
- Configure the center AC and branch ACs.
- Add the AP groups to which the APs belong to the corresponding WLAN hot standby instances.

1.3 Features

Basic Concepts

AC Keepalive Channel

After the hot standby function is enabled, the active AC periodically sends a keepalive packet to the standby AC, and the standby AC determines whether the active AC works normally based on the received keepalive packet. If the standby AC does not receive the packet in five consecutive keepalive periods, the standby AC determines that the active AC is faulty, and then notifies APs to activate the standby CAPWAP tunnel.

The keepalive period between ACs is 10s by default and is configurable.

Active CAPWAP Tunnel

To support the hot standby function, an AP must set up CAPWAP tunnels with two ACs that are configured with the hot standby relationship. The CAPWAP tunnel between the AP and the active AC is activated, and is called active CAPWAP tunnel.

Standby CAPWAP Tunnel

The CAPWAP tunnel between an AP and the standby AC is called standby CAPWAP tunnel. The standby CAPWAP tunnel is not used for communication between the AP and AC.

Hot Standby Instance

In A/A mode, the role of an AC varies according to APs. An AC that sets up an active CAPWAP tunnel with an AP serves as the active AC of the AP. An AC that sets up a standby CAPWAP tunnel with an AP serves as the standby AC of the AP. The AC with different roles must perform different backup operations, so different hot standby instances must be configured on the AC.

Overview

Feature	Description
Configuring	Enable the hot standby function to synchronize data.
Configuring Hierarchical AC	Configure WLAN hot standby connections in hierarchical AC networking.

1.3.1 Configuring Hot Standby

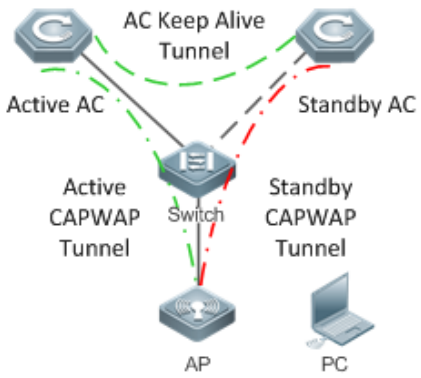
Configure addresses of hot standby neighbors and instances, and bind AP groups, DHCP address pool, and VRRP groups with the corresponding instances so that the hot standby function is enabled on the AP groups, DHCP address pool, and VRRP groups to support data synchronization and switchover.

Working Principle

The WLAN hot standby detection packet is a UDP packet, and the port ID is 7425. The control channel packet is a TCP packet, and the port ID is 6435. The data channel packet is a TCP packet, and the port ID is 6425. The heartbeat keepalive packet is an IP packet by default and can be configured as the UDP packet, the protocol field is 0, and the port ID is 7435.

WLAN hot standby enables switchover of the CAPWAP tunnels between ACs and APs within several milliseconds when an AC is unreachable or faulty, thus ensuring uninterrupted services for associated STAs to the maximum extent. Figure 1-4 shows the working principle of the WLAN hot standby function.

Figure 1-4 WLAN Hot Standby



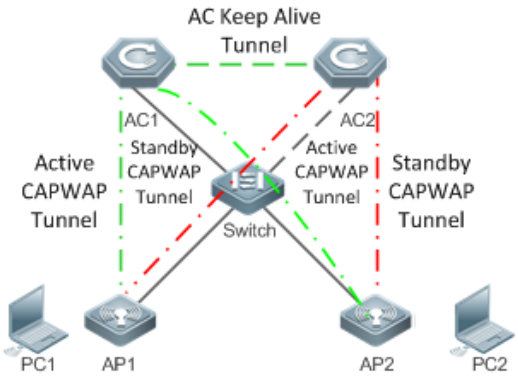
- Two ACs determine the active and standby roles through negotiation, and the keepalive mechanism is used between ACs.
- The AP sets up an active CAPWAP tunnel with the active AC and a standby CAPWAP tunnel with the standby AC.
- A STA is associated with the AP.
- The user communicates with external entities through the active CAPWAP tunnel.

- When the active AC is faulty, the standby AC detects the keepalive timeout event and immediately notifies the AP.
- The standby CAPWAP tunnel is activated, and the standby AC becomes the active AC.
- User's services are restored after the standby CAPWAP tunnel is activated.
- When the original active AC is restored, it sets up the hot standby relationship with the new active AC again. Then the original active AC becomes the standby AC and sets up a standby CAPWAP tunnel with the AP. In this way, ensuring service continuity.

Working modes of WLAN hot standby include the A/S mode and the A/A mode.

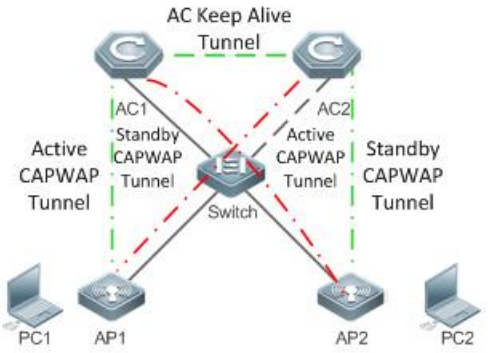
In A/S mode, one AC is the active AC, and the other AC is the standby AC. The active AC processes all services and transfers service status information to the standby AC for backup. The standby AC does not process services, and only backs up service data. In A/S mode, all the APs set up active CAPWAP tunnels with the active AC and standby CAPWAP tunnels with the standby AC. When both ACs work normally, all services are processed by the active AC. When the active AC is faulty, the standby AC takes over all services.

Figure 1-5 WLAN Hot Standby in A/S Mode



In A/A mode, both ACs are active ACs and process services, and serve as the standby AC of the other AC and back up service status information of the other AC. In A/A mode, some APs set up active CAPWAP tunnels with AC1, and standby CAPWAP tunnels with AC2. Other APs set up active CAPWAP tunnels with AC2, and standby CAPWAP tunnels with AC1. When both ACs work normally, the two ACs process services of APs with which active CAPWAP tunnels are set up. When AC1 is faulty, APs that set up active CAPWAP tunnels with AC1 switch over services to standby CAPWAP tunnels, and then AC2 processes services of all APs.

Figure 1-6 WLAN Hot Standby in A/A Mode



1.3.2 Configuring Hierarchical AC

Working Principle

Hierarchical AC is a special N+1 networking mode. In normal cases, the center AC is a high-performance AC and deployed at the center and branch ACs are deployed at branches. Hierarchical AC ensures unified upgrade, disaster recovery, unified management, and license sharing.

In hierarchical AC scenarios, the cold mode is added, which indicates lightweight data backup. In cold mode, most data backup with the peer is forbidden and only little data transmission is reserved. When traffic of the center AC is heavy, configure the working mode as cold to reduce the load of the center AC. In cold mode, when a branch AC is faulty, STAs need to be re-associated and STAs' IP addresses need to be obtained again for authentication. In cold mode, unified upgrade, unified management, and license sharing are reserved.

1.4 Configuration

Configuration	Description and Command	
Configuring the Hot Standby Function	(Mandatory) It is used to enable the hot standby function.	
	wlan hot-backup	Configures a hot standby neighbor.
	instance	Configures a hot standby instance.
	wlan hot-backup enable	Enables the hot standby function.
	(Optional) It is used to adjust the hot standby connection parameters.	
	local-ip	Configures the IP address of the local AC for the hot standby function.
	work-mode	Configures the hot standby working mode.
	hello-interval	Configures the heartbeat keepalive period for the hot standby function.
	kplv-pkt	Configures the format of the heartbeat keepalive packet for hot standby.

Configuration	Description and Command	
	priority level	Configures the priorities of instances.
	ap-group	Binds an AP group with an instance.
	dhcp-pool	Binds a DHCP address pool with an instance.
	dhcpv6-pool	Binds a DHCPv6 address pool with an instance.
	vrrp interface group	Binds a VRRP group with an instance.
	description	Configures the description for a hot standby peer.
Configuring Hierarchical AC	(Mandatory) It is used to enable the hierarchical AC function.	
	wlan hot-backup [**center** | **branch**]	Configures Hierarchical AC Roles.
	(Optional) It is used to set the lightweight backup mode.	
	work-mode cold	Configures Hierarchical AC Roles.

1.4.1 Configuring the Hot Standby Function

Configuration Effect

- Configure a hot standby connection to provide the hot standby service for other modules.

Notes

- After the hot standby function is enabled, the hot standby related configurations cannot be modified.

Configuration Step

Configuring Basic Information about Hot Standby

- Mandatory. The configuration is performed on the AC.
- Run the **wlan hot-backup** command to configure a hot standby neighbor. Unless otherwise specified, you must configure a hot standby neighbor on both ACs. Enter the hot standby configuration mode, and configure the working mode and instance for the hot standby function.
- In the hot standby configurations, the peer IP address is the loopback IP address of the peer AC. Ensure that the loopback IP address is correctly configured; otherwise, hot standby may become unavailable. In addition, configure routes to ensure that loopback IP addresses of the local and peer ends can be pinged successfully from each other.
- Run the **instance** command to configure an instance. Unless otherwise specified, you must configure the same instance on both ACs.

Command	**wlan hot-backup** *ip-address*
Parameter Description	*ip-address*: Indicates the IP address of the peer AC.
Defaults	No hot standby neighbor is configured.
Command Mode	Global configuration mode
Usage Guide	N/A

Command	**instance** *instance-id*
Parameter Description	*instance-id*: Indicates the ID of the instance.
Defaults	N/A
Command Mode	Hot standby configuration mode
Usage Guide	The value range is 0 to 65,535. In hierarchical AC scenarios, the value is 0-0.

Adjusting Hot Standby Parameters

- Optional. The configuration is performed on the AC.
- Run the **local-ip** command to configure the IP address of the local AC for hot standby. By default, the IP address of Loopback 0 on the AC is used. You can configure another IP address of the AC for setting up a hot standby relationship with the peer AC.
- Run the **work-mode** command to configure the hot standby working mode. Hot standby is switched to the quick switchover mode only when necessary, for example, in the onsite test environment. Two hot standby working modes are available:
  - Quick switchover mode: It is used in performance switchover scenarios that require sensitive detection and quick switchover, such as system demonstration and performance test. The default detection period is 10 ms.
  - Normal switchover mode: It is used in real-world application scenarios that require stable running and avoid hot standby flapping. The default detection period is 2s.
- Run the **hello-interval** command to configure the heartbeat keepalive period for the hot standby function. If quick switchover is required, you can set a short heartbeat keepalive period to accelerate hot standby detection and switchover. A shorter heartbeat keepalive period indicates that disconnection can be detected faster and it is easier to trigger a switchover. A longer heartbeat keepalive period indicates that the hot standby relationship is more stable.
- Run the **kplv-pkt** command to configure the format of heartbeat keepalive packets. If Network Address Translation (NAT) is deployed between ACs, IP packets are not allowed to be routed to the NAT device, which is limited by the intermediate NAT device. You can run this command to change the format of heartbeat keepalive packets to the UDP packets to ensure that the heartbeat channel is set up for hot standby.
- Run the **priority level** command to configure the priority of an instance. If an AC must be preferentially selected as the active AC, the hot standby priority of this AC must be increased. If an AC is required to support the switchback function, the hot standby priority of this AC must be set to 7.
- If the priority of an AC is high, the AC will be preferentially selected as the active AC when the hot standby connection is set up for the first time. If the AC with the priority of 7 is selected as the standby AC and completes batch backup of data, a hot standby switchback will be performed and this AC will be changed to the active AC again. To perform hot standby switchback, ensure that all APs that are connected to the peer AC also set up connections to the local AC. If this condition is met and the AC with the priority of 7 is selected as the standby AC, a hot standby switchback will be performed within the minimum switchover time (10 minutes by default, which is configurable) after batch backup is completed. Otherwise, a switchback will be performed forcibly 45 minutes after batch backup is completed. Some STAs may go offline due to the forced switchback.

Command	**local-ip** *ip-address*

Parameter Description	*ip-address*: indicates the IP address of the local AC.
Defaults	The IP address of Loopback 0 is used by default.
Command Mode	Hot standby configuration mode
Usage Guide	When the IP address of the local AC changes, the hot standby connection will be ended, and then the new IP address of the local AC will be used to set up a hot standby connection.

Command	**work-mode** [**normal** | **quick-switch** | **cold**]
Parameter Description	**normal**: Indicates the normal switchover mode. **quick-switch**: Indicates the quick switchover mode. **cold**: Indicates lightweight backup in HAC scenarios.
Defaults	normal
Command Mode	Hot standby configuration mode
Usage Guide	N/A

Command	**hello-interval** *hellointerval*
Parameter Description	*hellointerval*: Indicates the heartbeat keepalive period, in milliseconds. The value range is from 10 to 600000.
Defaults	The default value is related to the working mode. In normal mode, the default value is 2s (2000 ms). In quick switchover mode, the default value is 10 ms. After the hierarchical AC function is configured, the default value is 30s (30000 ms).
Command Mode	Hot backup configuration mode
Usage Guide	The value range is from 10 to 600000. In hierarchical AC scenarios, the value range is from 30000 to 600000.

Command	**kplv-pkt** [**ip** | **udp**]
Parameter Description	**ip**: Indicates that the heartbeat keepalive packet is an IP packet. **udp**: Indicates that the heartbeat keepalive packet is a UDP packet.
Defaults	IP packet
Command Mode	Hot standby configuration mode
Usage Guide	N/A

Command	**description** *name*
Parameter Description	*name*: Indicates the name of the hot standby peer.
Defaults	No name is configured.
Command	Hot standby configuration mode

Mode	
Usage Guide	N/A

Command	**priority level** *priority*
Parameter Description	*priority*: indicates the hot standby priority.
Defaults	The hot standby priority is 4 by default. In hierarchical AC scenarios, the hot standby priority is 7 for a branch AC.
Command Mode	Hot standby instance mode
Usage Guide	The value range is from 0 to 7. The default priority is 4, and the highest priority is 7. In hierarchical AC scenarios, the hot standby priority is 7 for a branch AC.

Binding the Hot Standby Function to an Instance

- Optional. The configuration is performed on the AC.
- Run the **ap-group** command to bind an AP group to a hot standby instance. After the AP group is bound to the hot standby instance, data of STAs associated with APs in the AP group can be synchronized from the active AC to the standby AC.
- Run the **dhcp-pool** command to bind a DHCP address pool with a hot standby instance. If IP addresses of STAs are on the hot standby AC, you need to bind the DHCP address pool to realize synchronization of DHCP entries between the active and standby ACs. After the DHCP address pool is bound to the instance, allocated IP addresses in this DHCP address pool can be synchronized from the active AC to the standby AC.
- Run the **dhcpv6-pool** command to bind a DHCPv6 address pool to a hot standby instance. If IP addresses of STAs are on the hot standby AC, you need to bind the DHCPv6 address pool to realize synchronization of DHCPv6 entries between the active and standby ACs. After the DHCPv6 address pool is bound to the instance, allocated IP addresses in this DHCPv6 address pool can be synchronized from the active AC to the standby AC.
- Run the **vrrp interface** command to bind a VRRP group to an instance if 802.1X or web-based authentication must support the hot standby function. After a VRRP group is bound to an instance, the virtual IP addresses in this VRRP group will determine the active/standby relationship based on the hot standby status.

Command	**ap-group** *ap-group*
Parameter Description	*ap-group*: Indicates the name of an AP group.
Defaults	No AP group is bound.
Command Mode	Hot standby instance mode
Usage Guide	N/A

Command	**dhcp-pool** *pool-name*
Parameter Description	*pool-name*: Indicates the name of a DHCP address pool.
Defaults	No DHCP address pool is bound.

Command Mode	Hot standby instance mode
Usage Guide	You can run the **show wlan hot-backup dhcp-pool config** command to check the binding configuration of a DHCP address pool.

Command	**dhcpv6-pool** *pool-name*
Parameter Description	*pool-name*: Indicates the name of a DHCPv6 address pool.
Defaults	No DHCPv6 address pool is bound.
Command Mode	Hot standby instance mode
Usage Guide	You can run the **show wlan hot-backup dhcpv6-pool config** command to check the binding configuration of a DHCPv6 address pool.

Command	**vrrp interface** *interface-name* **group** *vrrp-group*
Parameter Description	*interface-name*: Indicates the interface corresponding to the VRRP group. *vrrp-group*: Indicates the ID of a VRRP group.
Defaults	No VRRP group is bound.
Command Mode	Hot standby instance mode
Usage Guide	You can run the **show wlan hot-backup vrrp config** command to check the binding configuration of a VRRP group.

Enabling Hot Standby

- Mandatory. The configuration is performed on the AC.
- Unless otherwise specified, the hot standby function must be enabled on both ACs; otherwise, the hot standby function cannot take effect.
- You must ensure consistency in configurations of the two ACs that establish the hot standby relationship. In particular, the configuration sequence of interface-mapping configured in AP group configuration mode must be the same on both ACs.

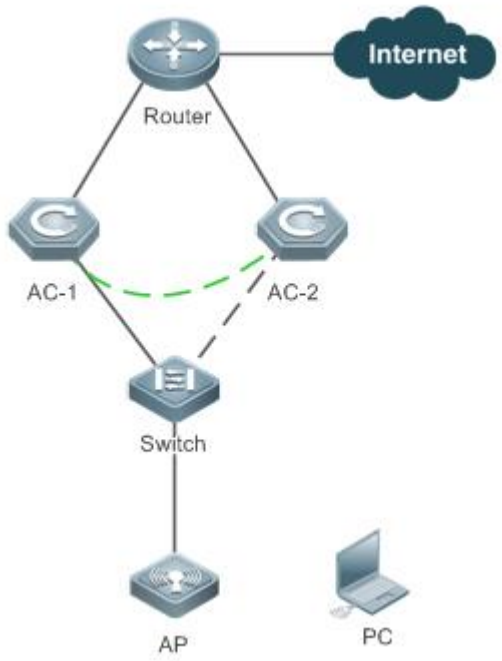
Command	**wlan hot-backup enable**
Parameter Description	N/A
Defaults	The hot standby function is disabled by default.
Command Mode	Hot standby configuration mode
Usage Guide	N/A

Verification

On the two ACs, check whether the hot standby connection is set up normally, and whether the hot standby status is normal.

Configuration Example

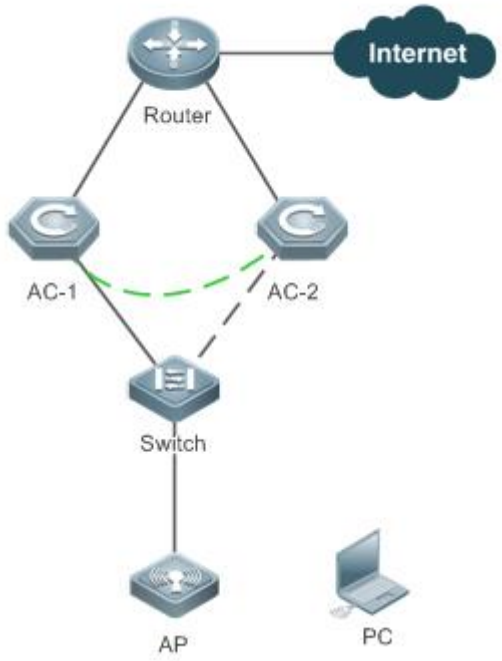
1+1 A/S Networking

Scenario **Figure 1-7**	
Configuration Steps	● Configure the peer IP addresses, including the IP address 192.168.1.100 of AC-1 and the IP address 192.168.1.200 of AC-2. ● Configure a hot standby instance. In the 1+1 A/S networking mode, configure only one instance on the two ACs, respectively. Note that the instance IDs configured on both ACs must be the same. ● Configure the priority of AC-1 for the hot standby instance. ● Configure the associated AP group. Bind the associated AP group **apg-a** to instance 10 on both ACs. ● Configure the VRRP group. In 1+1 A/S networking mode, both ACs have only one instance, and the two instances are in pairs. Therefore, you only need to configure one VRRP group, for example, VRRP group 1. Configure VRRP group 1 on the interface of VLAN 2 on two ACs, respectively. ● Enable the hot standby function.

AC-1	`AC-1# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC-1(config)# wlan hot-backup 192.168.1.200`
	`AC-1(config-hotbackup)# context 10`
	`AC-1(config-hotbackup-ctx)# priority level 7`
	`AC-1(config-hotbackup-ctx)# ap-group apg-a`
	`AC-1(config-hotbackup-ctx)# vrrp interface vlan 2 group 1`
	`AC-1(config-hotbackup-ctx)# exit`
	`AC-1(config-hotbackup)# wlan hot-backup enable`

AC-2	AC-2# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-2(config)# wlan hot-backup 192.168.1.100 AC-2(config-hotbackup)# context 10 AC-2(config-hotbackup-ctx)# ap-group apg-a AC-2(config-hotbackup-ctx)# vrrp interface vlan 2 group 1 AC-2(config-hotbackup-ctx)# exit AC-2(config-hotbackup)# wlan hot-backup enable
Verification	After the hot standby relationship is set up between AC-1 and AC-2, check the hot standby configuration.
AC-1	AC-1# show wlan hot-backup wlan hot-backup peer list: ip address hot-backup state description ------------------- ------------------- ------------------- ------------ 192.168.1.200 Enable CHANNEL_UP AC-1# show wlan hot-backup 192.168.1.200 wlan hot-backup 192.168.1.200 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 2000 kplv-pkt : ip ! context 10 hot-backup role : PAIR-ACTIVE hot-backup rdnd state : REALTIME-SYN hot-backup priority : 7
AC-2	AC-2# show wlan hot-backup wlan hot-backup peer list: ip address hot-backup state description ------------------- ------------------- ------------------- ------------ 192.168.1.100 Enable CHANNEL_UP AC-2# show wlan hot-backup 192.168.1.100 wlan hot-backup 192.168.1.100 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 1000 kplv-pkt : ip ! context 10 hot-backup role : PAIR-STANDBY hot-backup rdnd state : REALTIME-SYN hot-backup priority : 4

1+1 A/A Networking

Scenario **Figure 1-8**	
Configuration Steps	● Configure the peer IP addresses, including the IP address 192.168.1.100 of AC-1 and the IP address 192.168.1.200 of AC-2. ● Configure the instances and bind AP groups to instances. In 1+1 A/A networking mode, two instances must be configured and respectively bound to two AP groups on each of the two ACs. ● Configure VRRP groups. In 1+1 A/A networking mode, configure two instances on each of the two ACs. Assume that VRRP group 1 is configured on interfaces of VLAN 1 on AC-1 and AC-2, and VRRP group 2 is configured on interfaces of VLAN 2 on AC-1 and AC-2. Bind VRRP group 1 to instance 10, and VRRP group 2 to instance 20. ● Configure hot standby priorities. For instance 10, AC-1 is the active AC and therefore should be configured with the highest priority. For instance 20, AC-2 is the active AC and therefore should be configured with the highest priority. ● Enable the hot standby function.
AC-1	AC-1# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-1(config)# wlan hot-backup 192.168.1.200 AC-1(config-hotbackup)# context 10 AC-1(config-hotbackup-ctx)# ap-group apg-a AC-1(config-hotbackup-ctx)# vrrp interface vlan 1 group 1 AC-1(config-hotbackup-ctx)# priority level 7 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# context 20 AC-1(config-hotbackup-ctx)# ap-group apg-b AC-1(config-hotbackup-ctx)# vrrp interface vlan 2 group 2 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable

AC-2

```
AC-2# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
AC-2(config)# wlan hot-backup 192.168.1.100
AC-2(config-hotbackup)# context 10
AC-2(config-hotbackup-ctx)# ap-group apg-a
AC-2(config-hotbackup-ctx)# vrrp interface vlan 1 group 1
AC-2(config-hotbackup-ctx)# exit
AC-2(config-hotbackup)# context 20
AC-2(config-hotbackup-ctx)# ap-group apg-b
AC-2(config-hotbackup-ctx)# vrrp interface vlan 2 group 2
AC-2(config-hotbackup-ctx)# priority level 7
AC-2(config-hotbackup-ctx)# exit
AC-2(config-hotbackup)# wlan hot-backup enable
```

Verification

After the hot standby relationship is set up between AC-1 and AC-2, check the hot standby configurations.

AC-1

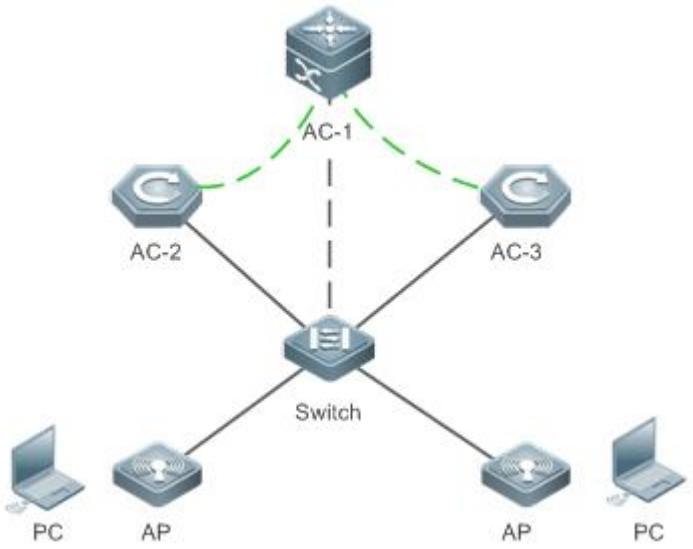
```
AC-1# show wlan hot-backup
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- ------------
192.168.1.200        Enable               CHANNEL_UP
AC-1# show wlan hot-backup 192.168.1.200
wlan hot-backup 192.168.1.200
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 2000
  kplv-pkt       : ip
  !
  context 10
    hot-backup role        : PAIR-ACTIVE
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 7
  !
  context 20
    hot-backup role        : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 4
```

AC-2

```
AC-2# show wlan hot-backup
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- -----------
192.168.1.100        Enable               CHANNEL_UP
AC-2# show wlan hot-backup 192.168.1.100
wlan hot-backup 192.168.1.100
```

```
hot-backup     : Enable
connect state  : CHANNEL_UP
hello-interval : 2000
kplv-pkt       : ip
!
context 10
  hot-backup role        : PAIR-STANDBY
  hot-backup rdnd state  : REALTIME-SYN
  hot-backup priority    : 4
!
context 20
  hot-backup role        : PAIR-ACTIVE
  hot-backup rdnd state  : REALTIME-SYN
  hot-backup priority    : 7
```

N+1 A/S Networking

Scenario **Figure 1-9**	
Configuration Steps	● Configure the peer IP addresses, including the IP address 192.168.1.100 of AC-1, IP address 192.168.1.200 of AC-2, and IP address 192.168.1.300 of AC-3. Configure two peer IP address on AC-1, and different peer IP addresses correspond to different instances. ● Configure the instances and bind AP groups to the instances. In N+1 A/S networking mode, one instance is configured on each of *N* ACs, and bound to the corresponding AP group. On the standby AC (AC-1 in this example), *N* instances must be configured and bound to AP groups on the corresponding active ACs. The AP groups configured on the *N* active ACs cannot conflict with each other. ● Configure VRRP groups. In N+1 A/S networking mode, one VRRP group must be configured on each of *N* active ACs, and *N* VRRP groups must be configured on the standby AC. ● Configure hot standby priorities. In N+1 A/S networking mode, the priorities of instances on the *N* active ACs must be set to the highest priority, and the priorities of instances on the standby AC can be set to the default value 4.

AC-1	AC-1# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-1(config)# wlan hot-backup 192.168.1.200 AC-1(config-hotbackup)# context 10 AC-1(config-hotbackup-ctx)# ap-group apg-a AC-1(config-hotbackup-ctx)# vrrp interface vlan 1 group 1 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable AC-1(config-hotbackup)# exit AC-1(config)# wlan hot-backup 192.168.1.300 AC-1(config-hotbackup)# context 20 AC-1(config-hotbackup-ctx)# ap-group apg-b AC-1(config-hotbackup-ctx)# ap-group apg-c AC-1(config-hotbackup-ctx)# vrrp interface vlan 2 group 2 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable
AC-2	AC-2# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-2(config)# wlan hot-backup 192.168.1.100 AC-2(config-hotbackup)# context 10 AC-2(config-hotbackup-ctx)# ap-group apg-a AC-2(config-hotbackup-ctx)# vrrp interface vlan 1 group 1 AC-2(config-hotbackup-ctx)# priority level 7 AC-2(config-hotbackup-ctx)# exit AC-2(config-hotbackup)# wlan hot-backup enable
AC-3	AC-3# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-3(config)# wlan hot-backup 192.168.1.100 AC-3(config-hotbackup)# context 20 AC-3(config-hotbackup-ctx)# ap-group apg-b AC-3(config-hotbackup-ctx)# ap-group apg-c AC-3(config-hotbackup-ctx)# vrrp interface vlan 2 group 2 AC-3(config-hotbackup-ctx)# priority level 7 AC-3(config-hotbackup-ctx)# exit AC-3(config-hotbackup)# wlan hot-backup enable
Verification	After the hot standby relationship is set up between AC-1 and AC-2 and between AC-1 and AC-3, check the hot standby configuration.
AC-1	AC-1# show wlan hot-backup wlan hot-backup peer list: ip address hot-backup state description ---------- ---------- ---------- ----------- 192.168.1.200 Enable CHANNEL_UP 192.168.1.300 Enable CHANNEL_UP

```
AC-1# show wlan hot-backup 192.168.1.200
wlan hot-backup 192.168.1.200
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 2000
  kplv-pkt       : ip
  !
  context 10
    hot-backup role        : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 4
AC-1# show wlan hot-backup 192.168.1.300
wlan hot-backup 192.168.1.300
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 2000
  kplv-pkt       : ip
  !
  context 20
    hot-backup role        : PAIR-STANDBY
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 4
```

AC-2

```
AC-2# show wlan hot-backup
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- -----------
192.168.1.100        Enable               CHANNEL_UP
AC-2# show wlan hot-backup 192.168.1.100
wlan hot-backup 192.168.1.100
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 2000
  kplv-pkt       : ip
  !
  context 10
    hot-backup role        : PAIR-ACTIVE
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 7
```

AC-3

```
AC-3# show wlan hot-backup
wlan hot-backup peer list:
ip address           hot-backup           state                description
-------------------- -------------------- -------------------- -----------
192.168.1.100        Enable               CHANNEL_UP
AC-3# show wlan hot-backup 192.168.1.100
```

```
wlan hot-backup 192.168.1.100
  hot-backup     : Enable
  connect state  : CHANNEL_UP
  hello-interval : 1000
  kplv-pkt       : ip
  !
  context 20
    hot-backup role        : PAIR-ACTIVE
    hot-backup rdnd state  : REALTIME-SYN
    hot-backup priority    : 7
```

Common Errors

- N/A

1.4.2 Configuring Hierarchical AC

Configuration Effect

Establish hot standby connections in hierarchical AC scenarios.

Notes

- The hierarchical AC roles (center AC and branch ACs) must be configured.
- After the hot standby function is enabled for a branch, the hierarchical AC role and working mode cannot be changed.
- In hierarchical AC scenarios, changing the forwarding mode may lead to disconnection and reconnection of the hot standby channel. The hot standby channel cannot be established in central forwarding mode.
- In hierarchical AC scenarios, the quick switchover mode is not supported and the minimum value of **hello-interval** is 30s.

Configuration Steps

↘ Configuring Hierarchical AC Roles

Hierarchical AC roles must be configured in hierarchical AC scenarios.

Command	**wlan hot-backup** [**center** | **branch**]
Parameter Description	**center**: Indicates the center AC. **branch**: Indicates the branch AC.
Defaults	No hierarchical AC role is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring the Cold Mode in Hierarchical AC Scenarios

- Configure the cold mode on branch ACs that require lightweight backup.

- In cold mode, most data backup with the peer is forbidden and only little data transmission is reserved. When traffic of the center AC is heavy, configure the working mode as cold to reduce the load of the center AC. In cold mode, when a branch AC is faulty, STAs need to be re-associated and STAs' IP addresses need to be obtained again for authentication.

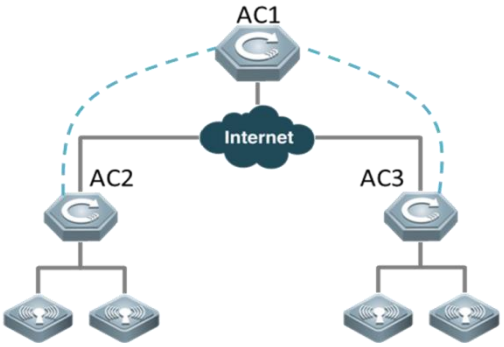
Command	**work-mode cold**
Parameter Description	N/A
Defaults	The working mode is normal by default.
Command Mode	Hot standby configuration mode
Usage Guide	N/A

Verification

On the center AC and branch ACs, check whether the hot standby connection is normally established and the hot standby status is normal.

Configuration Example

Hierarchical AC Networking

Scenario	
Figure 1-2	
Configuration Steps	• Configure hierarchical AC roles. Configure AC-1 as the center AC and AC-2 and AC-3 as branch ACs. • Configure peer IP addresses. The IP address of center AC-1 is 192.168.1.100, the IP address of branch AC-2 is 192.168.1.200, and the IP address of branch AC-3 is 192.168.1.300. Two peer IP addresses need to be configured on AC-1. Different peer IP addresses correspond to different configuration space. • Configure description of AC-2 as RD-Office and that of AC-3 as HR-Office. • Configure the working mode on AC-3 as cold. • Configure hot standby priorities. In N+1 A/S mode, the highest priority needs to be configured for hot standby instances on branch ACs, and the default priority 4 is configured for the hot standby instances on the center AC.

AC-1	`AC-1# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`AC-1(config)# wlan hot-backup center`

	AC-1(config)# wlan hot-backup 192.168.1.200 AC-1(config-hotbackup)# description RD_Office AC-1(config-hotbackup)# context 10 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable AC-1(config-hotbackup)# exit AC-1(config)# wlan hot-backup 192.168.1.300 AC-1(config-hotbackup)# description HR_Office AC-1(config-hotbackup)# work-mode cold AC-1(config-hotbackup)# context 20 AC-1(config-hotbackup-ctx)# exit AC-1(config-hotbackup)# wlan hot-backup enable
AC-2	AC-2# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-2(config)# wlan hot-backup branch AC-2(config)# wlan hot-backup 192.168.1.100 AC-2(config-hotbackup)# context 10 AC-2(config-hotbackup-ctx)# priority level 7 AC-2(config-hotbackup-ctx)# exit AC-2(config-hotbackup)# wlan hot-backup enable
AC-3	AC-3# configure terminal Enter configuration commands, one per line. End with CNTL/Z. AC-3(config)# wlan hot-backup branch AC-3(config)# wlan hot-backup 192.168.1.100 AC-3(config-hotbackup)# context 20 AC-3(config-hotbackup-ctx)# priority level 7 AC-3(config-hotbackup-ctx)# exit AC-3(config-hotbackup)# wlan hot-backup enable
Verification	After the hot standby relationship is established between AC-1 and AC-2 or AC-1 and AC-3, display the hot standby configurations.

AC-1	AC-1# show wlan hot-backup
	layer: center
	wlan hot-backup peer list:
	ip address hot-backup state description
	---------- ---------- ---------- -----------
	192.168.1.200 Enable CHANNEL_UP RD_Office
	192.168.1.300 Enable CHANNEL_UP HR_Office
	AC-1# show wlan hot-backup 192.168.1.200
	wlan hot-backup 192.168.1.200
	hot-backup : Enable
	  connect state : CHANNEL_UP
	  hello-interval : 30000
	  kplv-pkt : ip

	work-mode : NORMAL ! context 10 hot-backup role : PAIR-STANDBY hot-backup rdnd state : REALTIME-SYN hot-backup priority : 4 AC-1# show wlan hot-backup 192.168.1.300 wlan hot-backup 192.168.1.300 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 30000 kplv-pkt : ip work-mode : COLD ! context 20 hot-backup role : PAIR-STANDBY hot-backup rdnd state : REALTIME-SYN hot-backup priority : 4
AC-2	AC-2# show wlan hot-backup layer: branch wlan hot-backup peer list: ip address hot-backup state description 192.168.1.100 Enable CHANNEL_UP AC-2# show wlan hot-backup 192.168.1.100 wlan hot-backup 192.168.1.100 hot-backup : Enable connect state : CHANNEL_UP hello-interval : 30000 kplv-pkt : ip work-mode : NORMAL ! context 10 hot-backup role : PAIR-ACTIVE hot-backup rdnd state : REALTIME-SYN hot-backup priority : 7
AC-3	AC-3# show wlan hot-backup layer: branch wlan hot-backup peer list: ip address hot-backup state description 192.168.1.100 Enable CHANNEL_UP AC-3# show wlan hot-backup 192.168.1.100 wlan hot-backup 192.168.1.100

```
hot-backup     : Enable
connect state  : CHANNEL_UP
hello-interval : 30000
kplv-pkt       : ip
work-mode      : COLD
!
context 20
  hot-backup role        : PAIR-ACTIVE
  hot-backup rdnd state  : REALTIME-SYN
  hot-backup priority    : 7
```

1.5 Monitoring

Displaying

Command	Description
show wlan hot-backup [*ip-address*]	Displays the global AC hot standby configuration.
show wlan hot-backup dhcp-pool config *ip-address*	Displays the instance binding configuration of the DCHP address pool and the neighbor address.
show wlan hot-backup dhcpv6-pool config *ip-address*	Displays the instance binding configuration of the DCHPv6 address pool and the neighbor address.
show wlan hot-backup vrrp config *ip-address*	Displays the binding configuration between VRRP groups and instances for the neighbor addresses.

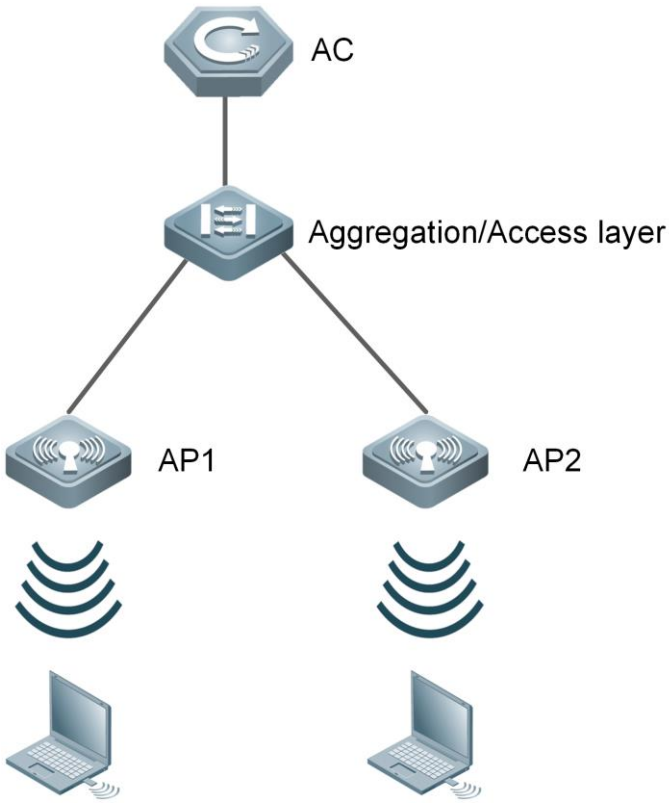
1 Configuring VAC

1.1 Overview

In an AC+fit AP distributed network, there are thousands of and even tens of thousands of APs. How to guarantee reliability of wireless access is essential on a large-scale network.

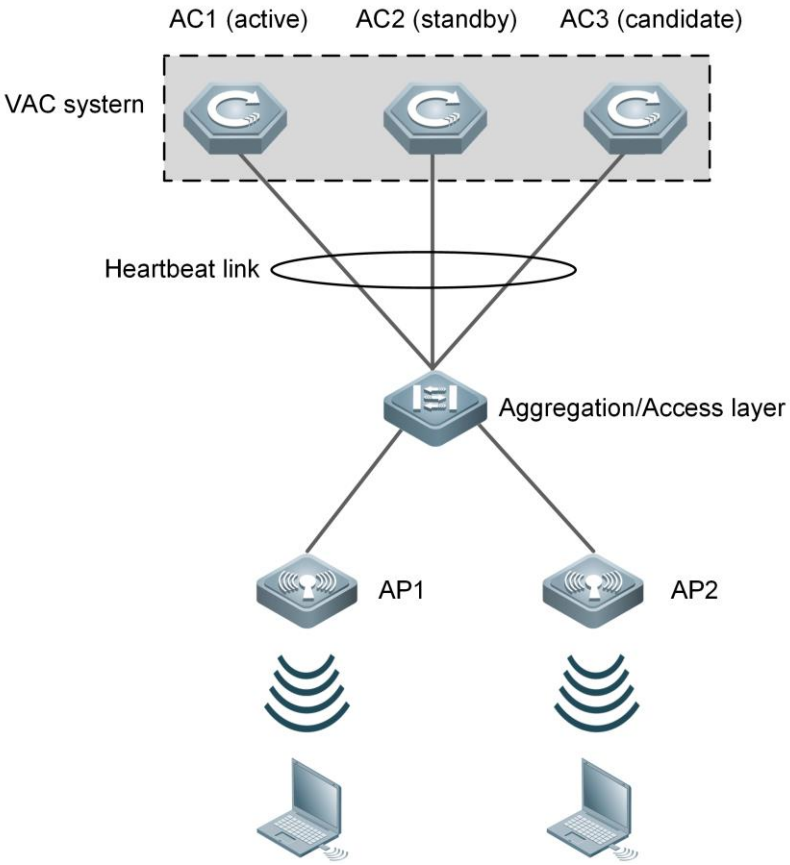
In existing AC+fit AP networking mode, an AP discovers the AC through the Control and Provisioning of Wireless Access Points (CAPWAP) protocol. The AP can receive services from the AC only after being successfully registered and associated with the AC. As a result, the process in which an AP detects whether the AC is faulty through CAPWAP keepalive packets is time-consuming. If an AC malfunctions, all APs need to re-register with another AC. The incurred network interruption duration imposes great impact on enterprises. How to shorten the switch time to reduce impact on the network is an issue to be urgently resolved.

Figure 4-1 Conventional Network Architecture



Virtual AC (VAC) is a network system virtualization technology that virtualizes multiple ACs into one virtual device. As shown in Figure 4-2, multiple ACs of the same model can form a VAC system. Compared with the conventional networking mode, this networking simplifies the network topology, reduces network management and maintenance costs, shortens the application recovery time and service interruption time, and improves network resource utilization.

Figure 4-2 VAC Networking Mode



1.2 Applications

Application	Description
Managing Multiple Devices	Multiple physical devices compose one logical device for unified management.
Improving the AC's Reliability	Multiple devices are available for fast switching, thereby improving reliability.

1.2.1 Managing Multiple Devices Uniformly

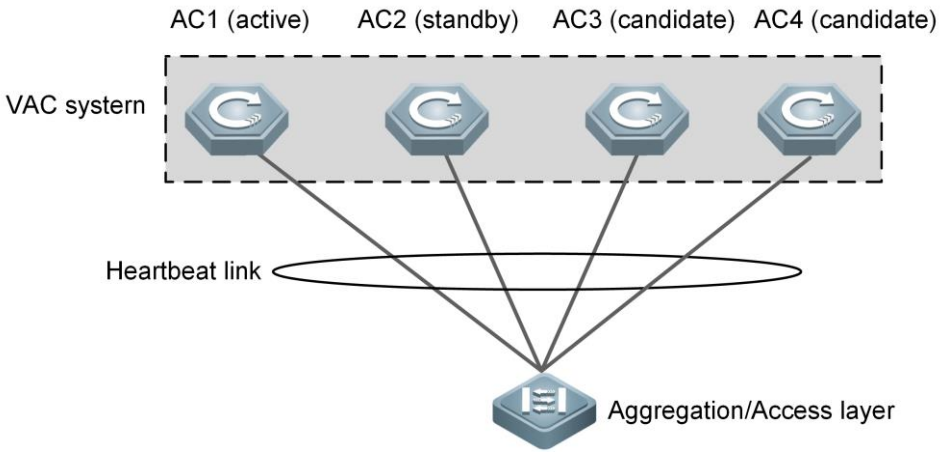
Scenario

When multiple physical devices compose a VAC system, the VAC system can be considered as one logical device. All configurations are managed on the active device.

As shown in Figure 4-3, four devices (numbered 1, 2, 3, and 4 from left to right in sequence) constitute a VAC system. Device 1 is the active device, Device 2 is the standby device, and Device 3 and Device 4 are candidate devices.

- Configurations only need to be performed on the active device for device management.

Figure 4-3



Deployment

- The active device is responsible for controlling the VAC system. It runs management plane and control plane protocols and participates in data forwarding.
- The standby device is responsible for running control plane protocols, participating in data forwarding, and taking over the work of the active device when the active device malfunctions.
- Candidate devices are responsible for running control plane protocols and participating in data forwarding. When the standby device malfunctions, a candidate device can take over the work of the standby device and serves as the standby device. A candidate device cannot take over the work of the active device. Therefore, when both the active device and standby device malfunction, the VAC system restarts.
- Control plane protocols back up each other among devices.

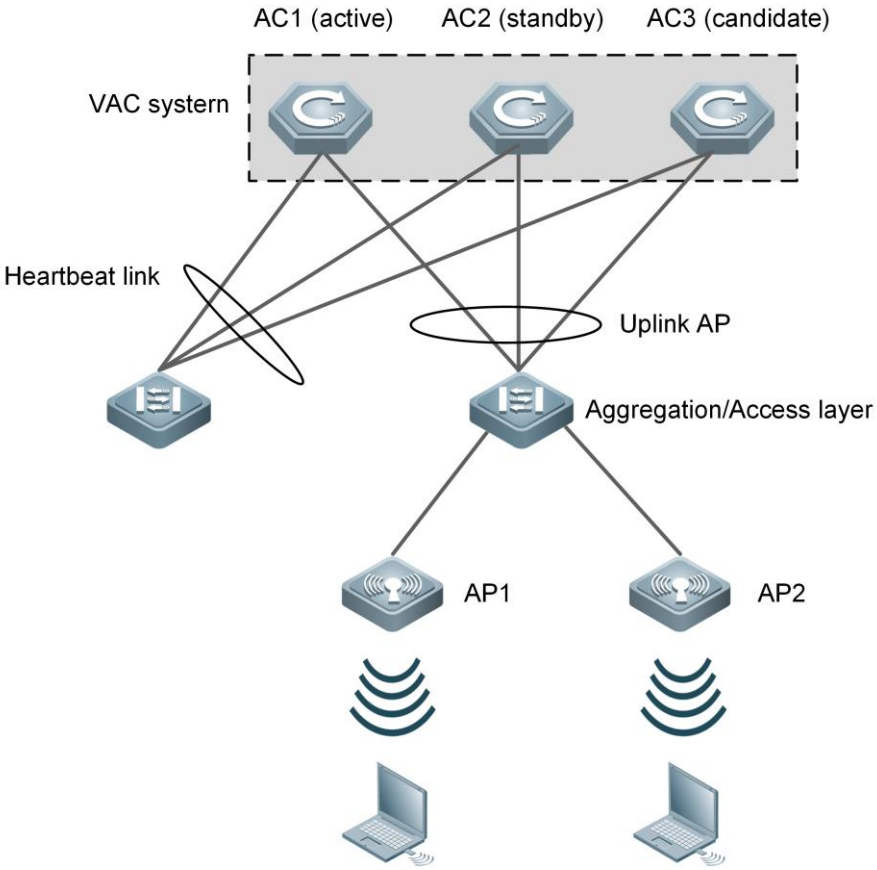
1.2.2 Improving the AC's Reliability

Scenario

As shown in Figure 4-4, when the AC malfunctions, all APs registered with the AC are disconnected. The APs need to rediscover another AC and complete registration so as to reconnect to the network. All devices in a VAC system are considered as one logical device. A device in the VAC system mutually serves as a backup of other devices. When one device malfunctions, services and data can be rapidly migrated to another device.

- Multiple ACs form a VAC system and the ACs provide redundancy. System management is conducted on the active device.
- A heartbeat link is configured between ACs to provide a data channel and exchange data. ACs are connected to the access/aggregation layer through the uplink AP.
- When one device in a VAC system malfunctions, other devices work properly.

Figure 4-4



Deployment

- The active device is responsible for managing the entire VAC system, running management plane and control plane protocols, and participating in data forwarding.
- The standby device is responsible for participating in data forwarding, running control plane protocols, and taking over the work of the active device when the global active device malfunctions.
- The heartbeat link occupies an independent interface on the AC, and services are not configured on the interface.

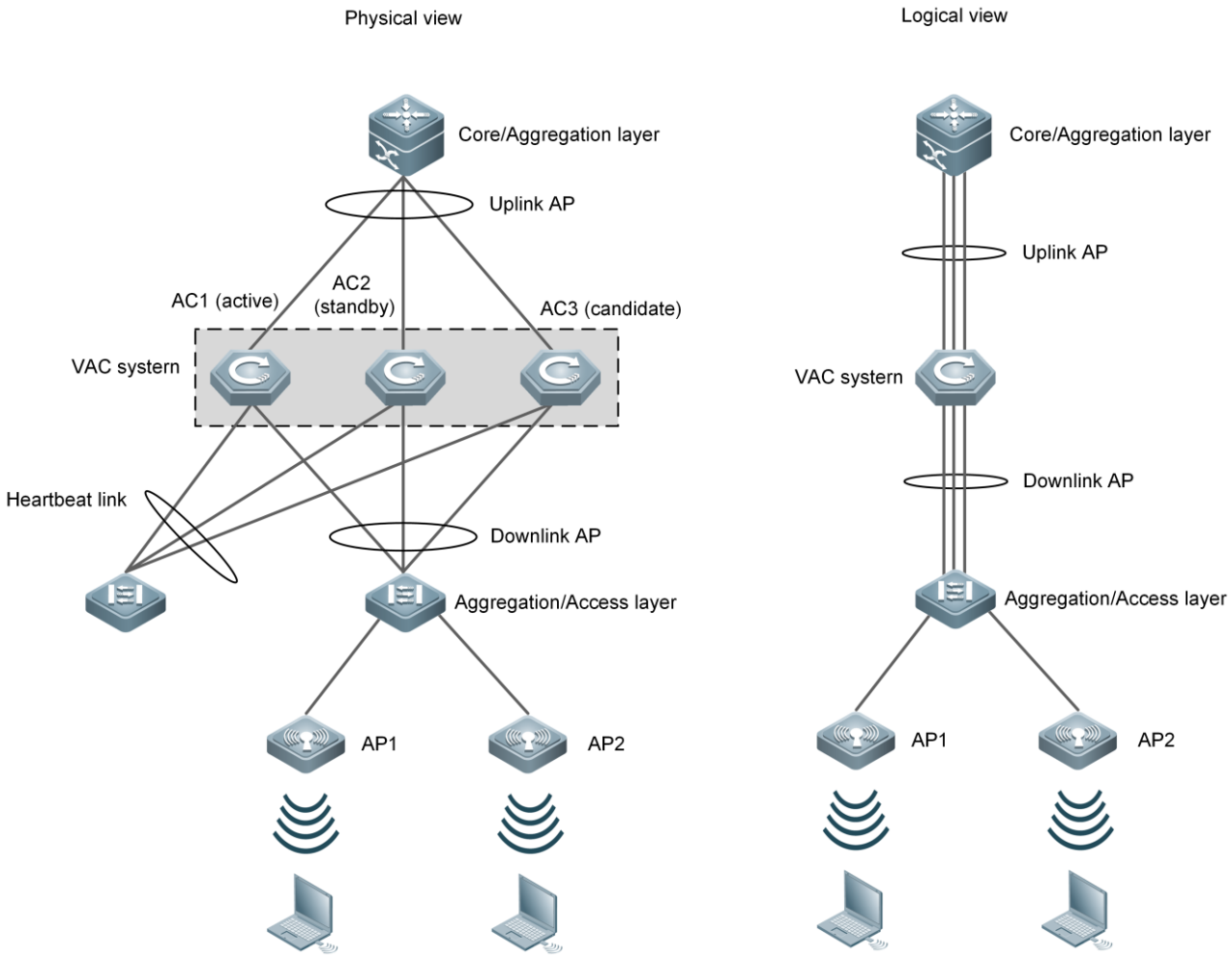
1.3 Features

Basic Concepts

↘ VAC System

A VAC system is a single logical entity composed of multiple independent ACs in the conventional network architecture that are connected through internal heartbeat links. A VAC system can be considered as an independent AC for management.

Figure 4-5 VAC System



Domain ID

A VAC system has a unique domain ID. Only devices with the same domain ID can form a VAC system.

Device ID

Each member device in a VAC system has a unique device ID. This device ID facilitates management on member devices. When adding a device to a VAC system, you need to configure a device ID for the device and ensure that the device ID is unique in the VAC system. If device IDs of member devices conflict in a VAC system, one member device is retained according to the priority.

Device Role

When a VAC system is built, one device is elected as the active device, another device is elected as the standby device according to the election protocol mechanism, and other devices serve as candidate devices. The active device is responsible for controlling the entire VAC system, running management plane protocols of the VAC system, running the control plane protocols of the active device, and participating in data forwarding. The standby device and candidate devices run their respective control plane protocols and participate in data forwarding. When the active device fails, the standby device serves as the active device to manage the VAC system.

The active device of a VAC system is elected as follows:

1 The rules for active device election are as follows (if the active device cannot be elected according to the previous rule, the next rule is used):

2 The current running device is elected as the active device preferentially (no device is the active device during startup).

3 A member device with the highest priority is elected as the active device.

4 A member device with a smaller device ID is elected as the active device.

5 A member device with a smaller MAC address is elected as the active device.

6 The VAC system allows a device to be added in hot mode. The system does not perform an active/standby switchover even if a device that joins the VAC system in hot mode has a higher priority than the active device in the VAC system.

7 The startup sequence of member devices may affect election of the active device. Some member devices may not join the VAC system in a timely manner due to slow startup (the VAC system directly conducts convergence if it does not discover a neighbor within 5 minutes). In this case, the member device will join the VAC system in hot mode. Even if its priority is higher than the running active device in the VAC system, the system does not perform an active/standby switchover.

Overview

Feature	Description
Heartbeat Link	Describes features of the heartbeat link of the VAC system.
Topology	Describes the topology of the VAC system.
Dual-Active Detection	Prevents dual active devices in the same VAC system.
Traffic Forwarding	An AP binds multiple physical connections to form a logical connection.
System Management	Manages devices in the VAC system.
Standby Device Preemption	The VAC system supports the standby device preemption function. If a new device that joins the VAC system has a higher priority than the existing standby device in the VAC system, the new device will preempt the standby device role.

1.3.2 Heartbeat Link

Working Principle

↘ Heartbeat Link

The active and standby devices in a VAC system are network entities and need to transmit management information to each other. Heartbeat links are used for transmitting management information (including role election and configuration backup information) and data streams between devices in the VAC system. You can configure one or more heartbeat links between two member devices of a VAC system. Two heartbeat links are recommended for scenarios demanding high reliability.

After the VAC system is established, if one heartbeat link fails, the VAC system automatically adjusts the configuration so that the backup traffic is not transmitted through the failed link.

If all heartbeat links are disconnected, the topology of the VAC system is split, and the standby device automatically becomes the active device. The configurations of the two devices are the same, which will trigger dual-active detection. One of the two active devices will enter the recovery state and the service interface on the device is disabled, preventing the impact on services on the user network.

If the active device malfunctions, the standby device can detect the fault of the active device through the heartbeat link, automatically becomes the active device, and takes over services.

Heartbeat links can be directly connected or connected through a Layer 2 switch.

Heartbeat Link Traffic

Data streams transmitted by heartbeat links between devices are classified into the following:

- Data streams flooded in a VLAN
- Data streams to be forwarded between devices, which need to be transmitted through heartbeat links

In addition, heartbeat links also transmit internal management packets of the VAC system, for example, hot standby control plane protocol information, and packets that carry the configuration to be delivered from the active device to other member devices.

1.3.3 Topology

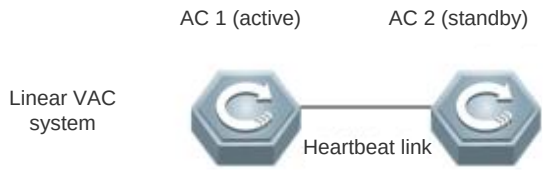
The VAC system supports the linear and star topologies. Devices are connected through a heartbeat link, which can be considered as a line and the topology is called linear topology. Multiple ACs are connected through a Layer 2 switch and the topology is called star topology.

Working Principle

Topology

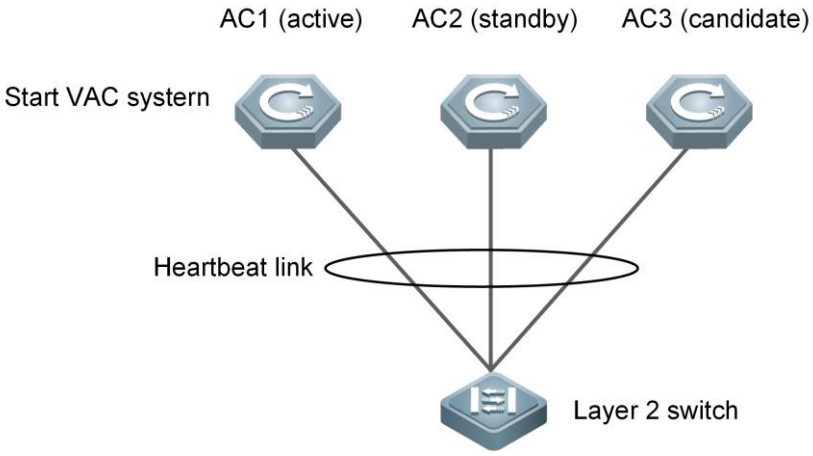
In the linear topology, ACs are directly connected through a heartbeat link. A linear VAC system can be composed of only two devices. A VAC system consisting of three or more devices must use the star topology.

Figure 4-6 Linear Topology



As shown in Figure 4-7, ACs can be connected through a Layer 2 switch to form a star topology. This topology reduces the number of interfaces occupied by heartbeat links.

Figure 4-7 Star Topology



Topology Election

Before a VAC system is established, member devices discover their neighbors through a topology discovery protocol, to determine the devices that constitute the VAC system, so as to determine the scope of the management domain. Then, one active device is elected to manage the VAC system and one standby device is elected as the backup of the active device. At this point, the topology of the VAC system is converged. Topology discovery protocol information is transmitted through heartbeat links. The startup time of different devices is different, so the first convergence time of the topology is different.

The rules for active device election are as follows (the first rule is used for active device election; if the active device is not elected according to the first rule, the system goes on with the next rule):

- The device whose topology is converged is elected as the active device preferentially.
- The device with a higher priority is elected as the active device.
- If the active device cannot be determined according to the preceding rules, the device with a smaller device ID is elected as the active device.
- If the active device cannot be determined according to the preceding rules, the device with a smaller MAC address is elected as the active device.

The rules for standby device election are as follows (the first rule is used for standby device election; if the standby device is not elected according to the first rule, the system goes on with the next rule):

- Compare with the ID of the switch connected to the active device. The device that does not reside on the same switch as the active device is preferentially elected as the standby device. If multiple devices are not on the same switch as the active device, the next rule is used.
- The device with a higher priority is elected as the standby device.
- If the standby device cannot be determined according to the preceding rules, the device with a smaller device ID is elected as the standby device.
- If the standby device cannot be determined according to the preceding rules, the device with a smaller MAC address is elected as the standby device.

Topology Combination

When two or more ACs with the same domain ID are connected through heartbeat links, topologies will be combined. One device will restart and join the VAC system in hot mode during topology combination.

The topology combination rules are as follows (the first rule is used; if the optimal topology is not selected according to the first rule, the system goes on with the next rule):

- The user configuration is prior to other configuration. The device configured with the highest priority will prevail.
- If the active device cannot be determined according to the preceding rule, the device with a smaller device ID will prevail.
- If the active device cannot be determined according to the preceding rule, the device with a smaller MAC address will prevail.

Heartbeat Link for a Layer 2 Network

- In a star topology, heartbeat links are not directly connected, and a Layer 2 switch is used to forward management packets carried over the heartbeat links. In a VAC system, management packets of devices cannot be forwarded across VLANs. Therefore, on the Layer 2 switch, interfaces of the heartbeat link of multiple ACs must be configured to be in the same VLAN. You are advised to configure a separate VLAN for interfaces of the heartbeat link on the switch, so as to prevent other interfaces in the same VLAN from interfering with management packet forwarding.

1.3.4 Dual-Active Detection

Working Principle

When the heartbeat link is disconnected, the standby device becomes the active device. If the original active device is still running, there are two active devices. In this case, IP address conflicts and other problems will be incurred on the LAN because they have the same configuration. In this case, the VAC system must detect whether dual active devices coexist, and take measures.

Rules of Dual-Active Detection

1 The device with a higher priority is preferred.

2 If the active device cannot be determined according to the preceding rule, the device with a smaller device ID is preferred.

3 If the active device cannot be determined according to the preceding rules, the device with a smaller MAC address is preferred.

4 If the active device cannot be determined according to the preceding rules, the device with longer startup time will be retained.

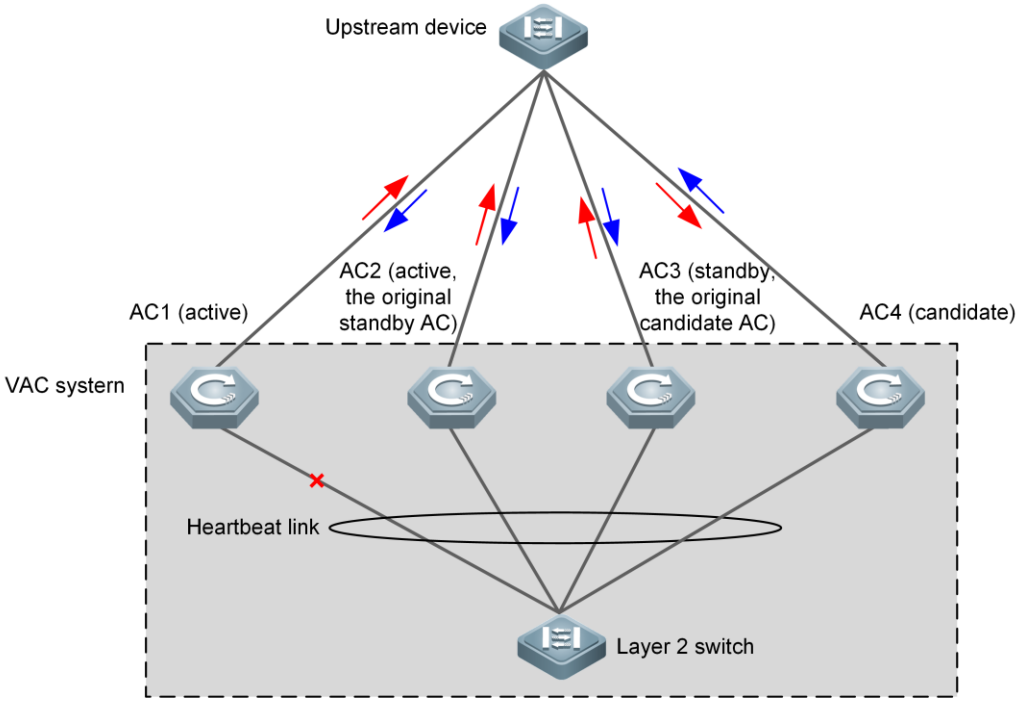
⚠ If dual-active detection is not configured, the network will be interrupted after the topology is split.

Dual-Active Detection Mode

The VAC system supports the dual-active detection mechanism by using an aggregate interface. Figure 4-8 shows the connection topology. Both the VAC system and upstream device need to support the dual-active detection function of the aggregate interface. When a heartbeat link is disconnected and dual active devices coexist, both active devices send detection packets to each member interface of the aggregate interface. The detection packets are transferred by the upstream device to the other active device. As shown in Figure 4-8, the aggregate interface contains four member

interfaces, each of which is connected to one device in the VAC system. When the topology is split, the four member interfaces send and receive detection packets to detect coexistence of dual active devices. Then the VAC system where one active device resides will be shut down to enter the recovery state, so as to prevent network exceptions.

Figure 4-8 Dual-Active Detection



1.3.5 Traffic Forwarding

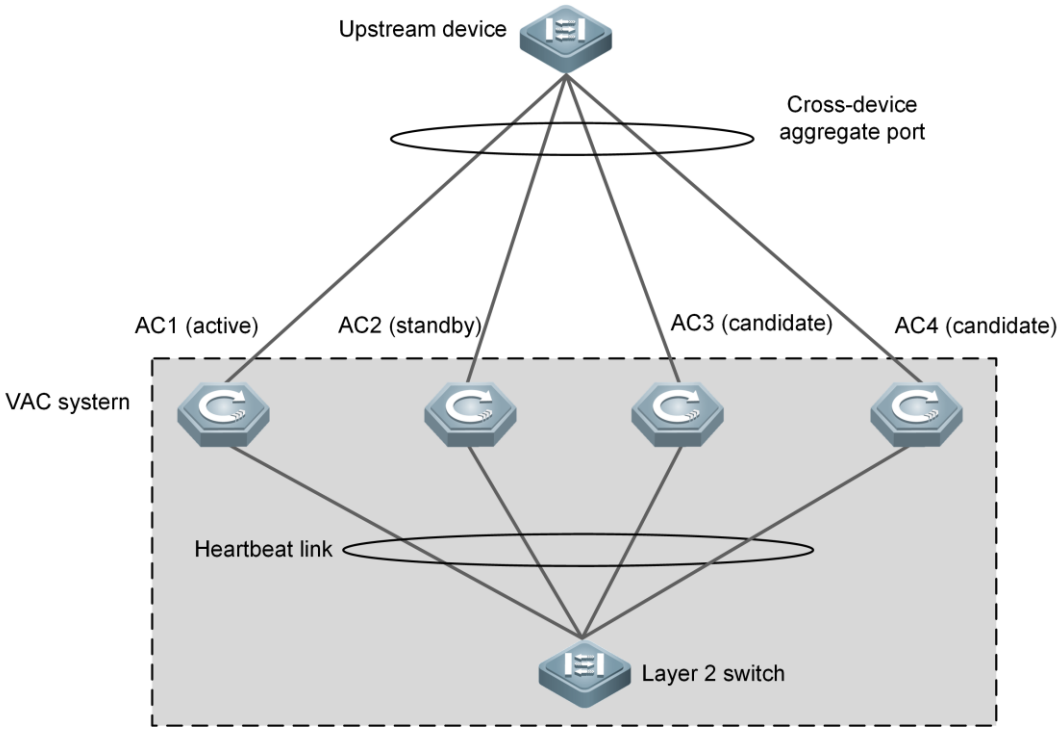
Working Principle

Cross-device Aggregate Interface Group

An aggregate interface is formed by binding multiple physical interfaces. The VAC system supports the aggregate interface across member devices.

As shown in Figure 4-9, four ACs compose the VAC system and the upstream device is connected to the VAC system as an aggregate interface. For the upstream device, the aggregate interface is equivalent to a common aggregate interface group.

Figure 4-9 Cross-device Aggregate Interface



Troubleshooting

It is recommended that a peripheral device be physically connected to each device in the VAC system when a cross-device aggregate interface is configured for the VAC system. This can ensure the bandwidth of heartbeat links (the cross-device aggregate interface preferentially selects the member interface as the egress, to prevent transmission of unnecessary traffic through heartbeat links), and improve network reliability (if a device malfunctions, member interfaces on normal devices can work properly).

The possible cross-device aggregate interface failures and incurred impact are described as follows:

- A single link fails.

If a single link of the cross-device aggregate interface fails but other links function properly, the cross-device aggregate interface redistributes traffic among the remaining normal links.

- On the active device, links of all member interfaces of the cross-device aggregate interface fail.

If links of all member interfaces of the cross-device aggregate interface on the active device fail, only member interfaces on other member devices continue to work properly. If the outbound interface of data streams from the aggregate interface to the VAC system is located on the active device, the VAC system forwards the data streams to the outbound interface through heartbeat links.

Control plane protocols run on each device. Therefore, protocol packets transmitted to the VAC system are forwarded to each device for protocol computing through the heartbeat links.

- All links to other member devices fail.

If all links between the cross-device aggregate interface and a member device fail, only member interfaces on other member devices continue to work properly. If the outbound interface of data streams from the aggregate interface to the VAC system is located on the member device, the VAC system forwards the data streams to the outbound interface through heartbeat links.

- All links fail.

If all links of the cross-device aggregate interface fail, the cross-device aggregate interface changes the interface status to Link-Down, just as a common aggregate interface does.

- The active device malfunctions.

If the active device malfunctions, hot standby switching is triggered and the original standby device becomes the active device. Meanwhile, member interfaces on other member devices continue to work properly. When the peer device in the VAC system that is connected to the cross-device aggregate interface detects a link failure, it adjusts the load balancing algorithm to distribute data streams to normal links.

- A member device malfunctions.

If a member device malfunctions, the member link of the aggregate interface connected to the member device is disconnected but other member links still work properly. When the peer device in the VAC system that is connected to the cross-device aggregate interface detects a link failure, it adjusts the traffic balancing algorithm to distribute data streams to normal links.

Traffic Balancing

There may multiple traffic egresses in a VAC system. The aggregate interface and Equal-cost Multi-path Routing (ECMP) have their own traffic balancing algorithms, for example, traffic is balanced based on the source and destination MAC addresses. For details, see the AP and ECMP configuration manuals. In this configuration manual, packets received by the local device can be configured to be preferentially forwarded by the local device. In this way, packets can be forwarded to other devices not through heartbeat links.

1.3.6 System Management

Working Principle

Console Access

The console of the active device in the VAC system is also used to manage multiple devices in the system. On the console of the standby device, CLI commands cannot be executed, but the protocol status of the standby device can be queried and protocol entries can be cleared. On the active device, services can be configured for member devices uniformly. You can also log in to the console of the active device through the serial port of the standby device. In addition, you can redirect to the console of a device by running the **session** command.

Interface Naming

In a running VAC system, multiple devices may use the same interface ID. Therefore, the device ID is introduced to interface naming.

For example, gigabitEthernet 1/0/1 indicates GE interface 1 in slot 0 of the device with the ID of 1; gigabitEthernet 2/0/2 indicates GE interface 2 in slot 0 of the device with the ID of 2.

System Upgrade

In most cases, the main program versions of member devices in the VAC system need to be consistent. However, there are numerous member devices and the upgrade is time-consuming, laborsome, and error-prone if the devices are upgraded in standalone mode. You can complete the system upgrade by using the following two methods:

- When the VAC system is established, the system automatically checks the main program version of all member devices. If inconsistency is identified, the system synchronizes the main program of the active device to all member devices.
- After the VAC system is established, the system automatically synchronizes the file downloaded over TFTP to all member devices.

System Logs

System logs can be generated on all member interfaces of the VAC system. System logs generated by the active device are directly generated on the console of the active device, and the format of generated system logs is identical to that of system logs generated in standalone mode. System logs generated by other member devices are also generated on the console of the active device, but the format of generated system logs is different from that of system logs generated in standalone mode because the device ID is generated.

For example, the system log generated in standalone mode is "%DEVICE-6-INSTALL: Install chassis WS5708 on device 1." The system log generated by the member device with the device ID of 2 should be "%DEVICE-6-INSTALL: (2*)Install chassis WS5708 on device 1.

1.3.7 Standby Device Preemption

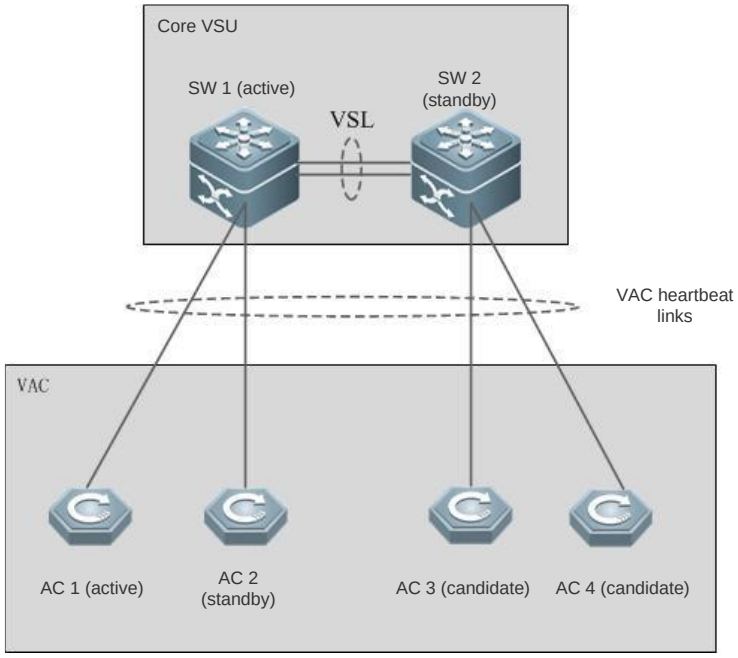
Working Principle

Standby Device Preemption

The VAC system supports the standby device preemption function. If a new device that joins the VAC system has a higher priority than the existing standby device in the VAC system, the new device will preempt the standby device role.

As shown in Figure 4-10, SW 1 and SW 2 compose a VSU, and ACs 1-4 are connected to the two switches and form a VAC system. The active and standby devices of the VAC system connect to SW 1 and the candidate ACs are connected to SW 2.

Figure 4-10 VSU+VAC



When the core VSU malfunctions, SW 1 is reset, which will result in splitting of the VAC system. AC 1 and AC 2 cannot communicate with external devices, resulting in AP disconnection. AC 3 and AC 4 have no standby devices and will be reset upon splitting. Therefore, when one switch in the VSU malfunctions, all ACs will become unavailable.

The standby device preemption function can solve this problem. ACs with high priority are connected to different switches. In this way, the active and standby devices in the VAC system are connected to different switches. When the VSU malfunctions, one switch is reset, and ACs connected to the other switch can take over services properly, preventing unavailability of all ACs.

1.4 Configuration

Configuration		Description and Command	
Configuring Basic VAC System Parameters in Standalone Mode		(Mandatory) It is used to configure VAC system parameters in standalone mode.	
		virtual-ac domain	Configures the domain ID.
		device	Configures the device ID in the VAC system.
		device priority	Configures the device priority.
		device connect_switch	Configures the ID of the switch connected to the AC.
		vac-port	Enters the heartbeat interface configuration mode.
		port-member interface	Adds a common interface to the heartbeat link interface pool.
		device convert mode	Switches the device from the standalone mode to the VAC mode.
Configuring VAC System Parameters in VAC Mode	Configuring VAC System Attributes	(Optional) It is used to configure device attributes in VAC mode.	
		device domain	Changes the domain ID of the device.
		device renumber	Changes the device ID.
		device description	Configures the device alias.
	Configuring Heartbeat Links	(Optional) It is used to configure heartbeat links.	
		vac-port	Enters the heartbeat interface configuration mode.
		port-member interface	Adds a common interface to the heartbeat link interface pool.
	Configuring Dual-active Detection	(Mandatory) It is used to configure the dual-active detection function.	
		dual-active detection	Configures the dual-active detection function.
		dual-active bfd interface	Configures BFD for an interface.
		dual-active interface	Configures the aggregate interface as the dual-active detection interface.

Configuration		Description and Command	
		dual-active exclude interface	Configures an excluded interface.
	Configuring Standby Device Preemption	**slave preemtive enable**	Configures standby device preemption.

1.4.1 Configuring Basic VAC System Parameters in Standalone Mode

Configuration Effect

Configure VAC-relevant basic parameters, so as to build a VAC system.

Configuration Step

Configuring VAC System Attributes

- Configure the same domain ID for multiple devices that need to compose a VAC system and ensure that the domain ID is unique on the LAN. In addition, configure a device ID for each device in the VAC system.
- (Mandatory) Run the **vitrual-ac domain** *domain_id* command to configure the domain ID.
- Run the **device** device_*id* command to configure a device ID for each device in the VAC system. This command is mandatory. When devices share the same priority, the device with a smaller device ID is preferentially elected as the primary device.
- (Optional) Run the **device** *device_id* **priority** *priority_num* command to configure the device priority. The value range is from 1 to 255. A larger value indicates a higher priority.

Command	**virtual-ac domain** *number*
Parameter Description	*number*: Indicates the virtual domain ID of a VAC system.
Defaults	The default domain ID is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	Only devices with the same domain ID can constitute a VAC system. The domain ID must be unique on a LAN.

Command	**device** *device_id*
Parameter Description	*device_id*: Indicates the ID of a device in the VAC system. The value varies with the product model.
Defaults	The default device ID is 1.
Command Mode	config-vac-domain configuration mode
Usage Guide	The device with a smaller device ID is elected as the active device if two devices are both active devices or if the two devices share the same priority and are just started with their roles not determined. This command can be used to change the ID of an AC only in standalone mode. The changed device ID takes effect only after device restart.

Command	**device** *device_id* **connect_switch** *switch_id*
Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. *switch_id*: Indicates the device ID. The value range is from 1 to 255.
Defaults	The default switch ID is 1.
Command Mode	config-vac-domain configuration mode
Usage Guide	This command is used to set the ID of the connected switch. If the specified switch ID is different from that of the active device, the device will be preferentially elected as the standby device. This command is available in both standalone and VAC modes. The changed priority takes effect only after the device restart. In VAC mode, *device_id* indicates the ID of the running device. If the device ID does not exist, the priority does not take effect.

Command	**device** *device_id* **priority** *priority_num*
Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. priority_num: Indicates the device priority. The value range is from 1 to 255.
Defaults	The default priority is 100.
Configuration Mode	config-vac-domain configuration mode
Usage Guide	A larger value indicates a higher priority. The device with a higher priority is elected as the active device. This command is available in both standalone and VAC modes. The changed priority takes effect only after device restart. In VAC mode, *device_id* indicates the ID of the running device. If the device ID does not exist, the configuration does not take effect.

The priority command is used to change the priority only and will not change the device ID. Therefore, a correct device ID must be entered during configuration. For example, the configured device ID is 1. If you enter the **device 2 priority 100** command, the priority does not take effect.

Command	**device convert mode** { **virtual** | **standalone** } [*device_id*]
Parameter Description	**virtual**: Switches to the VAC mode. **standalone**: Switches to the standalone mode. *device_id*: Indicates the ID of the device.
Defaults	The standalone mode is the default mode.
Command Mode	Privileged EXEC mode
Usage Guide	After the **device convert mode virtual** command is run, the software automatically backs up the global configuration file in standalone mode as **standalone.text**, deletes global configuration file **config.text**, and then asks you whether to use **config_vac.text** to replace **config.text**. If the user chooses **yes**, **config_vac.text** replaces **config.text**. Otherwise, the global configuration file **config.text** is not restored, and the related configuration of the VAC system is written to the configuration file **config_vac.dat** before the device is reloaded. After the **device convert mode standalone** command is run, the software automatically backs up

	the global configuration file in standalone mode as **virtuac-ac.text**, deletes global configuration file **config.text**, and then asks the user if **standalone.text** is allowed to replace **config.text**. If the user chooses **yes**, **standalone.text** replaces **config.text**. Otherwise, the global configuration file **config.text** is not restored, and the related configuration of the VAC system is written to the configuration file **config_vac.dat** before the device is reloaded. This command can be run in both standalone and VAC modes. In standalone mode, services are switched to the device itself. In VAC mode, when *device_id* is specified, services are switched to the device specified by *device_id*. When *device_id* is not specified, services are switched to the active device. It is recommended that services be switched to the standby device and active device in sequence.

Configuring Heartbeat Links

- Multiple interfaces need to be configured as heartbeat detection interfaces so as to establish a VAC system.
- (Mandatory) Run the **vac-port** command to enter the heartbeat interface configuration mode.
- (Mandatory) Run the **port-member interface** *interface-name* [**copper** | **fiber**] command to add heartbeat interfaces.
- When the device enters the heartbeat interface configuration mode, you can configure or delete heartbeat interfaces.

Command	**vac-port**
Parameter Description	N/A
Defaults	N/A
Command Mode	Configuration mode
Usage Guide	This command is available in both standalone and VAC modes.

Command	**port-member interface** *interface-name* [**copper** | **fiber**]
Parameter Description	*interface-name*: Indicates a 2-dimensional interface name, for example, Tengigabitethernet 1/1 and Tengigabitethernet 1/3. **copper**: Indicates the electrical interface. **fiber**: Indicates the optical interface.
Defaults	*N/A*
Command Mode	config-vac-port configuration mode
Usage Guide	This command is used to add member interfaces for heartbeat links. *interface-name* indicates the 2-dimensional interface name in standalone mode. It can be a 10GE or GE interface. The GE interface can be a combo interface. If the medium type is not specified, the GE interface is a GE electrical interface by default. The optical/electrical attribute must be specified for the combo interface. This command is available in both VAC and standalone modes.

⚠ In standalone mode, the heartbeat interface configuration does not take effect immediately. It can take effect only after the device switches to VAC mode and is restarted.

Verification

Run the **show virtual-ac config** [*device_id*] command to display the VAC system configuration on the device in standalone mode.

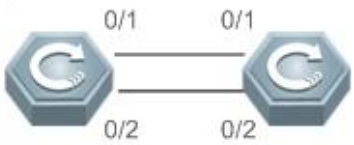
Command	**show virtual-ac config** [*device_id*]
Parameter Description	*device_id*: Indicates the device ID. If this parameter is specified, only the VAC system configuration of a specific device is displayed.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to display the VAC system configuration in standalone mode or VAC mode.

The VAC-relevant configuration is applicable to a single physical device, and the configuration is stored in the special configuration file **config_vac.dat**. Therefore, the **show running config** command cannot display VAC system configuration. Only the **show virtual-ac** config command can be executed to display the configuration of the VAC system.

In standalone mode, the running information of the VAC system is empty. When the **show virtual-ac** command is executed, a prompt is displayed, indicating that the standalone mode is used and there is no VAC system running information.

Configuration Example

Configuring Basic VAC System Parameters in Standalone Mode

Scenario **Figure 4-11**	AC 1 Device ID: 1 Priority: 200 AC 2 Device ID: 2 Priority: 100 VAC system  Heartbeat link AC 1 and AC 2 form a VAC system. The domain ID is 100. The device ID and priority of AC 1 are 1 and 200 respectively. Interfaces 0/1 and 0/2 are heartbeat interfaces. The device ID and priority of AC 2 are 2 and 100 respectively. Interfaces 0/1 and 0/2 are heartbeat interfaces.
Configuration Steps	1. Complete the following configuration on AC 1: ● Configure the VAC system attributes and heartbeat interfaces. ● Switch the device from the standalone mode to VAC mode. 2. Complete the following configuration on AC 2: ● Configure the VAC system attributes and heartbeat interfaces. ● Switch the device from the standalone mode to VAC mode.

Device-1	`Hostname# configure terminal`
	`Hostname(config)# virtual-ac domain 100`
	`Hostname(config-vac-domain)#device 1`
	`Hostname(config-vac-domain)#device 1 priority 200`
	`Hostname(config-vac-domain))#exit`
	`Hostname(config)# vac-port`

	Hostname(config-vac-port)#port-member interface GigabitEthernet 0/1 Hostname(config-vac-port)#port-member interface GigabitEthernet 0/2 Hostname(config)#exit
Device-2	Hostname# configure terminal Hostname(config)# virtual-ac domain 100 Hostname(config-vac-domain)# device 2 Hostname(config-vac-domain)# device 2 priority 200 Hostname(config-vac-domain))#exit Hostname(config)# vac-port Hostname(config-vac-port)#port-member interface GigabitEthernet 0/1 Hostname(config-vac-port)#port-member interface GigabitEthernet 0/2 Hostname(config-vac-port)#exit
Verification	● Run the **show virtual-ac config** command to display VAC system attributes of AC 1 and AC 2.
Device-1	Hostname#show virtual-ac config device_id: 1 (mac: 1414.4b5b.54f8) ! virtual-ac domain 100 ! device 1 device 1 priority 200 ! device convert mode virtual ! port-member interface GigabitEthernet 0/1 ! port-member interface GigabitEthernet 0/2 !
Device-2	Hostname#show virtual-ac config device_id: 2 (mac: 00d0.f822.33c0) ! virtual-ac domain 100 ! device 2 device 2 priority 100 ! device convert mode virtual ! port-member interface GigabitEthernet 0/1 ! port-member interface GigabitEthernet 0/2 !

1.4.2 Configuring VAC System Parameters in VAC Mode

1.4.2.1 Configuring VAC System Attributes

Configuration Effect

When devices constitute a VAC system or the VAC system is running, if some parameters need to be modified, you can log in to the console of the active device of the VAC system to modify parameters. You cannot enter the global configuration mode from the console of the standby device.

Notes

Configuration commands take effect only after the switch is restarted except the **device** *device_id* **description** *device*1 command, which takes effect immediately.

Configuration Step

↘ Entering the Domain Configuration Mode

- Optional.
- Run this command in VAC mode to enter the domain configuration mode. Only ACs with the same domain ID can form a VAC system. In VAC mode, you can change or configure the domain ID, device priority, and switch ID only after entering the domain configuration mode.

Command	**virtual-ac domain** *domain_id*
Parameter Description	*domain_id*: Indicates the virtual domain ID of the VAC system.
Defaults	The default domain ID is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	Only two devices with the same domain ID can constitute a virtual device. The domain ID must be unique on a LAN.

↘ Changing the Domain ID of the VAC System

- Optional.
- To change the domain ID of a device, run this command on the console of the active device in the VAC system.

Command	**device** *device_id* **domain** *new_domain_id*
Parameter Description	*device_id*: Indicates the ID of the running device in VAC mode. The value varies with the product model. *new_domain_id*: Indicates the changed domain ID. The value ranges from 1 to 255.
Defaults	The default value is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	This command is available only in VAC mode and the configuration takes effect only after device restart.

↘ Changing the Device ID

- Optional.
- To change the device ID of a device, run this command on the console of the active device in the VAC system.

Command	**device** *device_id* **renumber** *new_device_id*
Parameter Description	*device_id*: Indicates the ID of the running device in VAC mode. The value varies with the product model. *new_device_id*: Indicates the changed device ID.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	This command is available only in VAC mode and the configuration takes effect only after device restart. This command is used only to change the device ID and will not change configuration related to the device ID. In VAC mode, many configurations are related to the device ID, for example, the type of the device installed by running the **install** command, configuration commands in various interface modes, and configuration commands using the interface ID. After the device ID is changed, check whether all configuration is correct.

Changing the Device Priority

- Optional.
- To change the priority of a device, run this command on the console of the active device in the VAC system.
- A larger value indicates a higher priority. The device with a higher priority is elected as the active device.

Command	**device** *device_id* **priority** *priority_num*
Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. *priority_num*: Indicates the device priority. The value ranges from 1 to 255.
Defaults	The default priority is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	A larger value indicates a higher priority. The device with a higher priority is elected as the active device. This command is available in both standalone and VAC modes. The changed priority takes effect only after the device restart. This command will not change the device ID. In standalone mode, if *device_id* is set to 1 but the **device 2 priority 200** command is executed, the command does not take effect unless *device_id* is changed to 2 and the command is executed again. In VAC mode, *device_id* indicates the ID of the running device. If the device ID does not exist, the priority does not take effect.

Configuring the Device Alias

- Optional.
- To configure an alias for a device, run this command on the console of the active device in the VAC system.
- Run the **device** device_*id* **description** *device1* command to configure the device alias. The device alias can contain a maximum of 32 characters.

Command	**device device**_*id* **description** *dev-name*

Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. *dev_name*: Indicates the device name.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	This command is available in both standalone and VAC modes. The configuration takes effect immediately in VAC mode.

Configuring the ID of the Switch Connected to a Device

- Optional.
- To configure the ID of the switch connected to a device, run this command on the console of the active device in the VAC system.
- Run the **device** *device_id* **connect_switch** *switch_id* command to configure the ID of the switch connected to a device. The value range is from 1 to 255.

Command	**device** *device_id* **connect_switch** *switch_id*
Parameter Description	*device_id*: Indicates the ID of the device with the priority to be configured. switch_id: Indicates the ID of the switch connected to the device.
Defaults	N/A
Command Mode	config-vac-domain configuration mode
Usage Guide	This command is used to set the ID of the connected switch. If the specified switch ID is different from that of the active device, the device will be preferentially elected as the standby device. This command is available in both standalone and VAC modes. The changed switch ID takes effect only after device restart. In VAC mode, *device_id* indicates the ID of the running device. If the device ID does not exist, the configuration does not take effect.

Saving the Configuration File

Run the **exit** command to exit the VAC configuration mode and run the **write** command to save the configuration to the **config_vac.dat** file.

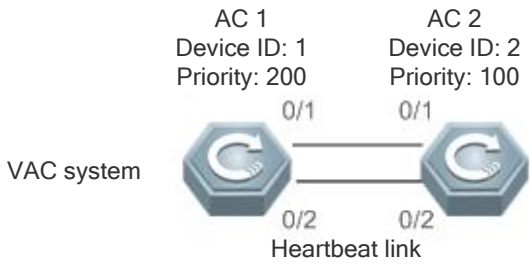
Verification

Run the **show virtual-ac** [**topology | config**] command to display information about the running VAC system, topology, or VAC system parameters.

Command	**show virtual-ac** [**topology	config**]
Parameter Description	Topology: Indicates topology information, that is, VAC system configuration.
Command Mode	Privileged EXEC mode
Usage Guide	This command is used to display the domain ID and the device ID, status, and role of each device.

Configuration Example

Configuring VAC System Attributes

Scenario **Figure 4-12**	 AC 1 and AC 2 form a VAC system. Change the device ID of AC 2 to 3 and priority to 150. Assume that AC 1 is the active device. Complete the configuration on the active device.
Configuration Steps	● Modify the configuration of AC 2.

AC 2	`Hostname#config`
	`Hostname(config)# virtual-ac domain 100`
	`Hostname(config-vac-domain)# device 2 renumber 3`
	`Hostname(config-vac-domain)# device 2 priority 150`
	`Hostname(config-vac-domain)# device 2 description AC3`

Verification	● Run the **show virtual-ac config** command to display the configuration.

AC 1	`Hostname#show virtual-ac config`
	`device_id: 1 (mac: 0x1201aeda0M)`
	`!`
	`virtual-ac domain 100`
	`!`
	`device 1`
	`device 1 priority 100`
	`!`
	`device convert mode virtual`
	`!`
	`port-member interface GigabitEthernet 0/1`
	`!`
	`port-member interface GigabitEthernet 0/2`
	`!`

	`device_id: 3 (mac: 0x1201aeda0E)`
	`!`
	`virtual-ac domain 100`
	`!`
	`device 3`
	`device 3 priority 150`
	`!`
	`device convert mode virtual`
	`!`
	`port-member interface GigabitEthernet 1/1`
	`!`

	port-member interface GigabitEthernet 1/2 ! device 3 description AC3 !

1.4.2.2 Configuring Heartbeat Links

Configuration Effect

When devices constitute a VAC system or the VAC system is running, if common interfaces need to be switched to heartbeat interfaces and vice versa, you can log in to the console of the active device in the VAC system for modification. You cannot enter the global configuration mode from the console of the standby device.

Notes

You can log in to the console of the VAC system through a serial port or in telnet mode, to add or delete heartbeat interfaces.

Configuration Step

Entering the Heartbeat Port Mode

- (Optional) Run the **vac-port** command to enter the heartbeat interface configuration mode.
- When the device enters the heartbeat interface configuration mode, you can add or delete heartbeat interfaces.

Command	**vac-port**
Parameter Description	N/A
Defaults	N/A
Command Mode	Configuration mode
Usage Guide	This command is available in both standalone and VAC modes.

Configuring Heartbeat Interfaces

- (Optional) Run the **port-member interface** *interface-name* [**copper** | **fiber**] command to configure a heartbeat interface.
- Run the **port-member interface** command to add or delete a heartbeat interface.

Command	**port-member interface** *interface-name* [**copper | fiber**]
Parameter Description	*interface-name*: Indicates a 2-dimensional interface name, for example, GigabitEthernet 0/1 and GigabitEthernet 0/3. **copper**: Indicates the electrical interface. **fiber**: Indicates the optical interface.
Defaults	N/A
Command Mode	config-vac-port configuration mode
Usage Guide	This command is available in both VAC and standalone modes. In standalone mode, the command configuration needs to be saved and the device where the heartbeat member interface resides

	needs to be restarted for the configuration to take effect. In VAC mode, the command configuration takes effect immediately.

The configured heartbeat member links take effect immediately during the running of the VAC system. Heartbeat interfaces need to be configured on all devices.

To prevent loops from being instantaneously generated when a heartbeat interface is switched to a common interface, the system automatically sets the interface to be in shutdown state when this command is executed. You can reconnect the link and run the **no shutdown** command to enable the interface.

If the VAC system topology is split because a heartbeat interface is switched to a common interface, the heartbeat interface cannot be deleted. You can disconnect the physical interface and then delete the heartbeat interface.

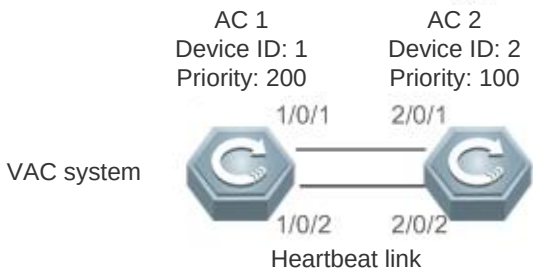
Verification

Run the **show virtual-ac link** [**port**] command to display the running status of the heartbeat interface.

Command	**show virtual-ac link** [**port**]
Parameter Description	**port**: Displays information about a specific interface.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Configuring Heartbeat Links

Scenario Figure 4-13	
Configuration Steps	● Add interface 1/0/3 as a heartbeat interface and remove the heartbeat interface 0/2.

	`Hostname#config`
	`Hostname(config)# vac-port`
	`Hostname(config-vac-port)# port-member interface Gigabitethernet 1/0/3`
	`Hostname(config-vac-port)# no port-member interface Gigabitethernet 1/0/2`

Verification	● Run the **show virtual-ac config** command to display heartbeat links. Assume that AC 1 is the active device. Run the command on the active device.

	`Hostname#show virtual-ac config`
	`device_id: 1 (mac: 0x1201aeda0M)`
	`!`

	Virtual-ac domain 100 ! device 1 device 1 priority 200 ! device convert mode virtual ! port-member interface Gigabitethernet 0/1 ! port-member interface Gigabitethernet 0/3 !
	device_id: 2 (mac: 0x1201aeda0E) ! virtual-ac domain 100 ! device 2 device 2 priority 100 ! device convert mode virtual ! port-member interface Gigabitethernet 0/1 ! port-member interface Gigabitethernet 0/2 !

1.4.2.3 Configuring Dual-active Detection

Configuration Effect

Configure a detection mechanism to prevent dual-active devices.

Notes

- Dual-active detection can be configured only in VAC mode.
- Dual-active detection is configured in global configuration mode and the dual-active detection configuration takes effect immediately on the active device. Run the **show running-config** command to display the configuration.
- BFD-based dual-active detection configuration cannot be displayed by running related BFD commands but by running the **show virtual-ac dual-active summary** command.

Configuration Step

↘ Configuring BFD-based Dual-active Detection

- In BFD-based dual-active detection, a direct link needs to be established between two devices and the interfaces at both ends of the link must be routed interfaces. The following configuration is required on both devices.
- Enter the interface configuration mode of the detection interface and configure the detection interface as a routed interface.

- Exit the interface configuration mode, and run the **virtual-ac domain** *domain_id* command to enter the config-vac-domain configuration mode.
- In config-vac-domain configuration mode, run the **dual-active detection bfd** command to enable BFD, which is optional.
- In config-vac-domain mode, run the **dual-active bfd interface** *interface-name* command to configure the BFD detection interface, which is optional.
- If no BFD detection interface is available after a BFD detection interface is deleted, BFD detection will be unavailable.

Command	**virtual-ac domain** *domain_id*
Parameter Description	*domain_id*: Indicates the virtual domain ID of the VAC system.
Defaults	The default domain ID is 100.
Command Mode	config-vac-domain configuration mode
Usage Guide	Only two devices with the same domain ID can constitute a virtual device. The domain ID must be unique on a LAN.

Command	**dual-active detection** { **aggregateport	bfd** }
Parameter Description	**aggregateport**: Specifies the aggregate interface-based detection. **bfd**: Indicates BFD detection.
Defaults	The dual-active detection function is disabled.
Command Mode	config-vac-domain configuration mode
Usage Guide	This command can be configured only in VAC mode.

Command	**dual-active bfd interface** *interface-name*
Parameter Description	*interface-name*: Indicates the type and ID of the detection interface.
Defaults	N/A
Command Mode	config-vac-domain configuration mode
Usage Guide	BFD detection interfaces must be routed interface and reside on different devices.

BFD detection interfaces must be direct routed interfaces and must reside on different devices.

The configured interface type is unlimited. Dual-active detection links are used to transmit only BFD packets, and traffic is light. Therefore, you are advised to configure a 1000M or 100M interface as the dual-active detection interface.

After a Layer 3 routed interface configured for dual-active detection is switched into a Layer 2 switching interface (by running the **switchport** command on the interface), the BFD dual-active detection configuration is automatically cleared.

You are advised to adopt the direct connection for the BFD link to connect only the active and standby devices.

When a dual-active conflict is detected and one VAC system is enabled to enter the recovery state, you can rectify the fault by eliminating the VSL failure but not by directly resetting the VAC system in recovery state. Otherwise, a dual-active device conflict will be incurred on a network.

Configuring Aggregate Interface-based Dual-active Detection

- To configure aggregate interface-based dual-active detection, configure an aggregate interface and then specify the aggregate interface as the detection interface.
- Run the **port-group** *ap-num* command to add a physical member interface to the aggregate interface.
- Run the **dual-active interface** *interface-name* command to configure the aggregate interface as the dual-active detection interface, which is optional.
- Run the **dad relay enable** command to enable the device to transfer dual-active detection packets on interfaces of upstream and downstream devices, which is optional.
- Disabling the aggregate interface-based dual-active detection will make dual-active detection of the aggregate interface to take ineffective.
- If no detection interface is available after a detection interface is deleted, detection will be unavailable.
- The function of forwarding aggregate interface-based dual-active detection packets is disabled by default.

Command	**virtual-ac domain** *domain_id*
Parameter Description	*domain_id*: Indicates the virtual domain ID of the VAC system.
Defaults	The default domain ID is 100.
Command Mode	Global configuration mode
Usage Guide	Only two devices with the same domain ID can constitute a virtual device. The domain ID must be unique on a LAN.

Command	**dual-active interface** *interface-name*
Parameter Description	*interface-name*: Indicates the type and ID of the detection interface.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	Detection interfaces must belong to an aggregate interface and member interfaces of the aggregate interface must reside on different devices.

It is recommended that physical interfaces that are added to an aggregate interface reside on different devices.

When a dual-active device conflict is detected and one VAC system is enabled to enter the recovery state, you can rectify the fault by eliminating the heartbeat link failure but not by directly resetting the VAC system in recovery state. Otherwise, a dual-active device conflict will be incurred on a network.

Configuring Excluded Interface List in Recovery Mode

- When dual-active devices are detected, one active device must enter the recovery mode. In recovery mode, all service interfaces of the device need to be disabled. To ensure normal use of service interfaces for some special

purposes (for example, configuring an interface for logging in to the management device remotely), you can configure some interfaces as excluded interfaces that do not need to be disabled in recovery mode.

- After entering the config-vac-domain configuration mode, run the **dual-active exclude interface** *interface-name* command to specify excluded interfaces that do not need to be disabled in recovery mode, which is optional.

Command	**dual-active exclude interface** *interface-name*
Parameter Description	*interface-name*: Indicates the type and ID of an interface.
Defaults	*N/A*
Command Mode	config-vac-domain configuration mode
Usage Guide	This command can be configured only in VAC mode. Excluded interfaces must be routed interfaces and cannot be heartbeat interfaces. You can configure multiple excluded interfaces.

⚠ Excluded interfaces must be routed interfaces and cannot be heartbeat interfaces.

⚠ After a routed interface is switched into a switching interface (run the **switchport** command on the interface), the excluded interface configuration associated with the routed interface is automatically cleared.

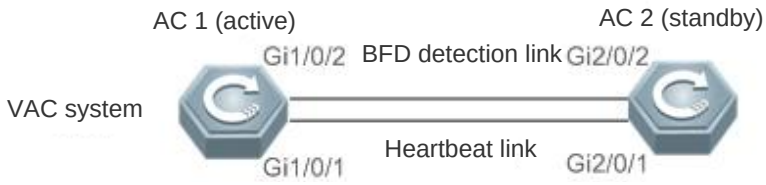
Verification

Run the **show virtual-ac dual-active summary** command to display the dual-active configuration.

Command	**show virtual-ac dual-active summary**
Parameter Description	**smmary**: Displays the summary of dual-active detection.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Configuring BFD-based Dual-active Detection

Scenario **Figure 4-14**	 - Device 1 and Device 2 constitute a VAC system (the domain ID is 100). The priority of Device 1 is 200 and the priority of Device 2 is 150. A connection is established between Gi1/0/1 of Device 1 and Gi2/0/1 of Device 2, which forms the VSL between Device 1 and Device 2. Gi1/0/2 of Device 1 is connected to G2/0/2 of Device 2. G1/0/2 and G2/0/2 are both routed interfaces. - G1/0/2 and G2/0/2 are a pair of BFD dual-active detection interfaces.
Configuration Steps	- Configure G1/0/2 and Port G2/0/2 as routed interfaces. - Enable BFD-based dual-active detection. - Configure G1/0/2 and Port G2/0/2 as BFD detection interfaces.

	Device 1 and Device 2 form a VAC system. Therefore, the configuration can be performed on Device 1 or Device 2. Device 1 is used as an example.

Switch 1	`Hostname(config)# interface GigabitEthernet 1/0/2`
	`Hostname(config-if-GigabitEthernet 1/0/2)# no switchport`
	`Hostname(config)# interface GigabitEthernet 2/0/2`
	`Hostname(config-if-GigabitEthernet 2/0/2)# no switchport`
	`Hostname(config-if)# virtual-ac domain 100`
	`Hostname(config-vac-domain)# dual-active detection bfd`
	`Hostname(config-vac-domain)# dual-active bfd interface GigabitEthernet 1/0/2`
	`Hostname(config-vac-domain)# dual-active bfd interface GigabitEthernet 2/0/2`

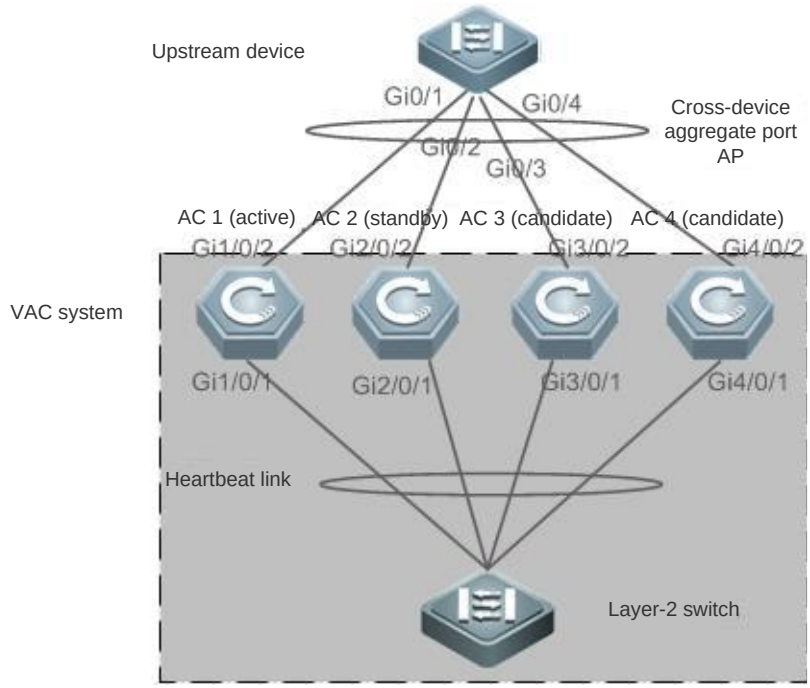
Verification	● Check the status of the dual-active detection function. ● Check the BFD-based dual-active detection configuration.

Switch 1	`Hostname# show switch virtual dual-active summary`
	`BFD dual-active detection enabled: Yes`
	`Aggregateport dual-active detection enabled: No`
	`Interfaces excluded from shutdown in recovery mode:`
	`In dual-active recovery mode: NO`
	`Hostname# show switch virtual dual-active bfd`
	`BFD dual-active detection enabled: Yes`
	`BFD dual-active interface configured:`
	`GigabitEthernet 1/0/2: UP`
	`GigabitEthernet 2/0/2: UP`

Common Errors

- A BFD detection interface is not a routed interface.
- Both BFD-based dual-active detection and aggregate interface-based dual-active detection are enabled.

↘ Configuring Aggregate Interface-based Dual-active Detection

Scenario **Figure 4-15**	 AC 1, AC 2, AC 3, and AC 4 form a VAC system (the domain ID is 1). The priority of AC 1 is 200, and the priorities of AC 2, AC 3, and AC4 are all 150. Gi1/0/1, Gi2/0/1, Gi3/0/1, and Gi4/0/1 of the VAC system establish connections with the Layer 2 switch, which form heartbeat links of the VAC system. G0/1, G0/2, G0/3, and G0/4 of the upstream device are connected to G1/0/2, G2/0/2, G3/0/2, and G4/0/2 of the VAC system respectively to form an aggregate interface that involves four member links. The ID of the aggregate interface is 1, and all members are GE SFP interfaces.
Configuration Steps	Configure AG 1 as the dual-active detection interface.

AC 1	`Hostname(config)# virtual-ac domain 100`
	`Hostname(c config-vs-domain)# dual-active detection aggregateport`
	`Hostname(config-vac-domain)# dual-active interface aggregateport 1`

Layer-2 Switch	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#interface  aggregateport 1`
	`Hostname(config-if-AggregatePort 1)#dad relay enable`

Verification	Check the status of the dual-active detection function.

AC 1	`Hostname#show virtual-ac dual-active summary`
	`BFD dual-active detection enabled: No`
	`Aggregateport dual-active detection enabled: Yes`
	`Interfaces excluded from shutdown in recovery mode:`
	`In dual-active recovery mode: No`
	`Hostname#show virtual-ac dual-active aggregateport`
	`Aggregateport dual-active detection enabled: Yes`
	`Aggregateport dual-active interface configured:`
	`  AggregatePort 1: UP`

	GigabitEthernet 1/0/2: UP GigabitEthernet 2/0/2: UP GigabitEthernet 3/0/2: UP GigabitEthernet 4/0/2: UP

Common Errors

A dual-active detection interface is not an aggregate interface.

1.4.2.4 Configuring Standby Device Preemption

Configuration Effect

Configure standby device preemption to reduce the possibility that both active and standby devices fail.

Notes

- The standby device preemption can be configured only in VAC mode.
- Standby device preemption is configured in global configuration mode and the configuration takes effect immediately on the active device. Run the **show running-config** command to display the configuration.

Configuration Step

Configuring Standby Device Preemption

Configuration Steps	Configure standby device preemption.
AC 1	Hostname(config)# virtual-ac domain 100 Hostname(config-vs-domain)# slave preemptive enable
Verification	Check the status of the dual-active detection function.
AC 1	Hostname#show running-config virtual-ac domain 100 slave preemptive enable

1.5 Monitoring

Displaying

Command	Description
show virtual-ac [**topology | config | role**]	Displays information about the running VAC system, topology, or VAC system parameters.
show virtual-ac dual-active summary	Displays the dual-active detection configuration.
show virtual-ac link [**port**]	Displays the heartbeat link running status in VAC mode.
session { **device** *device_id* | **master** }	Redirects to the console of the active device or any device.
show device id	Displays the device ID.

1 Configuring RIPT

1.1 Overview

The Remote Intelligent Perceptive Technology (RIPT) is also known as the smart access point (AP) technology. As a wireless network edge device (as compared with an AC), the smart AP can detect its connection with the access controller (AC) and take over external provisioning of wireless networks seamlessly once the connection fails. The wireless RIPT solution can be deployed on an enterprise branch network where the AC and APs are connected across a Wide Area Network (WAN), ensuring service availability in case of WAN faults. The solution can be also deployed on a Wireless Local Area Network (WLAN) network to reduce dependence on ACs and improve its availability.

Protocols and Standards

N/A

1.2 Applications

Application	Description
Deploying RIPT on a WLAN Network	Both the AC and APs are deployed on a Local Area Network (LAN).
Deploying RIPT on Enterprise Branch Networks	The AC is deployed in the enterprise headquarters, while APs are deployed in various branches and connected to the AC through a WAN.

1.2.1 Deploying RIPT on a WLAN Network

Scenario

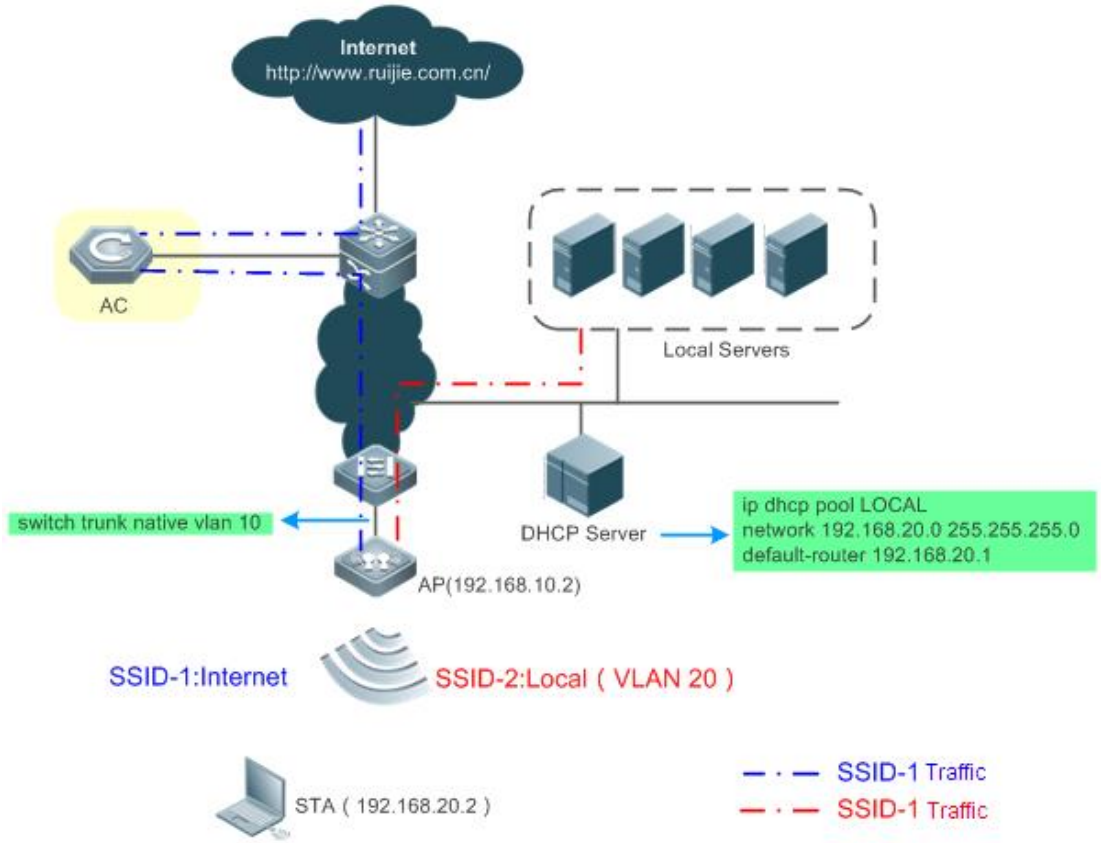
The following two types of WLANs are deployed to meet service requirements:

- WLAN for operators' Internet services: applies centralized forwarding and 802.1X/web authentication mode. There is potential demand for accounting.
- WLAN for LAN resource services: applies local forwarding and Wireless Application Protocol (WAP) or Wi-Fi Protected Access 2 - Pre-Shared Key (WAP2-PSK) authentication mode.

When the AC is unreachable (such as restart upon AC upgrade or outage of the equipment room), the wireless network can still access local resources.

For example, as shown in Figure 3-1, the AC is unreachable while the other devices such as switches and APs are normal. The WLAN service is not affected.

Figure 3-1



Remarks	The DHCP server for allocating an IP address to a STA cannot be configured on the AC. The AC cannot forward data traffic for SSID-2 in local forwarding mode.

Deployment

- Create a WLAN, and configure a forwarding mode and a security policy.
- Enable RIPT on APs.

1.2.2 Deploying RIPT on Enterprise Branch Networks

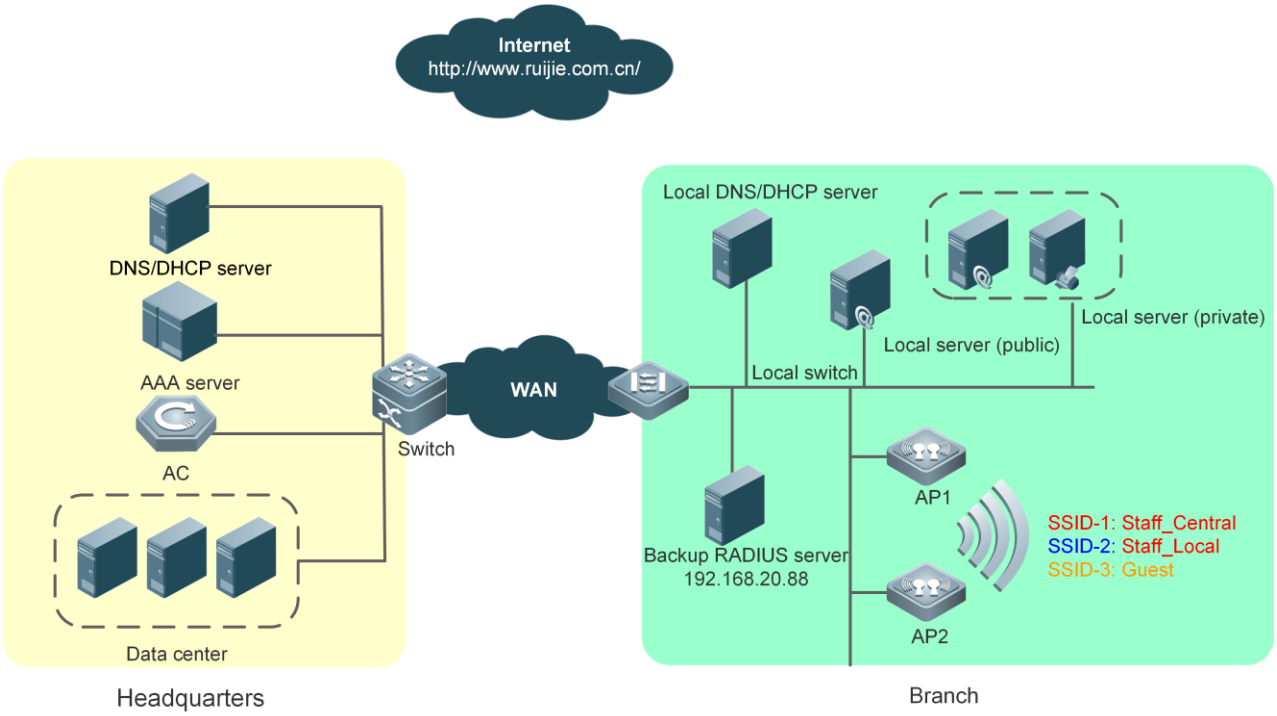
Scenario

The following are requirements for enterprise branch networks:

- An AC is deployed in the headquarters data center, while some APs and a DHCP server are deployed in the branches to serve STAs.
- A RADIUS server is deployed in the headquarters to perform access authentication for STAs in both the headquarters and all branches. If a backup RADIUS server is not deployed in the branch, access authentication for STAs in the branch fails when APs in the branch are disconnected from the AC of the headquarters (for example, when the WAN fails).
- Traffic for accessing the headquarters data center will pass the WAN between the branch and headquarters, whereas traffic for accessing local resources and Internet resources of the branch is forwarded in the branch instead of passing the WAN.

As shown in Figure 3-2, when the route from a branch AP to the headquarters AC is unreachable, the branch AP can still provide services for local resource access.

Figure 3-2



Remarks	The AC is deployed in the headquarters and connected to APs through the WAN. A DHCP server for IP address allocation is deployed in the branch. STA access authentication will be stopped when the WAN link fails. If 802.1X authentication is adopted, another WLAN can be deployed and the function of SSID enabling upon disconnection can be configured, so that the WLAN can provide network services for new STAs when the AP is disconnected. Free web authentication upon disconnection can be enabled to ensure that STAs passing web-based authentication can access the network when the AP is disconnected.

Deployment

- Deploy a WLAN for employees in the branch to access the headquarters data center, and enable the centralized forwarding mode. STA access authentication is performed in the headquarters.
- Deploy a WLAN for employees in the branch to access Internet and local resources, and enable the local forwarding mode and the 802.1X local authentication. When an AP works in connected mode, the headquarters RADIUS server performs authentication. When the AP works in standalone mode, another WLAN can be deployed and the function of SSID enabling upon disconnection can be configured, so that the WLAN can provide network services for new STAs; or the 802.1X authentication is prohibited for new STAs to ensure security.
- Deploy a WLAN for guests' access to Internet and public resources of the branch, and enable the local forwarding mode and web-based authentication. When an AP works in connected mode, the headquarters RADIUS server performs authentication. When the AP works in standalone mode, free web-based authentication can be enabled to ensure that new STAs can access the network.

- Create an AP group and configure WLAN-VLAN mapping.
- Configure the APs, add them to an AP group, and enable RIPT.

1.3 Features

Basic Concepts

Connected Mode and Standalone Mode

When a CAPWAP tunnel has been established between an AP and an AC, the AP works in connected mode.

When the CAPWAP tunnel between the AP and the AC is terminated, the AP works in standalone mode.

RIPT AP

An RIPT-enabled AP is called an RIPT AP, which is also known as a smart AP.

AC Configuration Change Monitoring

After reestablishing a CAPWAP tunnel in standalone mode with the AC, an RIPT AP should check the AC configuration change, so as to determine whether to maintain the online status of online STAs accordingly. Therefore, the AC configuration should be monitored to determine whether the AC has changed when the RIPT AP is offline.

The configuration is considerred to be changed when one of the following operations is performed:

- The AC enters the configuration mode using a CLI command, or a CLI command has been executed in configuration mode.
- The SET operation has been performed on the AC through the Simple Network Management Protocol (SNMP).

If either of the preceding operations is performed on the AC during AP logout, the AC configuration is considered to be changed. Then online STAs will be brought offline when the AP is reconnected to the AC.

When all the configuration of the AC has been stored in its flash memory, and the AC is restarted (or powered on after power-off) and the configuration file in the flash memory does not change, the configuration of the AC is considered to remain unchanged.

Overview

Feature	Description
Enabling RIPT	The AP automatically detects its connection with the AC. When the connection with the AC is terminated, the AP continues to provide services by smoothly switching to the standalone mode.
Enabling SSID Upon Disconnection	When the AP is disconnected, the WLAN provides SSIDs for STAs to access a network. In normal cases, this function is used with 802.1X authentication.
Enabling Free Web-based Authentication Upon Disconnection	After the AP is disconnected, STAs can access WLANs adopting web-based or MAC address bypass (MAB) authentication without being authenticated through web-based or MAB authentication.
Enabling the AP Standalone Mode	After the AP is disconnected, the AP can provide Wi-Fi services.

1.3.1 Enabling RIPT

An AP enabled with RIPT is an RIPT AP. When the AP detects that its connection with the AC is terminated, the AP automatically switches to the standalone mode. After a connection with the AC is reestablished, the AP switches back to the connected mode.

Working Principle

When the WLAN is set to the local forwarding mode, an RIPT AP has the same working mechanism as a common fit AP in connected mode. The AC performs STA association and authentication. When a new STA goes online, the AC backs up its information in real time to the associated RIPT AP. Then the RIPT AP creates STA information and a backup entry. When detecting that its CAPWAP connection with the AC is terminated, the RIPT AP automatically switches to the standalone mode. Then online STAs will maintain their online status, while new STAs can get online. If the WLAN works in centralized forwarding mode, online STAs will be brought offline and SSID broadcast is automatically disabled.

In standalone mode, the RIPT AP will first detect whether the AC configuration changes after reestablishing a CAPWAP tunnel with the AC. If the configuration of the AC does not change, the RIPT AP synchronies information about all online STAs to the AC, so that the AC reestablishes STA information. Then STA association and authentication are switched back to the AC, while the RIPT AP enters the connected mode. If the configuration of the AC has changed, the RIPT AP disconnects all online STAs, receives the new configuration, and then enters the connected mode.

1.3.2 Enabling SSID Upon Disconnection

When the AP connects to the AC, STAs cannot discover SSID or access a network. When the connection between the AP and AC is ended, the SSID is enabled for STAs to access the network. After the connection between the AP and AC recovers, the SSID becomes unavailable.

This function is a supplement to the RIPT AP enabled with 802.1X authentication. After the RIPT AP is disconnected, network access requests from STAs using 802.1X authentication cannot be processed. To enable STAs to access the network, configure another WLAN and enable this function.

Working Principle

If the function of SSID enabling upon disconnection is configured for STAs after the RIPT AP is disconnected, the WLAN can provide services and allow STA access. After the AP is re-connected, if the function of SSID enabling upon disconnection is configured for the WLAN, the WLAN stops working, STAs are not allowed to access the network, and online STAs become offline.

1.3.3 Enabling Free Web-based Authentication Upon Disconnection

When the AP connects to the AC, STAs can access the network only after passing web-based or MAB authentication. When the connection between the AP and AC is ended, STAs can access the network without passing web-based or MAB authentication. After the connection between the AP and AC is reestablished, STAs can access the network after passing web-based or MAB authentication.

Working Principle

An RIPT AP determines whether free web-based authentication is enabled for the WLAN after the AP is disconnected. If this function is enabled for the WLAN, STAs can directly access the network. After the AP connection is reestablished, STAs can access the network only after passing authentication.

1.3.4 Enabling the AP Standalone Mode

Before the AP establishes a connection with the AC after restart, the AP provides Wi-Fi services before restart. In the case of consistent software version, the AP provides uniform Wi-Fi services for STAs.

Working Principle

When RIPT is enabled on an AP, it can still provide Wi-Fi services normally even if the AP connection is terminated. However, after the AP restarts, it must connect to the AC and receive the configuration issued by the AC before it can provide Wi-Fi services. This function allows the AP to provide Wi-Fi services when the AP connection is terminated, and before the AP restarts and reconnects to the AC.

When the AP reconnects to the AC, if the version number of the AC is the same as that before AP disconnection, the process of restoring the connection is transparent to STAs. If the version number of the AC is different from that before AP disconnection, the AP's configuration is cleared, all STAs go offline, the AP reconnects to the AC, receives the latest configuration from the AC, and provides Wi-Fi services.

1.4 Configuration

Configuration	Description and Command	
Configuring RIPT	(Mandatory) It is used to enable RIPT.	
	ript enable	Enables RIPT.
	(Optional) It is used to configure SSID enabling upon disconnection.	
	enable-ssid at-capwap-down	Enables SSID upon disconnection.
	(Optional) It is used to enable free web-based authentication upon disconnection.	
	free-webauth at-capwap-down	Enables free web-based authentication upon disconnection.
	(Optional) It is used to enable the AP standalone mode.	
	ap-mode standalone	Enable the AP standalone mode.

1.4.1 Configuring RIPT

Networking Requirements

- An RIPT AP can independently work when its connection with the AC is terminated.
- When RIPT is enabled or disabled, the AP proactively terminates its CAPWAP connection with the AC and then reestablishes a new connection. This process occurs when the AP goes online for the first time.
- After SSID enabling is configured upon disconnection, the WLAN works only after the AP connection is ended.
- After free web-based authentication is enabled for a WLAN and the AP is disconnected, STAs can access the network without passing web-based or MAB authentication.

Notes

- Save the configuration before restarting the AC. If the configuration is not saved before the AC is restarted, the restarted AC will use the configuration stored in its flash memory. In this case, the configuration used on the RIPT

AP is different from that being used on the AC after the restart. Such a problem is handled in the same manner as the situation where the AC configuration has changed. Therefore, ensure that the AC configuration is saved before AC restart in the RIPT scenario.

- In 802.1X authentication scenarios, STAs are not allowed to access WLANs adopting 802.1X authentication after the AP connection is terminated.
- Configure the keepalive time of APs. For an RIPT AP, configure its keepalive time according to the status of the connection between the AP and the AC. For details, see **echo-interval** to be executed in AP configuration mode. This prevents instability of the CAPWAP tunnel between the AP and the AC, which may occur as a result of poor network communications between the AP and the AC.
- Ensure that requirements must be met during deployment of the DHCP server. If an RIPT AP or STA acquires its IP address through DHCP and the RIPT AP works in standalone mode, the DHCP server must be reachable for the RIPT AP and STA.

Configuration Steps

Creating a WLAN and Configuring the Local Forwarding Mode

- Mandatory. If the WLAN works in centralized forwarding mode, STAs will be brought offline after the RIPT AP switches to the standalone mode.
- Create the WLAN in global configuration mode on the AC.
- By default, the WLAN works in centralized forwarding mode.
- Run the **tunnel local** command in WLAN configuration mode to set the WLAN to the local forwarding mode.

Enabling RIPT

- Mandatory.
- Run the **ript enable** command to enable RIPT in AP or AP group configuration mode.
- Enabling the RIPT function on an AP does not affect existing services when the AP is connected to the AC.

Command	**ript enable**
Parameter Description	N/A
Defaults	RIPT is disabled.
Command Mode	AP or AP group configuration mode
Configuration Usage	N/A

Enabling or Disabling the AC Configuration Change Monitoring Function

Optional.

Command	**ript-monitor** { **enable** | **disable** }
Parameter Description	**enable**: Enables the AC configuration change monitoring function. **disable**: Disables the AC configuration change monitoring function.
Defaults	The AC configuration change monitoring function is enabled.
Command Mode	Privileged EXEC mode or global configuration mode
Configuration Usage	N/A

Enabling SSID Upon Disconnection

- Optional.
- Perform this operation in WLAN configuration mode.
- If RIPT is not enabled for the AP, this function does not take effect. After the AP connection is ended, SSID signals are not provided.
- Run the **enable-ssid at-capwap-down** command in WLAN configuration mode to enable SSID upon disconnection.

Command	enable-ssid at-capwap-down
Parameter Description	N/A
Defaults	By default, the function of SSID enabling upon disconnection is disabled.
Command Mode	WLAN configuration mode
Usage Guide	This function needs to be enabled only if 802.1X authentication is used.

Enabling Free Web Authentication Upon Disconnection

- Optional
- Perform this operation in WLAN configuration mode.
- Free Web authentication after connection interruption is performed only after this function is enabled on WLANs adopting web or MAB authentication.

Command	free-webauth at-capwap-down
Parameter Description	N/A
Defaults	By default, free web authentication upon disconnection is disabled.
Command Mode	WLAN configuration mode
Usage Guide	This function needs to be enabled only on WLANs adopting web or MAB authentication.

Enabling the AP Standalone Mode

Optional

Command	ap-mode standalone
Parameter Description	N/A
Defaults	The AP standalone mode is disabled by default.
Command Mode	AP or AP group configuration mode
Usage Guide	1. RIPT must be enabled. 2. Only OPEN or WPA/WPA2-PSK is supported. 3. The local forwarding mode must be used. 4. After the AC configuration changes, the latest configuration of the AP will take effect after 1 minute.

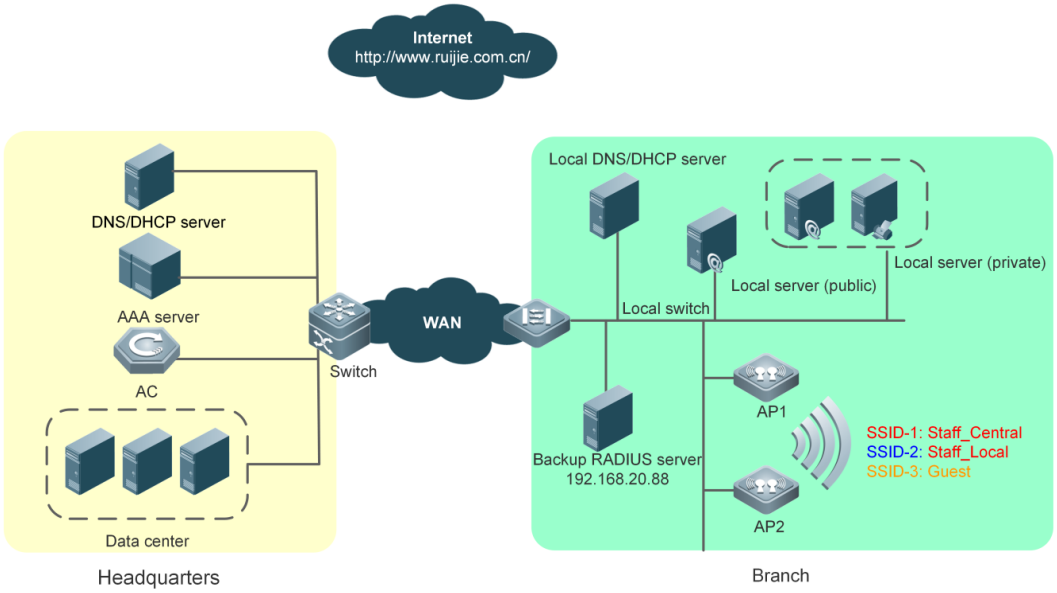
Verification

- Run the **show ap-config summary ript-enable** command to check whether RIPT and the standalone mode are enabled on the AP.

- Run the **show running-config** command to check whether the functions of SSID enabling upon disconnection and free web authentication upon disconnection are enabled.
- When the AC is correctly connected, STAs can normally go online. When the AC is restarted or disconnected, online STAs can maintain normal communications and new STAs can normally access the network.
- For WLANs with the function of SSID enabling upon disconnection enabled, SSID signals are provided only after the AP connection is ended.
- For WLANs enabled with web authentication and free web authentication upon disconnection, STAs can access the network without web authentication only after the AP connection is ended.
- Before the AP establishes a connection with the AC after restart, the AP provides Wi-Fi services as before restart.

Configuration Example

Configuring RIPT

Scenario **Figure 3-3**	
Configuration Steps	● Create a WLAN and set it to the local forwarding mode. ● Configure an AP group and specify WLAN mapping for the AP group. ● Configure the APs, add them to the AP group, and enable RIPT on the APs. ● For 802.1X authentication, configure SSID enabling upon disconnection. ● For Web authentication, enable free web authentication upon disconnection.

AC	`Hostname# configure terminal`
	`Hostname(config)# vlan 106`
	`Hostname(config-vlan)# exit`
	`Hostname(config)# vlan 107`
	`Hostname(config-vlan)# exit`
	`Hostname(config)# wlan-config 1 Staff`
	`Hostname(config-wlan)# tunnel local`
	`Hostname(config-wlan)# exit`
	`Hostname(config)# wlan-config 2 Staff_local`

```
Hostname(config-wlan)# tunnel local
Hostname(config-wlan)# exit
Hostname(config)# wlan-config 3 guest
Hostname(config-wlan)# tunnel local
Hostname(config-waln)# free-webauth at-capwap-down
Hostname(config-wlan)# exit
Hostname(config)# wlan-config 20 Staff-1x-esc
Hostname(config-wlan)# tunnel local
Hostname(config-wlan)# enable-ssid at-capwap-down
Hostname(config)# ap-group apg-test
Hostname(config-ap-group)# interface-mapping 1 106 ap-wlan-id 1
Hostname(config-ap-group)# interface-mapping 2 106 ap-wlan-id 2
Hostname(config-ap-group)# interface-mapping 3 107 ap-wlan-id 3
Hostname(config-ap-group)# interface-mapping 20 107 ap-wlan-id 4
Hostname(config-ap-group)# exit
Hostname(config)# ap-config AP1
Hostname(config-ap)# ap-group apg-test
Hostname(config-ap)# ript enable
Hostname(config-ap)# exit
Hostname(config)# ap-config AP2
Hostname(config-ap)# ap-group apg-test
Hostname(config-ap)# ript enable
Hostname(config-ap)# end
```

Verification

- Run the **show ap-config summary ript-enable** command to display the RIPT status of the APs.
- Run the **show running-config** command to display the configuration.

AC

```
Hostname# show ap-config summary ript-enable
AP Name                      IP Address      Mac Address    ript-enable
ap-mode    State
---------------------------- --------------- -------------- -----------
---------- -----
AP1                          172.18.18.11    001a.0000.de47 Y
Normal     Run
AP2                          172.18.18.12    001a.0000.de48 Y
Standalone Run
Hostname# show running-config
…
!
wlan-config 1 Staff
 tunnel local
```

```
!
wlan-config 2 Staff_local
 tunnel local
!
wlan-config 3 guest
 tunnel local
 free-webauth at-capwap-down
!
wlan-config 20 Staff-1x-esc
 tunnel local
 enable-ssid at-capwap-down
!
…
```

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Function
show ap-config summary ript-enable	Displays the RIPT configuration of APs.
show ript-monitor	Displays the AC monitoring configuration.

1 Configuring Track

1.1 Overview

The reliable network service (RNS) tests specific services provided by a peer device to monitor service availability, integrity of an end-to-end connection, and service quality. RNS test results can be used to achieve the following effects:

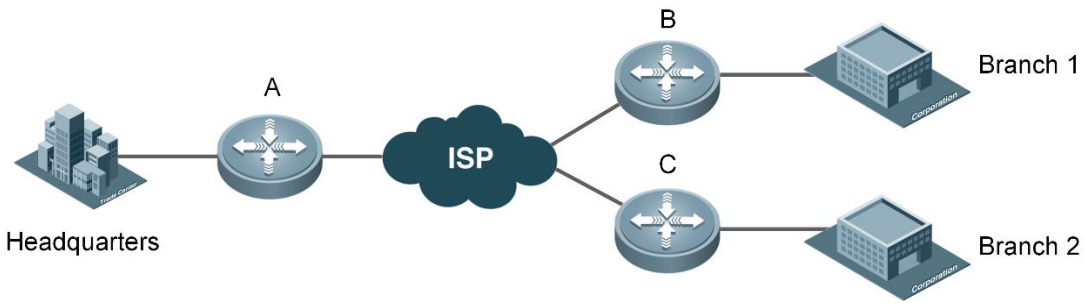
- Learn the network performance in a timely manner and take measures accordingly to handle network performance problems.
- Diagnose and locate network faults.

1.2 Applications

1.2.1 Testing and Evaluating Service Performance

Scenario

As shown in the following figure, a company will deploy a video conference system between the headquarters and branches, and has completed quality of service (QoS) configurations. Before deployment, the company needs to check whether new services can be provisioned normally without affecting existing services. The video conference system is sensitive to the User Datagram Protocol (UDP) delay and UDP transmission jitter of the network. The traditional ping tool can test the Internet Control Message Protocol (ICMP) performance, but cannot effectively evaluate the UDP transmission performance or measure the jitter.



Remarks	A, B, and C are switches.

Deployment

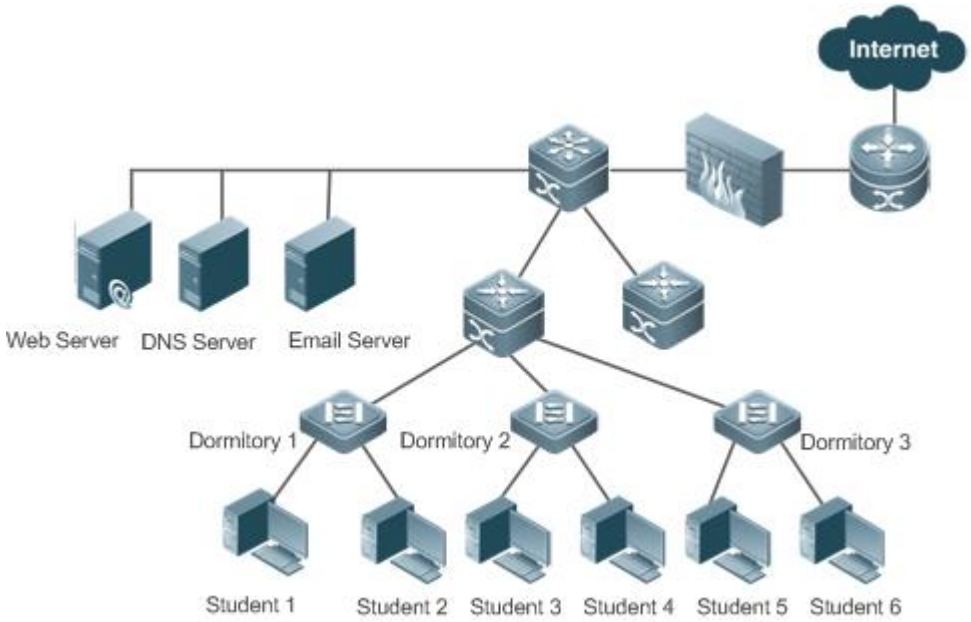
- Configure RNS on the egress switching device of each branch to test the UDP jitter and delay.
- On Switch A, specify the IP address and UDP port of the egress switching device in the headquarters, so UDP packets can be automatically sent and the egress switching device in the headquarters can automatically respond to the UDP packets. The egress switching device of the branch processes the sent and received packets to calculate the UDP jitter. To learn the performance in different periods of time, you also need to configure scheduling functions, such as periodic starting/stopping and repeated running, for the RNS.

1.2.2 Locating Network Faults

Scenario

On the campus network shown in Figure 1-1, Student 1 reports a web server access failure, Student 3 reports an Internet access failure, and Student 6 reports an email sending/receiving failure.

Figure 1-1



Deployment

- The administrator enables the domain name service (DNS) function on the access switch of dormitories to test whether the DNS server is faulty. If DNS fails, an ICMP echo packet is automatically triggered to test whether the web server is reachable.
- When a fault occurs, the administrator only needs to start a test. Then subsequent tests can be automatically triggered. The administrator can check the test results to locate the fault, which greatly reduces the workload for the administrator.

1.3 Features

Basic Concepts

↘ RNS Instance

An RNS instance can be treated as an RNS process. Before performing the RNS, you must create an RNS instance. In the RNS instance, you need to configure RNS parameters, such as the test type, test destination address, and test frequency. The instance ID is globally unique.

Feature	Description
RNS Test	Monitor network connectivity, service availability, integrity of an end-to-end connection, and service quality.
Track	Track test results and notify the related module of the results.

1.3.1 RNS Test

An RNS test is used to monitor network connectivity, service availability, integrity of an end-to-end connection, and service quality. For example, it can be used to test whether the DNS function of the device is normal. The device supports the following types of RNS tests: ICMP echo, DNS, TCP, UDP echo, and HTTP.

Working Principle

ICMP Echo Test

ICMP echo is a basic function of the RNS, and is implemented in compliance with RFC 2925. An ICMP packet is sent to check whether the destination is reachable and to calculate the network response time and packet loss rate.

An ICMP echo request packet is sent to the destination IP address based on the preset test time and frequency. Upon receipt of the ICMP echo request packet, an ICMP echo reply packet is returned from the destination IP address. Through the ICMP echo test, the response time and packet loss rate is calculated based on information related to the received ICMP echo reply packet, for example, the receipt time and number of packets. This helps you learn the network performance and status. The ICMP echo test results and historical information will be recorded, which can be displayed using commands.

For a successful ICMP echo test, the destination device must correctly respond to ICMP echo request packets.

DNS Test

In a DNS test, a DNS client is simulated to send a domain name resolution request to a specified DNS server. You can determine whether the DNS server is available and the domain name resolution speed by checking the domain name resolution result and the time required for domain name resolution. In the DNS test, the domain name resolution process is simulated, but the mapping between the resolved domain name and the IP address is not saved. The DNS test results and historical information will be recorded, which can be displayed using commands.

Procedure for Configuring an RNS Test

1 Create an instance of a specified test type and configure test parameters based on the test type.

2 Start the instance.

3 Use the RNS instance to construct a packet of the specific test type and send the packet to the peer end.

4 Upon receipt of the test packet, the peer end returns a reply packet of a corresponding type.

5 The RNS instance calculates the packet loss rate and round trip time (RTT) depending on whether a reply packet is received and the time of reply packet receipt.

6 Use the **show** or **debug** command to check the test result.

The preceding describes the general procedure for RNS tests.

Related Configuration

Configuring the Test Repeat Interval

By default, the test repeat interval is 60s.

In RNS configuration mode, run the **frequency** *millisecond* command to configure the test repeat interval.

Configure the frequency based on the following formula to ensure correct test calculation.

(**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring the Test Timeout

The default timeout varies according to the test type. You can run the **show ip rns configuration** command to display the timeout of a specific test type.

In RNS configuration mode, run the **timeout** *milliseconds* command to configure the timeout of an instance.

Configure the timeout based on a formula. For details, see "Usage Guide" of the **frequency** command.

Configure the test time threshold.

Configuring the Test Threshold

By default, the test threshold is 5000 ms.

In RNS configuration mode, run the **threshold** *milliseconds* command to configure the test threshold.

Configure the threshold based on a formula. For details, see "Usage Guide" of the **frequency** command.

Configuring a Tag for the Test

No default configuration is available.

In RNS configuration mode, run the **tag** *text* command to configure a test tag.

You can run the **tag** command to specify a tag to identify the test.

Configuring the Protocol Payload Size

The default protocol payload size varies with the test type. By default, the protocol payload size is the minimum or appropriate size for protocol packets of the corresponding test type.

In RNS configuration mode, run the **request-data-size** *bytes* command to configure the protocol payload size.

Perform this configuration in IP RNS configuration mode.

Configuring the TOS Field of Test Packets

By default, the TOS is 0.

In RNS configuration mode, run the **tos** number command to configure the TOS field in the IPv4 header of RNS test packets.

1.3.2 Track Association

Objects that can be tracked include the test result of an RNS instance, RNS list status, link status on an interface, and track list status. When the track status changes, an action of a module is triggered.

Working Principle

The test result of an RNS instance is tracked as follows:

- Configure a track object for tracking the test result of an RNS instance.
- When the test result of the RNS instance changes, the RNS module sends a status change message to the track module.

- The track module receives the test result. After the preset delay is reached, if the test result remains unchanged, the status of the track object is modified, and the module of the track object is notified of the modification. If the test result is normal within the period, the status of the track object is not modified and the corresponding module is not notified.

Related Configuration

Configuring a Track Object for Tracking the Link Status of An Interface

By default, the function of tracking the link status of an interface is disabled.

Run the **track interface line-protocol** command to configure a track object, which is used to track the link status of an interface.

If the link status of the interface is Up, the status of the track object is Up. If the link status of the interface is Down, the status of the track object is also Down.

Configuring a Track Object for Tracking the Test Result of an RNS Instance

By default, the function of tracking the test result of an RNS instance is disabled.

Run the **track rns** command to configure a track object, which is used to track the test result of an RNS instance. The RNS instance ID range is from 1 to 500.

If the RNS test succeeds, the track object is in Up state. If the RNS test fails, the track object is in Down state.

Configuring a Track Object for Tracking the Test Result of an RNS List

By default, the function of tracking the test result of an RNS list is disabled.

Run the **track rns-list** command to configure a track object, which is used to track the test result of an RNS list. The RNS instance ID range is from 1 to 500.

The result can be the AND or OR operation result of the status of all members. If the result of this track object is set to the OR operation result, and the OR result of the status of all the tracked RNS objects is Up, the status of this track object is Up. If the OR result of the status of all the tracked RNS objects is Down, the status of this track object is also Down. If the result of this track object is set to the AND operation result, and the AND result of the status of all the tracked RNS objects is Up, the status of this track object is Up. If the AND result of the status of all the tracked RNS objects is Down, the status of this track object is also Down.

Configuring a Track Object for Tracking the Status of a Track List

By default, the function of tracking the status of a track list is disabled.

Run the **track list** command to configure a track object, which is used to track the status of a track list. The result can be the AND or OR operation result of the status of all members.

If the result of this track object is set to the OR operation result of the status of all members, when all RNS tests succeed, the track object is in Up state. If one RNS test fails, the track object is in Down state. If the result of this track object is set to the OR operation result of the status of all members, when all RNS tests fail, the track object is in Down state. If one RNS test succeeds, the track object is in Up state.

Configuring a Track List Member

By default, no member is configured for the track list.

Run the **object** command to configure a track list member. The status of the member can be the same as or contrary to that of the corresponding track object.

Adjusting the Delay for Notifying the Status Change of a Track Object

By default, the delay for notifying the status change of a track object is 0.

Run the **delay** command to adjust the delay for track notification, including the delay values for notifying the status change of a track object from Up to Down and from Down to UP. The delay range is from 0 to 180, in seconds.

A longer delay indicates a longer waiting time for the associated track object being notified of the status; a shorter delay indicates a shorter waiting time for the associated track object being notified of the status.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	(Mandatory) It is used to configure basic function parameters of the RNS.	
	ip rns	Detailed configuration and brief configuration are supported: ● Detailed configuration: An RNS operation object is defined, which is used as the configuration ID for subsequent tests and parameters. ● Brief configuration: Subsequent configuration is not required, and tests can be started in one step. ICMP echo, DNS, and TCP tests can be started in one step.
	ip rns reaction-configuration	Configures the proactive threshold monitoring and triggering mechanism of an RNS test.
	ip rns reaction-trigger	Triggers another type of the RNS test in pending state when the monitoring threshold is exceeded during an RNS test.
	ip rns schedule	Configures the scheduling method, start time, and life time of an RNS test.
	ip rns restart	Restarts an RNS test.
	ip rns reset	Clears all the IP RNS configurations.
Configuring an ICMP Echo Test	(Optional) It is used to implement the ICMP echo test.	
	icmp-echo	Creates an ICMP echo test.
	request-data-size	Configures the protocol payload size.
	frequency	Configures the test repeat interval.
	tag	Configures a tag.
	threshold	Configures the test time threshold.
	timeout	Configures the test timeout.
	tos	Configures the ToS field in the IPv4 header of test packets.
Configuring a DNS Test	(Optional) It is used to implement the DNS test.	
	dns	Creates a DNS test.

Configuration	Description and Command	
	frequency	Configures the test repeat interval.
	tag	Configures a tag.
	threshold	Configures the test time threshold.
	timeout	Configures the test timeout.
	tos	Configures the ToS field in the IPv4 header of test packets.
Configuring Track	(Optional) It is used to configure track association.	
	track rns	Configures a track object for tracking the test result of an RNS instance.
	track rns-list	Configures a track object for tracking the status of an RNS list.
	track interface line-protocol	Configures a track object for tracking the link status of an interface.
	track list	Configures a track object for tracking the status of a track list.
	object	Configures a member object for a track list object.
	delay	Configures the delay for notifying the status change of a track object.

1.4.1 Configuring Basic Functions of the RNS

Configuration Effect

- Detailed configuration: Configures an RNS instance.
- Brief configuration: (Optional) Configure and start an RNS instance at a time.

Notes

- In detailed configuration mode, if you do not configure the test type after entering the IP RNS mode by running the command, the RNS instance will not be created.
- In detailed configuration mode, after configuring an RNS instance, you need to run the **ip rns schedule** command to configure the startup policy; otherwise, the test will not be implemented.

Configuration Step

Defining an RNS Operation Object

- Mandatory.
- Unless otherwise required, define an RNS operation object on each switch.
- Brief configuration is optional.

Configuring the Proactive Threshold Monitoring and Triggering Mechanism for an RNS Test

- Perform this configuration if required.
- Perform this configuration on every switch, unless otherwise required.

Enabling an RNS Instance to Trigger Another RNS Instance

- Perform this configuration if another RNS test in pending state needs to be triggered in the situation where the monitoring threshold is exceeded during an RNS test.
- If scheduling parameters are not configured for the triggered RNS instance, the default schedulingparameters are applied.
- Unless otherwise required, apply this configuration to each switch.

Configuring Scheduling Parameters of an RNS Instance

- Perform this configuration on every switch, unless otherwise required.
- In brief configuration mode, default parameter values are applied, so you do not need to perform this configuration.

Restarting an RNS Instance

- Perform this configuration, or directly run the **ip rns schedule X start-time now** command if an IP RNS instance in pending state needs to be reset.

Clearing Configurations of All RNS Instances

- Perform this configuration if required, for example, when many instances are configured but configurations are found incorrect.

Enabling the IP RNS Server

- This configuration is mandatory for UDP echo tests.
- Unless otherwise required, apply this configuration to each switch.

Verification

Run the **show ip rns configuration** command to display the RNS instance configuration.

Related Commands

Defining an IP RNS Operation Object

Command	**ip rns** *operation-number* [{ **dns** *destination-hostname* **name-server** *ip-address* | **icmp-echo** *destination-ip-address* } [**frequency** *seconds* | **timeout** *milliseconds* | **threshold** *milliseconds*] *]
Command	**ip rns** *operation-number*
Parameter Description	*operation-number*: Indicates the RNS instance ID. The value range is from 1 to 500. For details about parameters, see the configuration of the specific test type.
Command Mode	Global configuration mode
Usage Guide	The device supports only IPv4-related tests, but not IPv6-related tests. A maximum of 500 tests can be configured, depending on the device performance. The test function is only a value-added function. When a large number of tests are configured and consume a lot of system resources, the test function may be temporarily disabled to ensure normal operation of core services, such as route forwarding. Detailed configuration (**ip rns** *operation-number* with mandatory parameters specified**)**: Run this command and enter the IP RNS configuration mode. In this mode, you can define various test types. If the test type is not configured, the RNS test is not created. After configuring an RNS test, you must

	run the **ip rns schedule** command to configure scheduling parameters; otherwise, the test cannot be conducted. After configuring the type of an RNS test, you can run the **ip rns** command to enter the mode of the test type. To modify the type of an RNS test, you need to first delete the RNS instance by running the **no ip rns** command in global configuration mode. Brief configuration (**ip rns** with optional parameters specified): Running **ip rns** with optional parameters specified is equivalent that **ip rns operation-number**, **ip rns schedule**, detailed test configuration (such as the ICMP echo test), **frequency**, **timeout**, and **threshold** are executed according to the logical sequence. Among these commands, the **ip rns schedule** command is executed to start a test by using the **start-time now life forever** parameter. For details about restrictions of other configuration items, see the related description in the detailed configuration. Similarly, to modify a test in brief configuration mode, you need to first delete this RNS test by running the **no ip rns** command in global configuration mode.

Configuring the Proactive Threshold Monitoring and Triggering Mechanism for the Test

Command	**ip rns reaction-configuration** *operation-number* **react** *monitored-element* [**action-type** *option*] [**threshold-type** { **average** [*number-of-measurements*] | **consecutive** [*occurrences*] | **immediate** | **never** | **xofy**[*x-value y-value*] }] [**threshold-value** *upper-threshold lower-threshold*]
Parameter Description	*operation-number*: Indicates the RNS instance ID. The value range is from 1 to 500. *monitored-element*: Specifies the monitored element. **action-type** *option*: Indicates the action taken after the test is triggered. **average** [*number-of-measurements*]: Indicates that the subsequent associated actions are triggered if the average of *number-of-measurements* of the monitored element exceeds the threshold. **consecutive** [*occurrences*]: Indicates that the test is triggered if the consecutive number of *occurrences* of the monitored element exceeds the threshold. The default value of *occurrences* is 5. The value range is from 1 to 16. **immediate**: Indicates that the test is triggered immediately after the monitored element exceeds the threshold. **never**: Indicates that the test is never triggered. **xofy** [*x-value y-value*]: Indicates that results of X tests exceed the threshold in the last Y tests. The default values of X and Y are 5. The value of X or Y ranges from 1 to 16. **threshold-value** *upper-threshold lower-threshold*: Indicate the upper and lower thresholds. ● When the value of *monitored-element* is the RTT, the threshold is the time. For default values, see "Usage Guide". The value range is from 0 to 60,000, in milliseconds. ● You do not need to configure **threshold-value** when **react** is set to **timeout**.
Command Mode	Global configuration mode
Usage Guide	You can configure multiple thresholds for one RNS test to monitor different elements. The following table provides the mapping between test types and monitored elements.

Monitored Element	icmp-echo	dns
timeout	✓	✓
rtt	✓	✓

The following table lists the default thresholds of each monitored element.

Monitored Element	Upper Threshold	Lower Threshold

	timeout	-	-
	rtt	5000 ms	0 ms

Enabling an RNS Instance to Trigger Another RNS Instance

Command	**ip rns reaction-trigger** *operation-number target-operation*
Parameter Description	*operation-number*: Indicates the number of the source RNS instance that triggers the action. The value range is from 1 to 500. *target-operation*: Indicates the number of the target RNS instance that is triggered. The value range is from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	The trigger function is typically used in network fault diagnosis scenario. In a common scenario, you do not need to configure the trigger function.

Configuring Scheduling Parameters of an RNS Instance

Command	**ip rns schedule** *operation-number* [**life** { **forever** |*seconds* } | **start-time** { *hh*:*mm* [:*ss*] [*month day* | *daymonth*] | **pending** | **now** | **after***hh*:*mm*:*ss* } | **recurring**] *
Parameter Description	*operation-number*: Indicates the number of the RNS operation. The value range is from 1 to 500. **lifeforever**: Indicates that the RNS operation life time is valid forever. **life** *seconds*: Indicates the running time of the RNS instance, in seconds. *hh:mm[:ss]*: Indicates the start time of the RNS instance, in 24-hour format. *month*: Indicates the start month of the RNS instance. The default value is the current month. *day*: Indicates the start date of the RNS instance. The default value is the current date. **pending**: Indicates that the start time of the RNS instance is not defined, which is the default. **now**: Indicates that the operation start time is now, that is, the operation starts now. **after***hh:mm:ss*: Indicates that the RNS instance starts after a delay of hh:mm:ss. **recurring**: Indicates whether the RNS instance starts at the same time every day.
Command Mode	Global configuration mode
Usage Guide	If scheduling parameters of an RNS test have been configured by running the **ip rns schedule** command, parameters cannot be modified during running. To modify the configuration, you need to run the **no ip rns schedule** command to delete the scheduling parameters. **life** { *seconds* } indicates the running time of the RNS instance. That is, the test stops after a period of time specified by *seconds*.

Restarting an RNS Test by Running the ip rns restart Command

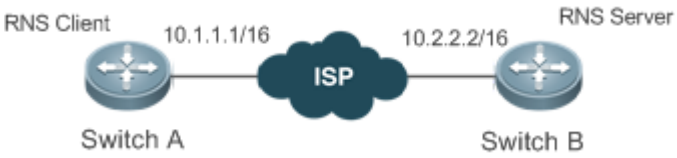
Command	**ip rns restart** *operation-number*
Parameter Description	*operation-number*: Indicates the number of an RNS test. The value range is from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	This command restarts an RNS test for which the scheduling policy is configured and is in pending state. This command is invalid for an RNS test for which the scheduling policy is not configured.

Clearing Configurations of All the IP RNS Instances by Running the ip rns reset Command

Command	ip rns reset
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command clears configurations of all the IP RNS instances. It is used only in extreme cases, for example, when many RNS tests are configured but the configurations are found incorrect.

Configuration Example

Configuring Basic Functions of the RNS

Scenario Figure 1-2	
Configuration Steps	● Configure instance 1 on Switch A. ● Configure the scheduling method, start time, and life time of instance 1. ● Configure the proactive threshold monitoring and triggering mechanism of instance 1. ● Trigger instance 2 in pending state when the monitoring threshold of instance 1 is exceeded.

Switch A	`A# configure terminal`
	`A(config)# ip rns 1`
	`A(config-ip-rns)# icmp-echo 10.1.1.1`
	`A(config-ip-rns-icmp-echo)# exit`
	`A(config)# ip rns schedule 1 start-time now life forever`
	`A(config)# ip rns reaction-configuration 1 react timeout threshold-type immediate action-type trigger`
	`A(config)# ip rns reaction-trigger 1 2`

Verification	Run the **show ip rns configuration** command to display the instance configuration.
	`Router# show ip rns configuration 1`
	`Entry number: 1`
	`Tag: ruijie555`
	`Type of operation to perform: icmp-echo`
	`Operation timeout (milliseconds): 5000`
	`Operation frequency (milliseconds): 60000`
	`Threshold (milliseconds): 5000`
	`Recurring (Starting Everyday): FALSE`
	`Life (seconds): 3500`
	`Next Scheduled Start Time:Start Time already passed`
	`Target address/Source address: 2.2.2.3/0.0.0.0`
	`Request size (ARR data portion): 36`

1.4.2 Configuring an ICMP Echo Test

Configuration Effect

Create an ICMP echo test.

Notes

Basic functions of the RNS must be configured.

Configuration Steps

Creating an ICMP Echo Test

- Mandatory.
- Unless otherwise required, create ICMP echo test instances on each switch.

Configuring Common Optional Parameters of the Test

- Mandatory if common optional parameters of the test, for example, the repeat interval, tag, time threshold, timeout, and ToS, are required to be changed.
- Perform this configuration on every switch, unless otherwise required.

Configuring the Protocol Payload Size

- Perform this configuration if required.
- Perform this configuration on every switch, unless otherwise required.

Verification

Run the **show ip rns configuration** command to display the instance configuration.

Related Commands

Creating an ICMP Echo Test

Command	**icmp-echo** { **oob** { *destination-ip-address* | *destination-hostname* [**name-server** *ns-ip-address*] } [**source-ipaddr** *src-ip-address*] [**out-interface** *type num* [**next-hop** *nh-ip-address*]]
Parameter Description	*destination-ip-address*: Indicates the destination IP address. *destination-hostname*: Indicates the destination host name. **name-server** *ip-address*: Specifies the DNS server when the destination host name is configured. By default, the DNS server configured by using the **ipname-server** command is used for address resolution. **source-ipaddr** *ip-address*: Indicates the source IP address. **out-interface** *type num*: Specifies the outbound interface (non-MGMT interface) of test packets. **next-hop** *A.B.C.D*: Indicates the IP address of the next hop.
Command Mode	IP RNS configuration mode (config-ip-rns)
Usage Guide	After an ICMP echo test is started, the system sends an ICMP echo request packet to test whether the device is connected to the target host. After an ICMP echo test is created, the system enters the IP RNS ICMP echo mode. By default, the protocol payload size of an ICMP echo request packet is 36

	bytes. You can run the **request-data-size** command to change the packet size. You need to configure the RNS test type (for example, ICMP echo and DNS) before configuring parameters. To modify the type of an RNS instance, you need to delete the RNS instance by running the **no ip rns** command in global configuration mode.

Configuring the Protocol Payload Size of an RNS Instance

Command	**request-data-size** *bytes*
Parameter Description	*bytes*: Indicates the bytes of a test packet. The minimum and maximum bytes vary with the test type. You need to configure this parameter based on the command prompt in corresponding test mode.
Command Mode	IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	This command is used to pad some bytes in a test packet so that large packets can be used for the test.

Configuring the Test Repeat Interval

Command	**frequency** *milliseconds*
Parameter Description	*milliseconds*: Indicates the packet sending interval, in milliseconds. The default value is 60000 ms. The value ranges from 10 to 604,800,000. The maximum value is one week.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	After an RNS instance is started, tests are conducted periodically. You can run the **frequency** command to specify the repeat interval. You need to configure the frequency based on the following formula to ensure correct test calculation: (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring a Tag for an RNS Instance

Command	**tag** *text*
Parameter Description	*text*: Sets the test tag. The value is a string of up to 79 characters.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	This command specifies a tag for a test, which is often used to indicate the function of the test.

Configuring the Time Threshold for an RNS Instance

Command	**threshold** *milliseconds*
Parameter Description	*milliseconds*: Indicates the time threshold for the test, in milliseconds. The value range is from 0 to 60,000. The default value is 5,000.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	Configure the threshold based on the following formula to ensure correct test calculation: (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring the Timeout for an RNS Instance

Command	**timeout** *millisecond*

Parameter Description	*millisecond*: Indicates the test timeout, in milliseconds. The value range is from 10 to 604,800,000. The default timeout varies according to the test type.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	Configure the timeout based on the following formula to ensure correct test calculation: (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring the ToS Field in the IPv4 Packet Header of an IP RNS Test

Command	**tos** *number*
Parameter Description	*number*: Sets the TOS field in the IPv4 header of test packets. The value range is from 0 to 255. The default value is 0.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	The ToS field has 8 bits in the IPv4 packet header. By setting the ToS field, the device can control the priority of the test packet. For different ToS fields, processing priorities are different on intermediate routers.

Configuration Example

Figure 1-3	
Configuration	Configure RNS instance 1 and parameters on Switch A.

Switch A	`A# configure terminal`
	`A(config)# ip rns 1`
	`A(config-ip-rns)#icmp-echo 10.2.2.2`
	`A(config-ip-rns-icmp-echo)#exit`
	`A(config)#ip rns schedule 1 start-time now life forever`

Verification	● Run the **show ip rns configuration** command to display the instance configuration.

Switch A	`A#show ip rns configuration 1`
	`Entry number: 1`
	`Tag:`
	`Type of operation to perform: icmp-echo`
	`Operation timeout (milliseconds): 5000`
	`Operation frequency (milliseconds): 60000`
	`Threshold (milliseconds): 5000`
	`Recurring (Starting Everyday): FALSE`
	`Life (seconds): foerver`
	`Next Scheduled Start Time:Start Time already passed`
	`Target address/Source address: 10.2.2.2/0.0.0.0`
	`Request size (ARR data portion): 36`

1.4.3 Configuring a DNS Test

Configuration Effect

Create a DNS test.

Notes

Basic functions of the RNS must be configured.

Configuration Step

Creating a DNS Test

- Mandatory.
- Unless otherwise required, create a DNS test on each switch.

Configuring Common Optional Parameters of the Test

- Mandatory if common optional parameters of the test, for example, the repeat interval, tag, time threshold, timeout, and TOS, need to be changed.
- Perform this configuration on every switch, unless otherwise required.

Verification

Run the **show ip rns configuration** command to display the instance configuration.

Related Commands

Creating a DNS Test

Command	**dns** *destination-hostname* **name-server** *ip-address* [**out-interface** *type num* [**next-hop** *ip-address*] | **source-ipaddr** *ip-address*] *
Parameter Description	*destination-hostname*: Indicates the destination host name. **name-server** *ip-address*: Indicates the DNS IP address. **source-ipaddr** *ip-address:* Indicates the source IP address. **out-interface** *type num*: Specifies the outbound interface (non-MGMT interface) of test packets. **next-hop** *ip-address*: Indicates the IP address of the next hop when the outbound interface is specified.
Command Mode	IP RNS configuration mode (config-ip-rns)
Usage Guide	After a DNS test is started, the system sends a DNS parsing request packet to test whether the device is connected to the target host. After a DNS test instance is created, the system enters the IP RNS DNS mode. You need to configure the RNS test type before configuring parameters. To modify the type of an RNS instance, you need to delete the RNS instance by running the **no ip rns** command in global configuration mode.

Configuring the Test Repeat Interval

Command	**frequency** *milliseconds*
Parameter Description	*milliseconds*: Indicates the packet sending interval, in milliseconds. The default value is 60000 ms. The value range is from 10 to 604800000. The maximum value is one week.
Command	IP RNS DNS configuration mode (config-ip-rns-dns)

Mode	IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	After an RNS instance is started, tests are conducted periodically. You can run the **frequency** command to specify the repeat interval. You need to configure the frequency based on the following formula to ensure correct test calculation: (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring a Tag for an RNS Instance

Command	**tag** *text*
Parameter Description	*text*: Sets the test tag. The value is a string of up to 79 characters.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	This command specifies a tag for a test, which is often used to indicate the function of the test.

Configuring the Time Threshold for an RNS Instance

Command	**threshold** *milliseconds*
Parameter Description	*milliseconds*: Indicates the time threshold for the test, in milliseconds. The value range is from 0 to 60000. The default value is 5000.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	Configure the threshold based on the following formula to ensure correct test calculation: (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configuring the Time Threshold for an RNS Instance

Command	**timeout** *millisecond*
Parameter Description	*millisecond*: Indicates the test timeout, in milliseconds. The value range is from 10 to 604800,000. The default timeout varies according to the test type.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	Configure the timeout based on the following formula to ensure correct test calculation: (**frequency** *milliseconds*) > (**timeout** *milliseconds*) >= (**threshold** *milliseconds*)

Configures the ToS Field in the IPv4 Header of Test Packets

Command	**tos** *number*
Parameter Description	*number*: Sets the ToS field in the IPv4 header of test packets. The value range is from 0 to 255. The default value is 0.
Command Mode	IP RNS DNS configuration mode (config-ip-rns-dns) IP RNS ICMP echo configuration mode (config-ip-rns-icmp-echo)
Usage Guide	The ToS field has 8 bits in the IPv4 packet header. By setting the ToS field, the device can control the priority of the test packet. For different ToS fields, processing priorities are different on intermediate routers.

Configuration Example

Scenario **Figure 1-4**	
Configuration Steps	● Configure RNS instance 1 and parameters on Switch A.

Switch A	`A# configure terminal`
	`A(config)# ip rns 1`
	`A(config-ip-rns)# dns www.ruijie.com.cn name-server 10.2.2.2`
	`A(config-ip-rns-dns)#exit`
	`A(config)ip rns schedule 1 start-time now life forever`

Verification	● Run the **show ip rns configuration** command to display the instance configuration.

Switch A	`A#show ip rns configuration 1`
	`Entry number: 1`
	`Tag:`
	`Type of operation to perform: dns`
	`Operation timeout (milliseconds): 5000`
	`Operation frequency (milliseconds): 60000`
	`Threshold (milliseconds): 5000`
	`Recurring (Starting Everyday): FALSE`
	`Life (seconds): forever`
	`Next Scheduled Start Time:Start Time already passed`
	`Target host name: www.ruijie.com.cn`
	`Name Server: 10.2.2.2`

Common Errors

The DNS IP address is incorrect.

1.4.4 Configuring Track Association

Configuration Effect

- Configure the track function to track the test result of an RNS instance.
- Configure the track function to track the link status of an interface.
- Configure the track function to track the status of a track list.
- Configure the track function to track the status of an RNS list.

Notes

- To configure the track function to track the test result of an RNS instance, you need to configure an RNS instance.
- To configure the track function to track the link status of an interface, you need to configure the interface.
- To configure the track function to track the status of a track list, you need to configure members for the track list.
- To configure the track function to track the status of an RNS list, you need to configure members for the RNS list.

Configuration Step

Configuring a Track Object

- Perform this operation if required.
- The following four methods are available to create a track object:
- Create a track object for tracking the test result of an RNS instance. Perform this configuration on every switch, unless otherwise required.
- Create a track object for tracking the link status of an interface. Perform this configuration on every switch, unless otherwise required.
- Create a track object for tracking the status of a track list. Perform this configuration on every switch, unless otherwise required.
- Create a track object for tracking the status of an RNS list. Perform this configuration on every switch, unless otherwise required.

Configuring the Notification Delay of a Track Object

- Perform this configuration if notifying the status change of a track object needs to be delayed.
- The delay for notifying the status change of a track object includes the delay for notifying the status change of a track object from Up to Down and the delay for notifying the status change of a track object from Down to UP. You can configure either delay or both of them.
- Perform this configuration on every switch, unless otherwise required.

Configuring a Track Member

- Perform this configuration if a track object for tracking the status of a track list needs to be configured.
- When configuring a track member, you can set the status of a member meeting conditions to Up or Down.
- Perform this configuration on every switch, unless otherwise required.

Verification

Check the status of a track object when the status of the track object (such as test results of an RNS instance, link status of an interface, or status of a track list) changes.

- After the preset delay, run the **show track** command to check whether the track status changes.

Related Commands

Configuring a Track Object for Tracking the Link Status of an Interface

Command	**track** *object-number* **interface** *interface-type interface-number* **line-protocol**
Parameter Description	*object-number*: Indicates the number of a track object. The value range is from 1 to 700. *Interface-type interface-number*: Indicates the interface type and interface number.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the link status of an interface. When the link status of the interface is Up, the status of the corresponding track object is Up.

Configuring a Track Object for Tracking the Test Result of an RNS Test

Command	**track** *object-number* **rns** *entry-number*
Parameter Description	*object-number*: Indicates the number of a track object. The value range is from 1 to 700. *entry-number*: Indicates the number of an RNS instance. The value range is from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the result of an RNS test. If the test succeeds, the track object is in Up state.

Configuring a Track Object for Tracking the Status of a Track List

Command	**track** *object-number* **listboolean** { **and** | **or** }
Parameter Description	*object-number*: Indicates the number of a track object. The value range is from 1 to 700.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the status of a track list. The result can be the AND or OR operation result of the status of all members.

Configuring a Track Member

Command	**object** *object-number* [**not**]
Parameter Description	*object-number*: Indicates the number of a track object. The value range is from 1 to 700.
Command Mode	Track configuration mode
Usage Guide	Run this command to configure a member for a track list. The number of track list members that can be configured is restricted only by the number of track objects.

Configuring a Track Object for Tracking the Status of an RNS List

Command	**track** *object-number* **rns-list** *men-list* { **and** | **or** }
Parameter Description	*object-number*: Indicates the number of a track object. The value range is from 1 to 700. men-list: Indicates the RNS list that is tracked. The value of **mem-list** can be an RNS instance or a series of RNS instances. If the value of **mem-list** is a series of RNS instances, the format is as follows: *smallest RNS ID–largest RNS ID*, for example, 10–20. The RNS ID range is from 1 to 500.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure a track object for tracking the status of an RNS list. The result can be the AND or OR operation result of the status of all members.

Configuring the Notification Delay of a Track Object

Command	**delay** { **up** *seconds* [**down** *seconds*] **|** [**up** *seconds*] **down** *seconds* }
Parameter Description	**up** *seconds*: Specifies the delay for notifying the status change of a track object from Down to Up, in seconds. The value range is from 0 to 180. The default value is 0. **down** *seconds*: Specifies the delay for notifying the status change of a track object from Up to Down, in seconds. The value ranges from 0 to 180. The default value is 0.
Command	Track configuration mode

Mode	
Usage Guide	When the status of a track object frequently changes, the status of the client that use this track object will frequently change. Using this command can delay notification of the status change of a track object. For example, if the status of a track object changes from Up to Down, and **delay down 10** is configured, the Down status of the track object is notified 10s later. If the status of the track objects changes to Up again within this period of time, no notification is sent. For the client that uses this track object, the status of the track object is always Up.

Displaying the Track Object Statistics

Command	**show track** [*object-number*]
Parameter Description	*object-number*: Indicates the number of a track object. The value range is from 1 to 700. The default value is all track objects.
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display statistics on track objects.

Configuration Example

Configuring Track Object 3 for Tracking the Link Status of FastEthernet 1/0

Configuration Steps	● Configure a track object for tracking the link status of an interface. ● Configure the delay for notifying the status change from Up to Down.

	`Hostname# configure terminal`
	`Hostname(config)# track 3 interface FastEthernet 1/0 line-protocol`
	`Hostname(config-track)# delay down 10`
	`Hostname(config-track)# exit`

Verification	Change the link status of FastEthernet 1/0 to Down. ● Immediately check the status of the track object, and verify that the status is still Up. ● Check the status of the track object 10s later, and verify that the status changes to Down.

	`Hostname# show track 3`
	`Track 3`
	`  Interface FastEthernet 1/0`
	`  The state is Up, delayed Down (5 secs remaining)`
	`    1 change, current state last: 300 secs`
	`  Delay up 0 secs, down 10 secs`

Configuring Track Object 3 (When the Status of Track Object 1 Is Up, and the Status of Track Object 2 Is Down, the Status of Track Object 3 is Up)

Configuration Steps	● Configure track object 1 and track object 2. ● Configure track object 3. Its members include track object 1 and track object 2.

	`Hostname # config terminal`
	`Hostname(config)# track 1 interface gigabitEthernet 0/0 line-protocol`
	`Hostname(config-track)# delay up 20 down 40`
	`Hostname(config-track)# exit`

	Hostname(config)# Hostname(config)# track 2 interface gigabitEthernet 0/1 line-protocol Hostname(config-track)# delay down 30 Hostname(config-track)# exit Hostname(config)# track 3 list Boolean and Hostname(config-track)# object 1 Hostname(config-track)# object 2 not Hostname(config-track)# exit
Verification	When the status of track objects 1 and 2 change, check the status of track object 3. ● When the status of track object 1 changes from Down to Up, and the status of track object 2 remains Down , verify that the status of track object 3 changes from Down to Up. ● When the status of track object 1 remains Up, and the status of track object 2 changes from Down to Up, verify that the status of track object 3 changes from Up to Down.
	Hostname# show track 3 Track 3 List boolean and Object 1 Object 2 not The state is Down 1 change,current state last:10 secs Delay up 0 secs,down 0 secs

Configuring Track Object 5 for Tracking the Test Result of RNS Instance 7

Configuration Steps	● Configure an RNS test. ● Configure a track object to track the result of the RNS test. ● Configure the delay for notifying the test result change from Up to Down, and the delay for notifying the test result change from Down to Up.
	Hostname# configure terminal Hostname(config)# ip rns 7 Hostname(config-ip-rns)# icmp-echo 2.2.2.2 Hostname(config-ip-rns-icmp-echo)# exit Hostname(config)# ip rns schedule 7 start-time now life forever Hostname(config)# track 5 rns 7 Hostname(config-track)# delay up 20 down 30 Hostname(config-track)# exit
Verification	Make the test result of RNS instance 7 change from successful to unsuccessful. ● When the test result changes to unsuccessful, immediately check the status of track object 7, and verify that the status is still Up. ● Check the status of the track object 30s later, and verify that the status changes to Down.
	Hostname# show track 5 Track 5

	Reliable Network Service 7 The state is Down 2 change, current state last: 10 secs Delay up 20 secs, down 30 secs

Configuring Track Object 5 for Tracking the Test Results of an RNS List (Consisting of RNS Instances 1, 2–5, and 8)

Configuration Steps	● Configure and start an RNS test (see *RNS Configuration*). ● Configure a track object for tracking the test result of an RNS list. ● Configure the delay for notifying the test result change from Up to Down, and the delay for notifying the test result change from Down to Up.
	Hostname(config)# track 5 rns-list 1,2-5,8 and Hostname(config-track)# delay up 20 down 30 Hostname(config-track)# exit
Verification	Let the test result of one of the RNS instances 1, 2-5, and 8 changes from successful to unsuccessful. ● When the test result changes to unsuccessful, immediately check the status of track object 7, and verify that the status is still Up. ● Check the status of the track object 30s later, and verify that the status changes to Down.
	Hostname# show track 5 Track 5 rns-list 1,2-5,8 and The state is Down 2 change, current state last: 10 secs Delay up 20 secs, down 30 secs

Common Errors

- The track object for tracking an RNS test is configured, but the RNS test is not configured.
- The track object for tracking the link status of an interface is configured, but the corresponding interface is not configured.
- The track object for tracking the status of a track list, but no member of the RNS list is configured.
- The track object configured for tracking an RNS list, but the RNS test is not configured.

1.5 Monitoring

Displaying

Command	Description
show ip rns configuration [*operation-number*]	Displays configurations of one or more RNS instances.
show ip rns collection-statistics [*operation-number*]	Displays detailed statistics on one or more RNS instances.
show ip rns operational-state [*operation-number*]	Displays the current RNS status.

show ip rns reaction-configuration [*operation-number*]	Displays proactive threshold monitoring information about one or more RNS instances.
show ip rns reaction-trigger [*operation-number*]	Displays information about the test triggered by one or more RNS instances.
show ip rns statistics [*operation-number*]	Displays brief statistics on one or more RNS instances.
show track [*object-number*]	Displays brief statistics on one or more track objects.

Debugging



Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug track { **all** | **proc-event** | **rdnd-event** | **client** }	Debugs the track module.
debug rns { **all** | **interface** | **lib** | **rdnd-event** | **restart** | **rns_id** [**0, 500**] }	Debugs the RNS module.

Configuring Network Management and Monitoring

1. Configuring SPAN
2. Configuring NTP
3. Configuring SNTP
4. Configuring FTP Server
5. Configuring FTP Client
6. Configuring TFTP Server
7. Configuring TFTP Client
8. Configuring SNMP
9. Configuring RMON
10. Configuring NETCONF
11. Configuring CWMP
12. Configuring gRPC
13. Configuring INC
14. Configuring MQTT
15. Configuring RPCAP

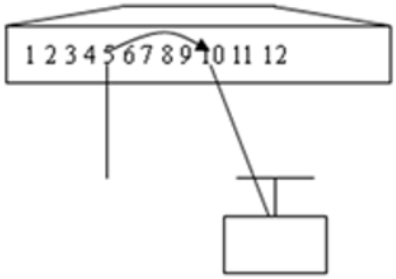
1 Configuring SPAN

1.1 Overview

The Switched Port Analyzer (SPAN) is to copy packets of a specified port to another device port that is connected to a network monitoring device, so as to achieve network monitoring and troubleshooting.

All incoming and outgoing packets of a source port can be monitored through SPAN. For example, as shown in the following figure, all packets on Port 5 are mapped to Port 10, and the network analyzer connected to Port 10 receives all packets that pass through Port 5.

Figure 1-1 SPAN Configuration



The SPAN function is mainly applied in network monitoring and troubleshooting scenarios to monitor network information and rectify network faults.

1.2 Features

Basic Concepts

SPAN Session

A SPAN session is a data stream between the SPAN source port and destination port, which can be used to monitor packets of one or more ports in the inbound, outbound, or both directions. Switched ports, routed ports, and aggregate ports can be configured as source or destination ports of SPAN sessions. Normal operations on a switch are not affected when ports of the device are added to a SPAN session.

You can configure a SPAN session on a disabled port but the SPAN session is inactive. A SPAN session is in active state only after the port on which the SPAN session is configured is enabled. In addition, a SPAN session does not take effect after a device is powered on. It is active only after the destination port is in operational state. You can run the **show monitor** [**session** *session-id*] command to display the operation status of a SPAN session.

SPAN Data Streams

A SPAN session involves data streams in three directions:

- Incoming data streams: All packets received by a source port are copied to the destination port. You can monitor incoming packets of one or more source ports in a SPAN session. Some incoming packets of a source port may be discarded for some reasons (for example, considering port security). However, such packets are still mirrored to the destination port.
- Outgoing data streams: All packets transmitted by a source port are copied to the destination port. You can monitor outgoing packets of one or more source ports in a SPAN session. Packets transmitted from other ports to a source port may be discarded for some reasons and such packets will not be transmitted to the destination port. The format of outgoing packets of a source port may be changed for some reasons. For example, after routing, packets transmitted from the source port are changed in source MAC addresses, destination MAC addresses, VLAN IDs, and TTLs, and their formats are also changed after being copied to the destination port.
- Bidirectional data streams: Bidirectional data streams include incoming and outgoing data streams. In a SPAN session, you can monitor data streams of one or more source ports in inbound and outbound directions.

Source Port

A source port is called a monitored port. In a SPAN session, data streams of the source port are monitored for network analysis and troubleshooting. In a single SPAN session, you can monitor the incoming, outgoing, and bidirectional data streams, and the number of source ports is not restricted.

A source port has the following features:

- A source port can be a switched port, a routed port, or an aggregate port.
- A source port cannot be used as a destination port simultaneously.
- A source port and a destination port can belong to the same VLAN or different VLANs.

Destination Port

A SPAN session has one destination port (called a monitoring port) for receiving packets copied from a source port.

A destination port has the following features:

- A destination port can be a switched port, a routed port, or an aggregate port.
- A destination port cannot be used as a source port simultaneously.

Overview

Feature	Description
SPAN	Configures mirroring of ports on the same device.

1.2.1 SPAN

SPAN is used to monitor data streams on switches. It copies frames on one port to another switch port that is connected to a network analyzer or RMON analyzer so as to analyze communication of the port.

Working Principle

When a port transmits or receive packets, the SPAN-enabled device checks that the port is configured as a SPAN source port. Then it copies the packets transmitted and received by the port to the destination port.

Configuring a SPAN Source Port

You need to specify a SPAN session ID and source port ID to configure a SPAN source port, and set the optional SPAN direction item to determine the direction of SPAN data streams or specify an Access Control List (ACL) to mirror specific data streams.

Configuring a SPAN Destination Port

You need to specify a SPAN session ID and destination port ID to configure a SPAN destination port, and set the optional switching function item to determine whether to enable the switching function and configure the SPAN destination port to remove tags.

Related Configuration

The SPAN function is disabled by default. It is enabled only after a session is created, and the SPAN source and destination ports are configured. A SPAN session can be created when a SPAN source port or destination port is configured.

Configuring a SPAN Source Port

A SPAN session does not have a SPAN source port by default. You can run the **monitor session** *session-id* **source interface** *interface-id* [**both** | **rx** | **tx**] command to configure a SPAN source port.

session-id: Indicates the SPAN session ID. The number of supported SPAN sessions varies with products.

interface-id: Indicates the SPAN source port to be configured.

rx: Indicates that only packets received by the source port are monitored.

tx: Indicates that only packets transmitted by the source port are monitored.

both: Indicates that packets transmitted and received by the source port are copied to the destination port for monitoring. If none of **rx**, **tx**, and **both** is selected, **both** is enabled by default.

Configuring a SPAN Destination Port

A SPAN session does not have a SPAN destination port by default. You can run the **monitor session** *session-id* **destination interface** *interface-id* [**encapsulation replicate** | **switch**] command to configure a SPAN destination port.

encapsulation replicate: Forcibly removes tags (VLAN information carried in packets) from packets.

switch: Indicates that the SPAN destination port only receives packets mirrored from the SPAN source port and discards other packets if this option is disabled, and receives both packets mirrored from the SPAN source port and packets from non-source ports if this option is enabled, that is, communication between the destination port and other devices is not affected.

When the SPAN destination port is configured, the relevant function is disabled by default if **encapsulation replicate** or **switch** is not configured.

During SPAN configuration, pay attention to the following points:

- The SPAN destination port participates in STP tree calculation.
- If the VLAN configuration of the source port is changed, the configuration takes effect immediately.
- If the VLAN configuration of the destination port is changed, the configuration takes effect immediately.
- If the source port or destination port is disabled, SPAN will become ineffective.

- When VLAN (VLAN list) is used as the mirroring source, ensure that the destination port has sufficient bandwidth to receive mirroring data from the VLAN.
- Not all devices support all options of the preceding commands.

1.3 Configuration

Configuration	Description and Command	
Configuring SPAN Basic Functions	(Mandatory) It is used to create SPAN.	
	monitor session *session-id* **source interface** *interface-id* [**both | rx | tx**]	Configures a SPAN source port.
	monitor session *session-id* **destination interface** *interface-id*[**switch | encapsulation replicate**]	Configures a SPAN destination port.

1.3.1 Configuring SPAN Basic Functions

Configuration Effect

- Configure source and destination ports for a SPAN session.
- Configure a destination port to monitor any packets transmitted and received by a source port.

Notes

- If the switching function is disabled on a SPAN destination port, the destination port receives only mirrored packets and discards other packets that pass through the port. After the switching function is enabled, the destination port can receive non-mirrored packets.

Configuration Step

Configuring a SPAN Session

- Mandatory.
- Perform this configuration in global configuration mode.
- You can configure a SPAN session when configuring a SPAN source port or destination port, or when configuring a specified VLAN or some VLANs as a data source or data sources of SPAN.

Configuring a SPAN Source Port

- Mandatory.
- Perform this configuration in global configuration mode.
- You can select the SPAN direction when configuring a SPAN source port. **both** is configured by default, that is, both transmitted and received packets are monitored.

Configuring a SPAN Destination Port

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

- A SPAN session is active only when a SPAN source port is configured (or a VLAN is specified as the data source of SPAN) and a SPAN destination port is configured.

Verification

- Run the **show monitor** command or the **show running** command to verify the SPAN configuration. Alternatively, analyze packet obtaining on the SPAN destination port and check whether the SPAN function takes effect based on obtained packets.

Related Commands

Configuring a SPAN Source Port

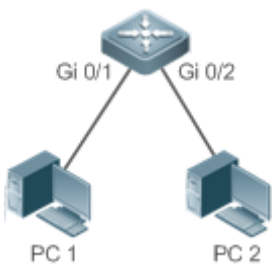
Command	**monitor session** *session-id* **source interface** *interface-id* [**both** | **rx** |**tx**]
Parameter Description	*session-id:* Indicates the ID of a SPAN session. *interface-id:* Indicates the interface ID. **both:** Indicates that packets in the inbound and outbound directions are monitored. It is configured by default. **rx:** Indicates that packets in the inbound direction are monitored. **tx:** Indicates that packets in the outbound direction are monitored.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a SPAN Destination Port

Command	**monitor session** *session-id* **destination interface** *interface-id*[**switch** | **encapsulation replicate**]
Parameter Description	*session-id:* Indicates the ID of a SPAN session. *interface-id*: Indicates the interface ID. **switch:** Indicates that the switching function is enabled on the SPAN destination port. It is disabled by default. **encapsulation replicate:** Indicates that the encapsulation function is enabled on the mirroring port. Mirrored packets are untagged forcibly if this function is enabled. It is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Local Mirroring

Scenario **Figure 1-2**	

Configuration Steps	● As shown in Figure 1-2, add ports Gi 0/1 and Gi 0/2 of Device A to VLAN 1. ● Create SVI 1 and set the address of SVI 1 to 10.10.10.10/24. ● Set IP addresses of PC 1 and PC 2 to 10.10.10.1/24 and 10.10.10.2/24 respectively. ● Configure SPAN for Device A and configure Gi 0/1 and Gi 0/2 as the source port and destination port of SPAN respectively.

A	`Hostname# configure`
	`Hostname(config)# vlan 1`
	`Hostname(config-vlan)# exit`
	`Hostname(config)# interface vlan 1`
	`Hostname(config-if-VLAN 1)# ip address 10.10.10.10 255.255.255.0`
	`Hostname(config-if-VLAN 1)# exit`
	`Hostname(config)# monitor session 1 source interface gigabitEthernet 0/1`
	`Hostname(config)# monitor session 1 destination interface gigabitEthernet 0/2`

Verification	● Run the **show monitor** command to check whether SPAN is configured correctly. After successful configuration, PC 1 sends ping packets to SVI 1 and PC 2 conducts monitoring by using the packet obtaining tool.

A	`Hostname# show monitor`
	`sess-num: 1`
	`span-type: LOCAL_SPAN`
	`src-intf:`
	`GigabitEthernet 0/1 frame-type Both`
	`dest-intf:`
	`GigabitEthernet 0/2`

Common Errors

- The session ID specified during configuration of the SPAN source port is inconsistent with that specified during configuration of the SPAN destination port.
- Packet loss may occur if packets of a port with high bandwidth are mirrored to a port with low bandwidth.

1.4 Monitoring

Displaying

Command	Description
show monitor	Displays all mirroring sessions existing in the system.
show monitor session *session-id*	Displays a specified mirroring session.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Description	Command
debug span	Debugs SPAN.

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 1 millisecond on a LAN and smaller than decades of milliseconds on a WAN). In addition, NTP can prevent attacks by using encrypted acknowledgment.

The device supports the NTP client and NTP server. That is, 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 the 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

In Figure 1-1:

- DEVICE-A is used as a reliable reference clock source to provide time synchronization for external devices.
- On DEVICE-B, DEVICE-A is used as the NTP server and synchronizes time with DEVICE-A.
- DEVICE-B provides time synchronization for DEVICE-C after successful synchronization.

Figure 1-1



Deployment

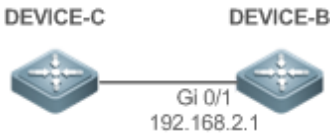
Configure DEVICE-B to work in NTP external reference clock mode.

1.2.2 Synchronizing Time Based on the 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 work in NTP local reference clock mode.

1.3 Features

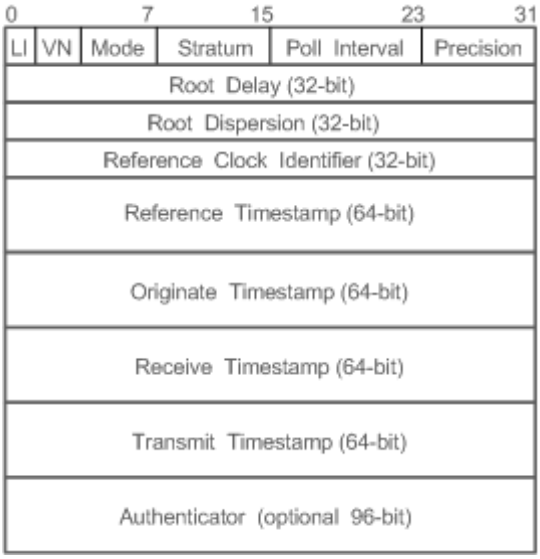
Basic Concepts

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.

The value 00 indicates no warning information; the value 01 indicates that there are 61 seconds in the previous minute; the value 10 indicates that there are 59 seconds in the previous minute; the value 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.

The value 0 indicates that the field is not defined; the value 1 indicates symmetric active; the value 2 indicates symmetric passive; the value 3 indicates a client; the value 4 indicates a server; the value 5 indicates broadcast; the value 6 indicates control information; the value 7 is reserved.

- Stratum: indicates the 8-bit stratum of a local clock. The value 0 indicates that the field is not defined; the value 1 indicates the master reference clock source; other values indicate slave reference clock sources.
- Poll Interval: indicates the poll interval, in seconds. The value is an 8-bit integer.
- Precision: indicates the time precision of a local clock, in seconds. The value is an 8-bit integer.
- Root Delay: indicates the round-trip time (RTT) 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 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 on a network.

NTP Client

A device is used as an NTP client that synchronizes time with an NTP server on a network.

Stratum

In NTP, the stratum is used to describe the number of 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	Allows network devices to synchronize time with their servers or reliable clock sources to implement high-precision time correction.
NTP Authentication	Uses NTP packet encryption and authentication to protect unreliable clock sources against time synchronization interference on a device.
NTP Access Control	Filters sources of received NTP packets based on an Access Control List (ACL).

1.3.1 NTP Time Synchronization

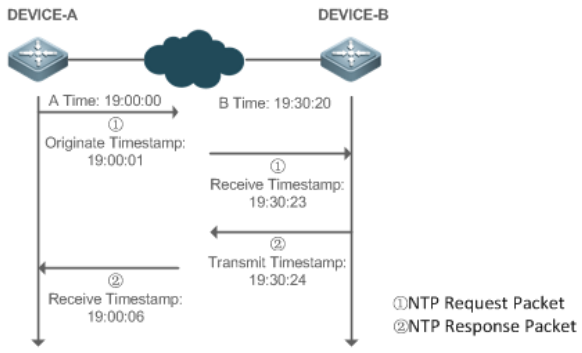
Working Principle

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.

Figure 1-4 shows the format of an NTP time synchronization packet.

Figure 1-4 Working Principle of NTP



DEVICE-B is used as an NTP reference clock source, DEVICE-A is used as an NTP client that synchronizes time with DEVICE-B. At a time point, the local clock of DEVICE-A is 19:00:00 and the local clock of DEVICE-B is 19:30:20.

1 DEVICE-A sends an NTP request packet. The local time (T0) when the packet leaves from DEVICE-A is 19:00:00 and is filled in Originate Timestamp.

2 After a 2-second network delay, the local time (T1) when DEVICE-B receives the request packet is 19:30:23 and is filled in Receive Timestamp.

3 DEVICE-B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from DEVICE-B is 19:30:24 and is filled in Transmit Timestamp.

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

Calculation for time synchronization is as follows:

- DEVICE-A obtains the time difference of 30 minutes and 20 seconds between DEVICE-B and DEVICE-A by using the formula ((T1-T0)+(T2-T3))/2.

- DEVICE-A obtains the packet round-trip delay of 4s between DEVICE-A and DEVICE-B by using the formula (T3-T0)-(T2-T1).

NTP Working Mode

- External clock reference mode

A device is used as both a server and a client. When 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

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), that is, NTP is enabled.
- Then the device works in external clock reference mode.

Performing 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 external clock reference mode.
- Run the **ntp master** command to configure a device to work in local clock reference mode.

1.3.2 NTP Authentication

To prevent malicious damage on an NTP server, NTP uses the authentication mechanism to check whether time synchronization information is originated from the announced server and check the information return path to protect the device against interference.

Working Principle

An NTP client and an NTP server are configured with the same key. When sending request and response packets, a device calculates hash values of the packets by using the MD5 or HMAC-SHA256 algorithm based on the specified key and NTP packet content, and fills hash values into packet authentication information. The device receiving the packets checks whether the packets are sent by a trusted device or modified based on the authentication information.

Related Configuration

Configuring a Global Authentication Mechanism

- By default, no NTP authentication mechanism is enabled.
- Run the **ntp authenticate** command to enable the NTP authentication mechanism.

Configuring a Global Authentication Key

- By default, no global authentication key is configured.
- Run the **ntp authentication-key** command to configure an NTP global authentication key.

Configuring a Globally Trusted Key ID

- 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.

1.3.3 NTP Access Control

Working Principle

An ACL provides the minimum security measure.

Related Configuration

Configuring Access Control Rights for NTP Services

- By default, there is no access control right for NTP.
- Run the **ntp access-group** command to configure 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 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 work in local clock reference mode.	
	ntp master	Configures the NTP master clock.
	(Optional) It is used to configure the local clock reference mode for the device.	
	ntp interval	Configures the interval for time synchronization between the NTP client and the NTP server.

Configuration	Description and Command	
	(Optional) It is used to disable NTP.	
	no ntp	Disables all functions of NTP and clears all NTP configurations.
	ntp disable	Disables the device from receiving NTP packets from a specified interface.
	ntp service disable	Disables the NTP time synchronization service.
Configuring NTP Authentication	(Optional) It is used to protect the device gaaisnt interference by unreliable clock sources.	
	ntp authenticate	Enables an 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 sources of received NTP packets.	
	ntp access-group	Configures 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 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 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 on 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 does not synchronize 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.

Configuration Step

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 Between the NTP Client and the NTP Server

- 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.

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 from Providing 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 as a client, configure the **ntp service disable** command to disable the NTP device from providing 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 or IPv6 address of the reference clock source. *domain*: Indicates the IPv4 or IPv6 domain name of the reference clock source. *version*: Indicates the NTP version number. The value is 1, 2, or 3. *interface*: Indicates the interface type, including aggregate interface, dialer GigabitEthernet interface, loopback interface, multi-link interface, null interface, tunnel interface, virtual PPP interface, virtual template interface, and VLAN interface. *keyid*: Indicates the key used for encrypted communication with the corresponding server. It is not encrypted by default. The value range is from 1 to 4294967295. **prefer**: Indicates whether the reference clock source has a high priority.
Command Mode	Global configuration mode
Usage Guide	By default, no NTP server is configured. The client supports interaction with up to 20 NTP servers. You can configure an authentication key for each server (after configuring global authentication and the key) to initiate encrypted communication with the servers. ⚠ If it is necessary to configure an authentication key, you must configure NTP 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 range is from 10 to 2592000. The default value is 64.
Command Mode	Global configuration mode
Usage Guide	The default NTP time synchronization interval is 64s.

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. The value range is 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 rapidly disable all functions of NTP and clear all NTP configurations.

Disabling the Device from Receiving 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 from Providing 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).

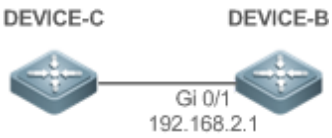
Configuration Example

Configuring the External Clock Reference Mode of NTP

Scenario Figure 1-5	
	● DEVICE-B is configured to work in 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	● Configure the local clock as the NTP reference clock source on DEVICE-A. ● Configure DEVICE-A as the reference clock source on DEVICE-B. ● Configures DEVICE-B as the reference clock source on DEVICE-C.
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.

↘ Configuring the Local Clock Reference Mode of NTP

Scenario **Figure 1-6**	
	● The local clock is used as the NTP reference clock source on DEVICE-B. ● DEVICE-C synchronizes time with DEVICE-B.
Configuration Steps	● Configure the local clock as the NTP reference clock source on DEVICE-B. ● Configure DEVICE-C to synchronize time with DEVICE-B.
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 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 Step

Configuring the Global Authentication Mechanism

- Mandatory.
- By default, the security authentication mechanism is disabled.

Configuring a Global Authentication Key

- Mandatory.
- By default, a device is not configured with an authentication key.

Configuring a Globally Trusted Key ID

- 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 the Authentication Mechanism

Command	**ntp authenticate**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, a client does not use the global authentication mechanism. If no authentication mechanism is used, communication will not be encrypted. A global security indicator is not enough to imply that communication between the client and server is implemented in an encrypted manner. Other global keys and an encryption key for the server must be configured for initiating encrypted communication between the client and server.

Configuring a Global Authentication Key

Command	**ntp authentication-key** *key-id* { **hmac-sha256** | **md5** } *key-string* [*enc-type*]
Parameter Description	*key-id*: Indicates the ID of a global authentication key. The value range is from 1 to 4294967295. **hmac-sha256**: Specifies the HMAC-SHA256 authentication algorithm. **md5**: Specifies the MD5 authentication algorithm. *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*: Indicates whether an entered key is encrypted. The value 0 indicates no encryption, and the value 7 indicates simple encryption. The default value is 0.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key

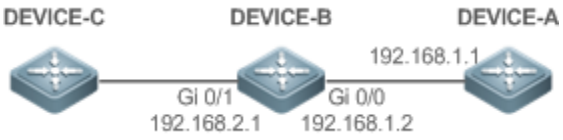
Command	**ntp trusted-key** *key-id*
Parameter Description	*key-id*: Indicates the ID of a trusted key. The value range is from 1 to 4294967295.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring a Trusted Key for an External Reference Clock Source

Refer to Related Commands

Configuration Example

Configuring NTP Authentication

Scenario Figure 1-7	
	● DEVICE-B is configured to work in NTP client/server mode and provides NTP services requiring 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	● Configure DEVICE-A as the reference clock source on DEVICE-B. ● Configure DEVICE-B as the reference clock source on DEVICE-C.

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 the minimum security measure. A more secure method is to use an NTP authentication mechanism.

Notes

- The system does not support control query (used to control NTP servers by using network management devices, for example, setting the leap second indicator or monitoring its working status).
- 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.

Configuration Step

↘ Configuring Access Control Rights for NTP

- Optional.
- Run the **ntp access-group** command to configure access control rights and a corresponding ACL for NTP.

Verification

Run the **show run** command to verify the NTP configuration.

Related Commands

↘ Configuring 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 requests for local NTP services. **query-only**: Allows only control query for local NTP services. *access-list-number*: Indicates the number of an IP ACL. The value range is from 1 to 99 and from 1300 to 1999. For details about how to create an IP ACL, see *Configuring ACL*.

	access-list-name: Indicates the name of an IP ACL. For details about how to create an IP ACL, see *Configuring ACL*.
Command Mode	Global configuration mode
Usage Guide	Configure NTP access control rights. When an access request arrives, the NTP-enabled device matches the request against 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 at 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

Command	Description
show ntp server	Displays NTP server information.
show ntp status	Displays NTP information.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug ntp	Enables debugging.
no debug ntp	Disables debugging.

1 Configuring SNTP

1.1 Overview

The Simple Network Time Protocol (SNTP) is a simplified version of the Network Time Protocol (NTP), which is used to synchronize 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. Typically, SNTP precision can reach about 1s, which meets basic requirements of most scenarios. Because 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.

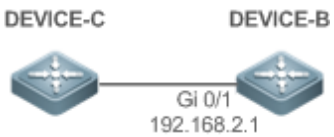
1.2.1 Synchronizing Time with an NTP Server

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

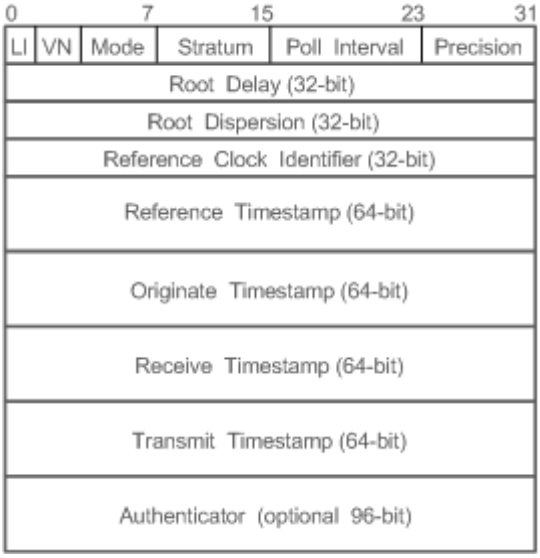
SNTP Packet

SNTPv4 is developed based on NTP, which is intended to simplify functions of NTP. It does not change the NTP specifications and implementation of NTP. The packet format of SNTPv4 is the same as that of NTP defined in RFC 1305, with only some data fields initialized into preset values.

As defined in RFC 1305, 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.

The value 00 indicates no warning information; the value 01 indicates that there are 61 seconds in the previous minute; the value 10 indicates that there are 59 seconds in the previous minute; the value 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.

The value 0 indicates that the field is not defined; the value 1 indicates symmetric active; the value 2 indicates symmetric passive; the value 3 indicates a client; the value 4 indicates a server; the value 5 indicates broadcast; the value 6 indicates control information; the value 7 is reserved.

- Stratum: indicates the 8-bit stratum of a local clock. The value 0 indicates that the field is not defined; the value 1 indicates the master reference clock source; other values indicate slave reference clock sources.
- Poll Interval: indicates the poll interval, in seconds. The value is an 8-bit integer.
- Precision: indicates the time precision of a local clock, in seconds. The value is an 8-bit integer.
- Root Delay: indicates the round-trip time (RTT) 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.

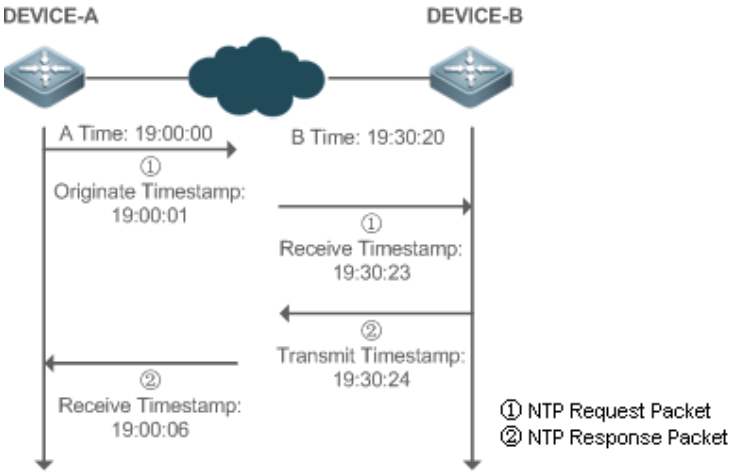
1.3.1 SNTP Time Synchronization

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 is used as an NTP reference clock source, DEVICE-A is used as an SNTP client that synchronizes time with DEVICE-B. At a time point, the local clock of DEVICE-A is 19:00:00 and the local clock of DEVICE-B is 19:30:20.

- DEVICE-A sends an SNTP/NTP request packet. The local time (T0) when the packet leaves from DEVICE-A is 19:00:00 and is filled in Originate Timestamp.
- After a 2-second network delay, the local time (T1) when DEVICE-B receives the request packet is 19:30:23 and is filled in Receive Timestamp.
- DEVICE-B processes the NTP request and sends an NTP response packet one second later. The local time (T2) when the response packet leaves from DEVICE-B is 19:30:24 and is filled in Transmit Timestamp.

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

The specific calculations for time synchronization are as follows:

- DEVICE-A obtains the time difference of 30 minutes and 20 seconds between DEVICE-B and DEVICE-A by using the formula ((T1-T0)+(T2-T3))/2.
- DEVICE-A obtains the packet round-trip delay of 4s between DEVICE-A and DEVICE-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 **sntp 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 connects to 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 Step

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 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** command in 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	Because SNTP is fully compatible with NTP, the server can be configured as a public NTP server on the Internet. Because 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.

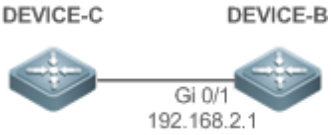
Configuring the SNTP Time Synchronization Interval

Command	**sntp interval** *seconds*
Parameter Description	*seconds*: Indicates the time synchronization interval, in seconds. The value range is from 60 to 65,535. The default value is 1800s.

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

Configuring SNTP Time Synchronization

Scenario Figure 1-4	
	● DEVICE-B is 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

Command	Description
show sntp	Displays SNTP parameters.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug sntp	Enables debugging.

1 Configuring FTP Server

1.1 Overview

The device can be configured as the File Transfer Protocol (FTP) server to connect to an FTP client. Then the FTP client can upload files to and download files from the FTP server through FTP.

You 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

- RFC 959: FILE TRANSFER PROTOCOL (FTP)
- RFC 3659: Extensions to FTP
- RFC 2228: FTP Security Extensions
- RFC 2428: FTP Extensions for IPv6 and NATs
- RFC 1635: How to Use Anonymous FTP

1.2 Applications

Application	Description
Providing FTP Services on a LAN	The device provides file upload and download services for a user on a Local Area Network (LAN).

1.2.1 Providing FTP Services on a LAN

Scenario

Provide file upload and download services for a user on a LAN.

As shown in Figure 1-1, enable the FTP server only on a LAN.

- G is enabled with the FTP server function and S is enabled with Layer 2 transparent transmission.
- A user initiates a request for FTP upload and downloa services.

Figure 1-1



Remarks	S is an access device.

Deployment

- G is enabled with the FTP server.
- As a Layer 2 device, S provides 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 resources for free through anonymous FTP. In addition, FTP provides functions such as login, directory query, file operation, and session control. Among the TCP/IP protocol suite, 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 RFC 959.

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 two 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 the 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, the binary mode facilitates faster transfer of all files and reliable transfer of ASCII files.

FTP Working Modes

FTP provides two working modes:

Figure 1-2

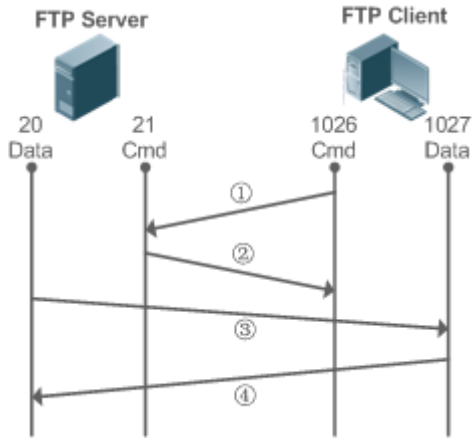
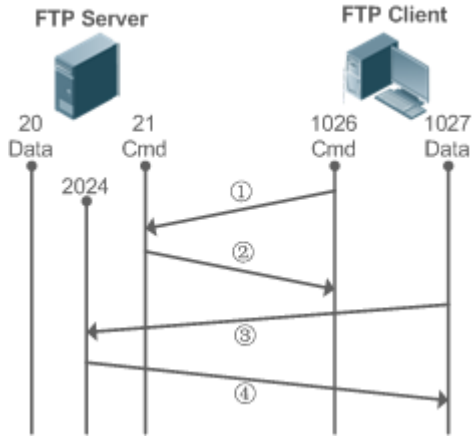


Figure 1-3



- 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 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 PORT mode. However, after the connection is established, the client sends the **PASV** command but not the **PORT** command. After receiving the **PASV** command, the FTP server enables high-end port 2024at 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 authentication, FTP client commands can be executed. 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 details of FTP client commands, see the FTP client software document. In addition, many FTP client tools such as CuteFTP and FlashFXP provide the graphic user interface (GUI), which simplifies operations by eliminating the need for users to configure FTP commands.

Overview

Feature	Description
Enabling the FTP Server Function	Provides functions of uploading, downloading, displaying, creating, and deleting files for an FTP client.

1.3.1 Enabling the FTP Server Function

Working Principle

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 the User Name, Password, and Top-Level Directory

There is no authorized user or top-level directory by default.

Run the **ftp-server username password** and **ftp-server topdir** commands to configure the authorized user and top-level directory.

The user name, password, and top-level directory must be configured; 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 the login timeout for an FTP session.
	ftp-server login times	Configures the valid login count.

Configuration	Description and Command	
	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 must be configured.
- To enable the server to close an abnormal session within a limited period, configure the idle timeout of a session.

Configuration Step

Enabling the FTP Server Function

- Mandatory.
- Unless otherwise specified, enable the FTP server function on each device.

Configuring the Top-Level Directory

- Mandatory.
- Unless otherwise specified, configure the top-level directory as the root directory on each device.

Configuring the 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 a client is disconnected from the server due to an error or other 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 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 FTP server function for the first time.

Configuring the Valid Login Count

Command	**ftp-server login times** *times*
Parameter Description	*times:* Indicates the valid login count. The value range is 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** *time*
Parameter Description	*time*: Indicates the login timeout, in minutes. The value range is from 1 to 30.
Command Mode	Global configuration mode
Usage Guide	The login timeout refers to the maximum duration that the session lasts since the session has been established. If you do not pass 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 the User Name and Password for Server Login

Command	**ftp-server username** *username* **password** [**0** | **7**] *password*

Parameter Description	*username*: Indicates a user name. **0**: Indicates that the password is not encrypted (cleartext) . **7**: Indicates that the password is encrypted (ciphertext). *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 in the password are viewed as part of the password. A cleartext password consists of 1 to 25 characters; a ciphertext 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, in minutes. The value range is from 1 to 3600.
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, a file is completely transferred), the server starts to count the idle time again, and stops when the next FTP client command operation is being performed. Therefore, the idle timeout has no effect on some time-consuming file transfer operations.

Displaying the FTP Server Status

Command	**show ftp-server**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Run this command to display the 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 or error events of the FTP server.

Configuration Example

The following configuration example is related to the FTP server only.

Creating an FTP Server on an IPv4 Network

Scenario	● A TCP connection is established from a server to a client.
Configuration Steps	● Enable the FTP server function. ● Configure the top-level directory or 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# showRuijie#sho ftp-server`
	`    ftp-server information`
	`==================================`
	`enable : Y`
	`topdir : tmp://`
	`timeout: 130min`
	`username:aaaa          config : Y`
	`password:(PLAINT)bbbb         connect num[2] config : Y`
	`    [0]trans-transfer 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]control connection : N`
	`port data connection : N`
	`passive data connection : N`
	`Ruijie#`

Common Errors

- No user name is configured.

- No password is configured.
- No top-level directory is configured.

1.5 Monitoring

Displaying

Command	Description
show ftp-server	Displays the FTP server configuration.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug ftp-server err	Debugs FTP server error events.
debug ftp-server pro	Debugs FTP server message events.

1 Configuring FTP Client

1.1 Overview

The File Transfer Protocol (FTP) is an application of the Transmission Control Protocol/Internet Protocol (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 FTP. A user uses the client to send a command to the server. The server responds to the command and sends the execution result to the client. By means of command interaction, the user can view files in the server directory, copy files from a remote computer to a local computer, or transfer local files to a remote computer.

FTP is designed to facilitate sharing of program or data files and enable remote operations through programs. Users do not need to worry about differences in files systems across different hosts. Data is transmitted efficiently and reliably, allowing for secure remote file operations.

The device used as the FTP client is different from the standard FTP client that run interactive commands. Instead, you enter the **copy** command in the 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.

Original devices support TFTP. However, TFTP is used to transfer small files. FTP is used to transfer large files. Implementing FTP on a device enables the file transfer between the device and other clients or servers.

Protocols and Standards

- RFC 959: FILE TRANSFER PROTOCOL (FTP)

1.2 Applications

Application	Description
Uploading a Local File to a Remote Server	Local and remote server 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 server 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 upload on the FTP client.
- Enable file upload 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.

In Figure 1-2, resources are shared only on the Intranet.

Figure 1-2



Deployment

- Implement only communication on the intranet.
- Enable file download on the FTP client.
- Enable file download 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 active or passive mode.

FTP Transmission Mode

The transmission between an FTP client and an FTP server is available in two modes, namely, ASCII and binary modes.

Specifying the Source Interface's IP Address for FTP Transmission

An FTP client is configured with a source interface's 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's IP Address for FTP Transmission	Configures a source IP address of an FTP client for communication with an FTP server.

1.3.1 Uploading FTP Files

FTP enables file upload. Start both the FTP client and FTP server, and upload files from the FTP client to the FTP server.

1.3.2 Downloading FTP Files

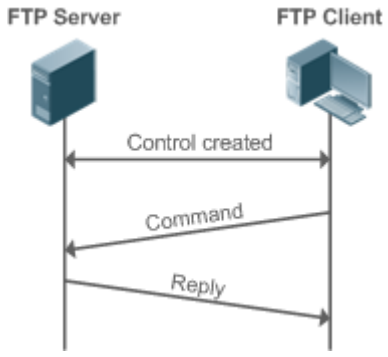
FTP enables file download. Start both the FTP client and FTP server, and download files from the FTP server to the FTP client.

1.3.3 FTP Connection Mode

FTP needs to use two TCP connections: control link (command link) that is used to transfer commands between the FTP client and server, and data link that is used to upload or download data.

1. Control connection: Only control connections need to be established for some simple sessions. 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.

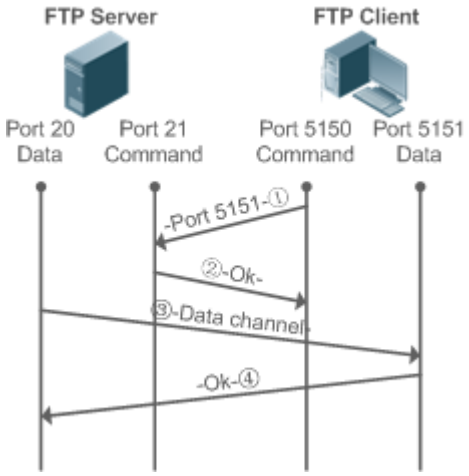
FTP supports two data connection modes: active (PORT) and passive (PASC). The two modes are different in establishing a data connection.

- Active mode

In this mode, an FTP server connects to an FTP client proactively when a data connection is established. This mode involves four steps:

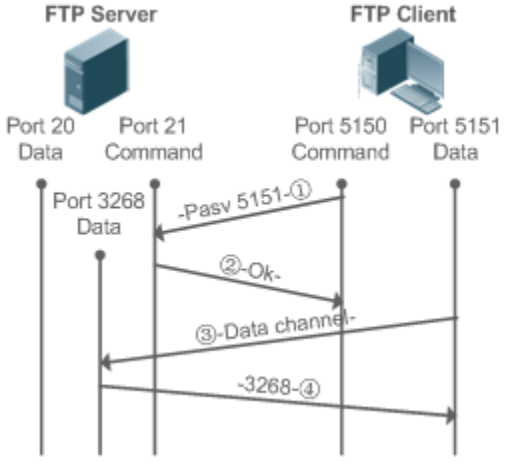
1. The client uses source port 5150 to communicate with the server through port 21 to send a connection request and to notify the server that the port to be used is port 5151.
2. After receiving the request, the server sends a response OK (ACK). The client and server exchanges control signaling by console 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.

Figure 1-4 PORT Mode



- Passive mode

Figure 1-5 PASV (Passive) 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 involves four steps:

1. In passive mode, a client initializes a 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 notifies the client of the port number.
3. After receiving the message, the client uses port 5151 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).

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 active, 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 initiates a command to establish a data connection. The device used as the FTP client works in PASV mode by default.

1.3.4 FTP Transmission Mode

FTP provides two transmission modes: ASCII and binary. The device used as the FTP client 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. In Windows, this file has no line feeds and displays many black squares. Therefore, the binary mode facilitates faster transfer of all files and more reliable transfer of ASCII files.

1.3.5 Specifying the Source Interface's IP Address for FTP Transmission

An FTP client is configured with a source interface's 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 the FTP server that does not support file size response to FTP clients.

1.4 Configuration

Configuration	Description and Command	
Configuring Basic Functions	(Mandatory) It is used to configure the FTP client function.	
	copy flash	Uploads a file.
	copy ftp	Downloads a file.

Configuration	Description and Command	
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	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.

1.4.1 Configuring Basic Functions

Configuration Effect

- Implement file upload and download.

Notes

- Pay attention to command formats for uploading and downloading.

Configuration Step

Uploading a File

- Mandatory.
- Perform this configuration when a file needs to be uploaded.
- Configure the FTP URL as the destination address of **copy** in privileged EXEC mode.

Downloading a File

- Mandatory.
- Perform this configuration 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. The value consists of no more than 32 bytes, excluding delimiters such as /, : and space. This parameter is mandatory. *password:* Specifies a password for accessing the FTP server. The value consists of no more than 32 bytes, 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. Executing 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 memory 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. The value consists of no more than 32 bytes, excluding delimiters such as /, : and space. This parameter is mandatory. *password:* Specifies a password for accessing the FTP server. The value consists of no more than 32 bytes, 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. Executing 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 memory 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 **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 memory.

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

- Configure connection and transmission modes and configure a source interface's IP address of the client for file upload and download.

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 Interface's IP Address of the FTP Client

- Optional.
- Configure the source interface's IP address of the FTP client.

In global configuration mode, the **ftp client source** command is used to configure the source interface and source interface's IP address. The original **ftp client soure-address** command is abandoned and hidden. If the **ftp client soure-address** command is used, it is identified as a new configuration command and is saved.

Restoring Default Settings

- Optional.
- Restore 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 port**
Parameter Description	
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 Interface's IP Address of the FTP Client

Command	**ftp-client source** { *ip-address* | *ipv6-address* | *interface-type interface-number* }
Parameter Description	*ip-address:* Specifies the IPv4 address of a local interface. *ipv6-address:* Specifies the IPv6 address of a local interface. *interface-type interface-number*: Specifies a source interface of a client.
Command Mode	Global configuration mode
Usage Guide	Run this command to configure an interface's IP address of the client for connection with the server. By default, the client is not configured with a local IP address. Instead, the IP address is selected for the client based on the route.

Setting the Transmission Mode to ASCII

Command	**ftp-client ascii**
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	Run this command to set the transmission mode to ASCII. The default transmission mode is binary.

Restoring Default Settings

Command	**default ftp-client**
Parameter Description	
Command Mode	Global configuration mode
Usage Guide	Run this command to restore default settings, namely, connection mode set to passive (PASV), transmission mode to binary, and source IP address removed.

Configuration Example

Configuring Optional Functions

Configuration Steps	● Set the connection mode of FTP to PORT ● Set the transmission mode to ASCII.

	● Set the source IP address to 192.168.23.167.

	`Hostname# configure terminal`
	`Hostname(config)# ftp-client ascii`
	`Hostname(config)# ftp-client port`
	`Hostname(config)# ftp-client source 192.168.23.167`
	`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 192.168.23.167`
	`!`

Common Errors

- The source IP address is not a local IP address.

1.5 Monitoring

Displaying

Command	Description
show running-config	Displays the FTP client configuration.

Debugging

⚠ Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug ftp-client	Debugs the FTP client.

1 Configuring TFTP Server

1.1 Overview

You can configure the device as the Trivial File Transfer Protocol (TFTP) server. Then a TFTP client can be connected to the TFTP server to upload files to or download files from the device.

You can easily obtain files such as upgrade package files from the device or copy files to the file system of the device functioning as the TFTP server.

Protocols and Standards

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

1.2 Applications

Application	Description
Providing the TFTP Service on a LAN	The device provides file upload and download for users on a local area network (LAN).

1.2.1 Providing the TFTP Service on a LAN

Scenario

Enable users in a LAN to upload and download files.

In Figure 1-1:

- Device G serves as a TFTP server.
- The user sends a TFTP upload or download request.

Figure 1-1



Deployment

- Enable the TFTP server on device G.
- The user uploads files to or download files from device G.

1.3 Features

Basic Concepts

TFTP

TFTP, defined by the IETF Network Working Group, works at the application layer. Based on the User Datagram Protocol (UDP), TFTP is a simple protocol to transfer files. TFTP provides only the file uploading and downloading functions instead of many common FTP functions. It does not support the directory list and the authentication function, and does not provide any security mechanism. TFTP uses the way of acknowledged retransmission upon timeout to ensure data transmission, which covers three transmission modes: netascii in the form of an 8-bit ASCII code, 8-bit octet of the source data type, and mail (which is no longer supported). TFTP uses UDP port 69. TFTP is defined in RFC 1350.

TFTP Packet

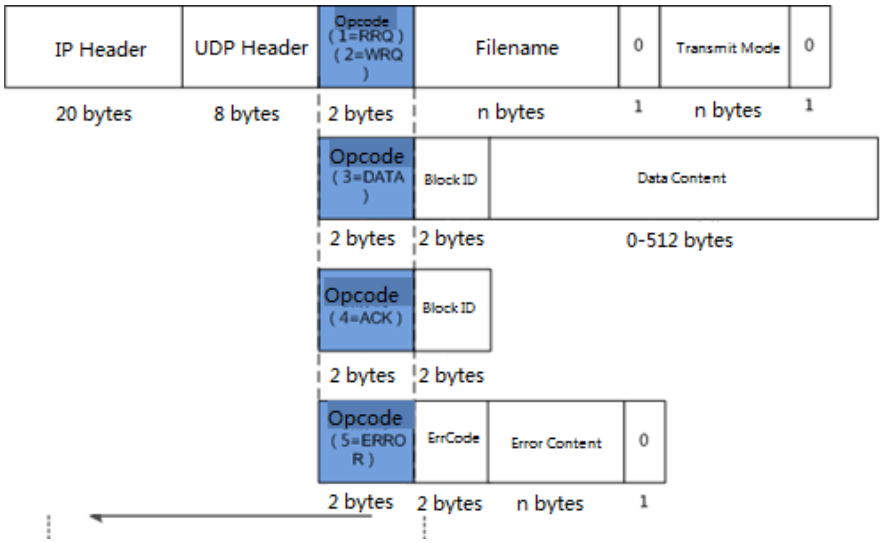
Any transfer begins with a request to read or write a file from a TFTP client. After the TFTP server grants the request, the file is sent in fixed-length blocks of 512 bytes. A data packet of less than 512 bytes indicates the termination of a transfer.

Each data packet contains a block of data, and must be acknowledged by an acknowledgement packet before the next data packet can be sent. If no acknowledgement packet is received within specified time, the last sent data packet is retransmitted.

The TFTP packet header includes an opcode field, which indicates the packet type. TFTP supports the following five types of packets:

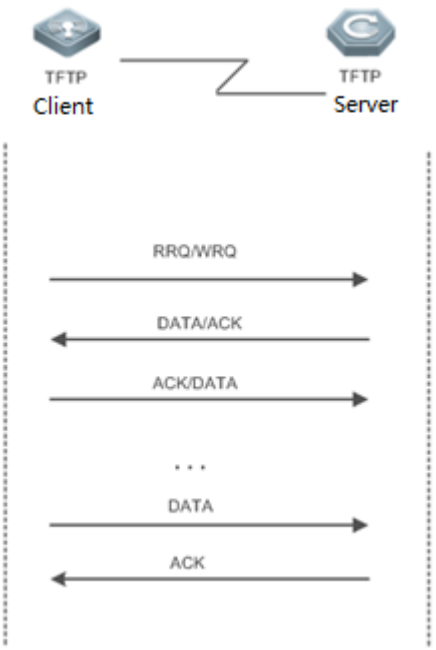
- Read Request (RRQ)
- Write Request (WRQ)
- Data
- Acknowledgment (ACK)
- Error

Figure 1-2



Working Principle

Figure 1-3



- The TFTP client initiates an RRQ or WRQ to the TFTP server.
- Upon receipt of the RRQ, the TFTP server first determines whether the read condition is met (for example, whether the file exists or whether the client has the access permission), and returns a data packet to the TFTP client if the condition is met. Upon receipt of the WRQ, the TFTP server first determines whether the write condition is met (for example, whether there is a sufficient space or whether the client has the write permission), and returns an ACK packet to the TFTP client if the condition is met.
- The TFTP client receives the data packet in the case of file downloading, and replies with an ACK packet; or receives the ACK packet in the case of file uploading, and then sends a data packet.
- The process of transmission acknowledgement repeats till the last DATA packet is less than 512 bytes, which indicates the end of transmission.
- If errors occur during transmission, an error packet is returned.

Overview

Feature	Description
Enabling the TFTP Server Function	Provides the TFTP client with file uploading and downloading functions.

1.3.1 Enabling the TFTP Server Function

Working Principle

After the TFTP server function is enabled on the device, configure a top directory so that the TFTP service is available for users.

Related Configuration

Enabling the TFTP Server Function

- By default, the TFTP server function is disabled.
- Run the **tftp-server enable** command to enable the TFTP server function.

Configuring the Top Directory

- The default top directory is **flash:**.
- Run the **tftp-server topdir** command to configure the top directory.

1.4 Configuration

Configuration	Description and Command	
Basic Functions	(Mandatory configuration) It is used to enable the TFTP server function.	
	tftp-server enable	Enables the TFTP server function.
	tftp-server topdir	Configures the top directory of the TFTP server.

1.4.1 Basic Functions

Networking Requirements

- Enable the TFTP server function on the device to allow the connected TFTP client to upload and download files.

Notes

- The top directory needs to be configured.

Configuration Step

Enabling the TFTP Server Function

- Mandatory.
- Unless otherwise specified, enable the TFTP server function on each device.

Configuring the Top Directory

- Mandatory.
- Unless otherwise specified, configure a top directory as the root directory on each device.

Verification

Connect the TFTP server to the TFTP client.

- Check whether the client is connected to the server.
- Check whether the client can normally download files from and upload files to the server.

Related Commands

Enabling the TFTP Server Function

Command	**tftp-server enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	The client cannot access the TFTP server before a top directory is correctly configured for the server. Therefore, it is recommended that you configure the top directory of the server first if it is the first time for you to enable the TFTP server. For details about how to configure the top directory, see the following configuration.

Configuring the Top Directory of the TFTP Server

Command	**tftp-server topdir** *directory*
Parameter Description	*directory*: Indicates the access path.
Command Mode	Global configuration mode
Usage Guide	For example, you can set the top directory of the server to **/dir**. Then the TFTP client can access files and folders in the **/dir** directory only on the device after logging in, and the TFTP client cannot return to the parent directory of the **/dir** directory due to restrictions of the top directory.

Enabling TFTP Server Debugging

Command	**debug tftp-server**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	You can run this command to enable TFTP server debugging, so that process or error information of the TFTP server can be output as necessary.

Displaying the Download Progress of a Client

Command	**show tftp-server updating-list**
Parameter Description	N/A
Command Mode	All modes except user mode
Usage Guide	The command is used to display the download progress of a TFTP client, excluding its completed download.

Configuration Example

Establishing the TFTP Server Function on an IPv4 Network

Scenario	• Enable the TFTP server function. • Set the top directory of the TFTP server to **/dir**.
	`Hostname(config)#tftp-server topdir /tmp`

	`Hostname(config)#tftp-server enable`

Verification	● Run the **show tftp-server** command to display the configuration.
	`Hostname#show tftp-server`
	`…`
	`tftp-server information`
	`==========`
	`enable : Y`
	`topdir : tmp:/`

Common Errors

No top directory is configured.

1.5 Monitoring

Displaying

Command	Function
show tftp-server	Displays the configuration of the TFTP server.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Function
debug tftp-server	Enables TFTP server debugging.
show tftp-server updating-list	Displays the download progress of a client.

1 Configuring TFTP Client

1.1 Overview

The Trivial File Transfer Protocol (TFTP) is an application of the Transmission Control Protocol/Internet Protocol (TCP/IP). File transfer between the TFTP client and server is implemented based on the User Datagram Protocol (UDP). Compared with TCP-based FTP, 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 large file transfer.

Protocols and Standards

- RFC 783: 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 Figure 1-1, 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 Figure 1-2, 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's 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	Uploads a file from the TFTP client to the TFTP server.
Downloading a File Using TFTP	Downloads a file from the TFTP server to the TFTP client.

Feature	Description
Specifying the Source Interface's IP Address for TFTP Transmission	Specifies the source IP address for the TFTP client to communicate with the TFTP server.
Specifying the Port Number for a Connection with the TFTP Server	Specifies 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's IP Address for TFTP Transmission

You can configure the source IP address for the TFTP client to connect to and share files with the TFTP server.

1.3.4 Specifying the Port Number for a 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 function.	
	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 establishing a TFTP connection.
	tftp-client port	Configures the port number used by the TFTP client to connect to 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 Step

Uploading a File

- Mandatory.
- Configure TFTP-related Uniform Resource Locators (URLs) for the destination address under **copy** in privileged EXEC mode.

Downloading a File

- Mandatory.
- Configure 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*: Indicates the directory on the local device. If no directory is specified, the current directory is used. *local-file*: Indicates the name of the local file to be operated. *dest-address*: Indicates the IP address of the TFTP server. *remote-directory*: Indicates the directory on the TFTP server. *remote-file*: Indicates the name of the file to be operated on the TFTP server. ⚠ The directory specified by *local-directory* must already exist on the device. Running 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*: Indicates the IP address of the TFTP server. *remote-directory*: Indicates the directory on the TFTP server. *remote-file*: Indicates the name of the file to be operated on the TFTP server. *local-directory*: Indicates the directory on the local device. If no directory is specified, the current directory is used. *local-file*: Indicates the name of the local file to be operated. ⚠ The directory specified by *local*-directory must already exist on the device. Running this command does not automatically create a directory.
Command	Global configuration mode

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 at 192.168.23.69 and rename the file **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 at 192.168.23.69 to the **flash** directory of the device and rename it **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 Establishing a TFTP Connection

- Optional.
- Configure the source IP address of the TFTP client used for establishing a TFTP connection.

Configuring the Port Number Used by the TFTP Client to Connect to the TFTP Server

- Optional.
- Configure the port number used by the TFTP client to connect to the TFTP server.

Verification

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

Related Commands

Configuring the Source IP Address for Establishing a TFTP Connection

Command	**tftp-client source** { **ip** *ip-address* | **ipv6** *ipv6-address* | *interface-type interface-number* }
Parameter Description	*ipv6*-address: Indicates the IPv6 address of the local interface. *ip-address*: Indicates the 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 to 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 to the TFTP Server

Command	**tftp-client port** *port-number*
Parameter Description	*port*-number: Indicates the 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 to the TFTP server.

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show running-config	Displays the TFTP client configuration.

Debugging

Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug tftp	Debugs the TFTP client.

1 Configuring SNMP

1.1 Overview

The Simple Network Management Protocol (SNMP), established as a network management standard in August 1988 by RFC 1157, is widely supported by various vendors. It has since become a universal standard for managing networks across heterogeneous environments. SNMP enables network administrators to perform essential functions including querying network node information, configuring networks, locating faults, planning capacity, and monitoring and managing networks.

↘ SNMP Versions

The following SNMP versions are supported:

- SNMPv1: The first official version of SNMP is defined in RFC 1157.
- SNMPv2C: The community-based SNMPv2 management architecture is defined in RFC 1901.
- SNMPv3: SNMPv3 provides the following security features by identifying and encrypting data.

1 Ensures that data is tampered-resistant during transmission.

2 Ensures that data is transmitted from valid data sources.

3 Encrypts packets and ensures data confidentiality.

Protocols and Standards

- RFC 1157, Simple Network Management Protocol (SNMP)
- RFC 1901, Introduction to Community-based SNMPv2
- RFC 2578, Structure of Management Information Version 2 (SMIv2)
- RFC 2579, Textual Conventions for SMIv2
- RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
- RFC 3412, Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
- RFC 3413, Simple Network Management Protocol (SNMP) Applications
- RFC 3414, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
- RFC 3415, View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
- RFC 3416, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
- RFC 3417, Transport Mappings for the Simple Network Management Protocol (SNMP)
- RFC 3418, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
- RFC 3419, Textual Conventions for Transport Addresses

1.2 Applications

Application	Description
Managing Network Devices Based on SNMP	Network devices are managed and monitored based on SNMP.

1.2.1 Managing Network Devices Based on SNMP

Scenario

In Figure 1-1, network device A is managed and monitored based on SNMP network manager.

Figure 1-1



Remarks	Device A is a network device that needs to be managed. The PC is a network management station.

Deployment

The network management station is connected to 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 proactively sent by the network devices to manage and monitor the network devices.

1.3 Features

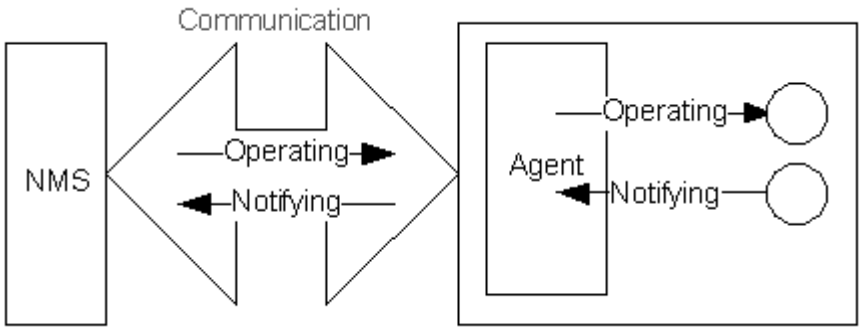
Basic Concepts

SNMP is an application layer protocol that works in client/server 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.

Figure 1-2



SNMP Network Manager

The SNMP network manager is a system that controls and monitors a network based on SNMP and is also called the NMS.

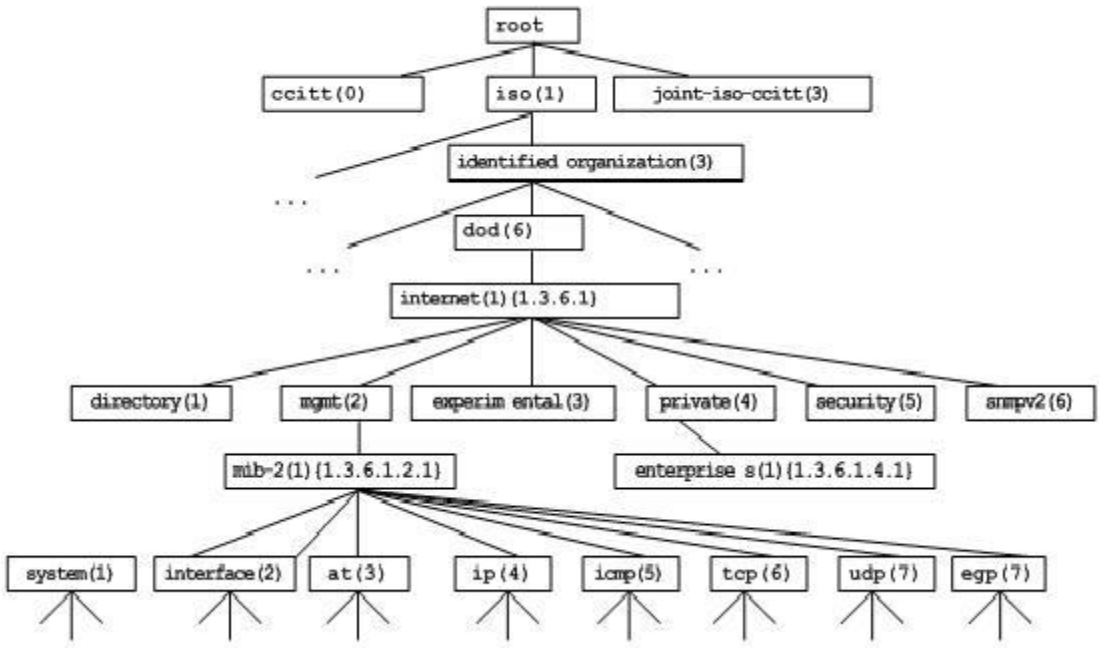
SNMP Agent

The SNMP agent (agent for short) 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 proactively send messages to the NMS.

MIB

The MIB is virtual, containing extensive information within managed network devices. To uniquely identify specific management units in SNMP packets, the MIB utilizes a hierarchical tree structure. Each node in this structure denotes a distinct management unit. A sequence of digits serves as a unique identifier for each management unit system across network devices. Essentially, the MIB functions as a repository of network device unit identifiers.

Figure 1-3 Tree Hierarchical Structure



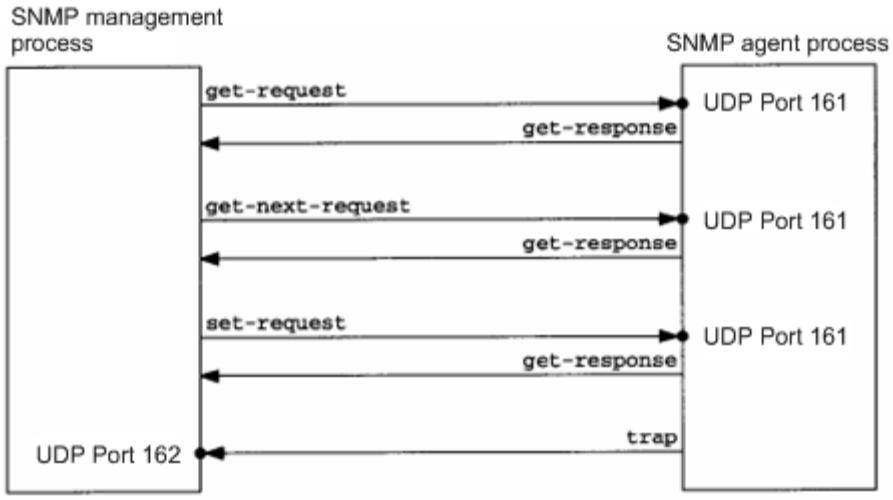
Operation Types

Six operation types are defined for information exchange between the NMS and 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 proactively sends a message to notify the NMS of event occurrence.

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 that SNMPv1 does not support the Get-bulk operation. Figure 1-4 illustrates 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 the authentication name and access permission.
SNMPv3	SNMPv3 redefines the SNMP architecture and enhances security functions, including the security model based on users and access control model based on views. The SNMPv3 architecture includes all functions of SNMPv1 and SNMPv2C.

SNMP MIB Cache Function	The SNMP MIB cache function enables the master device to collect MIB variables on the standby/backup device in advance and cache the collected MIB variables. In this way, the NMS can directly read the cached MIB variables from the master device, avoid accessing the standby/backup device and reducing the consumed time.

1.3.1 Basic SNMP Functions

Working Principle

Working Process

SNMP involves a request-response interaction (refer to Figure 1-4 for packet exchange details). The NMS initiates requests to the agent, including Get-request, Get-next-request, Get-bulk, and Set-request. Upon receiving these requests, the agent executes necessary operations and responds with a Get-response. Occasionally, the agent sends trap and Inform messages to the NMS. While the NMS does not need to reply to trap messages, it must send back an Inform-response to the agent; otherwise, the agent will resend the Inform message.

Related Configuration

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 1572 bytes, and the default UDP port number 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 device NE information.

The **snmp-server udp-port** command is used to set the UDP port number of the SNMP service or restore the default value.

The **snmp-server source-interface** command is used to set the source interface through which packets are received from SNMP.

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 proactively 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 proactively send trap messages to the NMS.

Setting Trap Message Parameters

By default, SNMP is not allowed to proactively send a trap message to the NMS, an interface is enabled to send a Link Trap message, the device is disabled from sending a system reboot trap message, 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 the agent to proactively send a trap message to the NMS.

The **snmp trap link-status** command is used to enable an interface to send a Link Trap message.

The **snmp-server trap-source** command is used to specify the source address for sending messages.

The **snmp-server queue-length** command is used to set the length of a trap message queue.

The **snmp-server trap-timeout** command is used to set the interval for sending a trap message.

The **snmp-server trap-format private** command is used to enable the device to carry private fields in an outgoing trap message.

The **snmp-server system-shutdown** command is used to enable the device to send a system reboot trap message.

Configuring the SNMP Attack Defense and Detection Function

By default, the SNMP attack defense and detection function is disabled.

The **snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** } command is used to enable the attack defense and detection function.

Configuring Password Dictionary Check for the Community and User

Password dictionary check for community and user is disabled by default.

You can enable password dictionary check for SNMP community and user using the **snmp-server enable secret-dictionary-check** command. This command needs to be used in conjunction with the **password policy** command in global configuration mode.

Configuring the SNMP Logging Function to Record 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 device to record Get and Set operations. **get-operation** controls Get and Get-Next operations records, and **set-operation** controls 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 an interval of 5 minutes.

Run the **no snmp-server heartbeat on** command to disable the heartbeat trap function.

Run the **snmp-server heartbeat period** command 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 on devices.

SNMPv2C introduces the Get-bulk operation mechanism, allowing for retrieval of extensive data or entire tables in fewer request-response cycles, thus optimizing efficiency. Additionally, SNMPv2C enhances error handling by providing more detailed error message types to the management workstation through expanded error codes, unlike SNMPv1 which offers only one generic error code. Given the coexistence of SNMPv1 and SNMPv2C capable management workstations on networks, SNMP agents must discern between SNMPv1 and SNMPv2C packets and respond accordingly with 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 pivotal for enabling the SNMP agent function because it defines community attributes and specifies the NMS scope where access to the MIB is permitted.

1.3.3 SNMPv3

SNMPv3 redefines the SNMP architecture and includes functions of SNMPv1 and SNMPv2.

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 services provided by the SNMP engine.

SNMPv3 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 SNMP agent engine IDs on devices when the NMS manages devices. SNMPv3 defines the discover and report operation mechanisms. When the NMS does not learn 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. Security models include SNMPv1, SNMPv2C, and SNMPv3. SNMPv3 includes SNMPv1 and SNMPv2C into the security model.

Table 1-1 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 based on the authentication name.
SNMPv2c	noAuthNoPriv	Authentication name	N/A	Data validity is confirmed based on the authentication name.

Table 1-2 SNMPv3 Security Model and Security Level

Security Model	Security Level	Authentication	Encryption	Description
SNMPv3	noAuthNoPriv	User name.	N/A	Data validity is confirmed based on the user name.
SNMPv3	authNoPriv	MD5/SHA /SHA256/SHA512	N/A	The data authentication mechanism based on HMAC-MD5 or HMAC-SHA is provided.
SNMPv3	authPriv	MD5/SHA /SHA256/SHA512	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. RFC 3411 defines the format of an engine ID:

- The first 4 bytes indicate the private enterprise ID (allocated by IANA) of a vendor, which is expressed in hexadecimal notation.
- The fifth byte indicates remaining bytes:
- 0: Reserved.
- 1: The rightmost 4 bytes indicate an IPv4 address.
- 2: The rightmost 16 bytes indicate an IPv6 address.
- 3: The rightmost 6 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 a 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 a view and the **snmp-server group** command is used to configure 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 a user.

The NMS can communicate with the agent by using only authorized users.

An SNMPv3 user can specify the security level (whether authentication and encryption are required), authentication algorithm (MD5 or SHA), authentication password, encryption password (DES), and encryption password.

1.3.4 SNMP MIB Cache Function

In the scenario where multiple devices are virtualized into one device and unified management is performed, the NMS needs to collect MIB variables on the standby/backup device through the master device. The collection process takes a long time if there are many devices.

Working Principle

The SNMP MIB cache function can be enabled to reduce the time consumed by the collection process. This function enables the master device to collect MIB variables on the standby/backup device in advance and cache the collected MIB variables. In this way, the NMS can directly read the cached MIB variables from the master device, avoid accessing the standby/backup device and reducing the consumed time.

Related Configuration

Configuring the SNMP MIB Cache Function

The SNMP MIB cache function is disabled by default.

Run the **snmp-server cache enable** command to configure the SNMP MIB cache function.

Configuring the SNMP MIB Cache Update Interval

The cache update interval is 300s by default.

Run the **snmp-server cache update-timer** *seconds* command to configure the SNMP MIB cache update interval.

Enabling the Cache Function on a Node with a Specified OID and Configuring the Cache Update Interval of This Node

The MIB cache function is disabled by default. The cache update interval of a node with a specified object identifier (OID) is consistent with the global cache update interval by default.

Run the **snmp-server cache oid** *oid-string* [**update-timer** *seconds*] command to enable the cache function on a node with a specified OID and configure the cache update interval of this node.

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 defense and detection function.
	snmp-server enable secret-dectionaty-check	Configures password dictionary check for communities and users.
Enabling the Trap Function	(Optional) It is used to enable the agent to proactively send a trap message to the NMS.	
	snmp-server host	Configures the NMS host address.
	snmp-server enable traps	Enables the agent to proactively send a trap message to the NMS.
	snmp trap link-status	Enables an interface to send a Link Trap message.
	snmp-server system-shutdown	Enables the device to send a system reboot trap message.
	snmp-server trap-source	Specifies the source address for sending a trap message.
	snmp-server heartbeat	Configures the heartbeat trap function and interval.
Disabling the Agent Function	(Optional) It is used to disable the agent function when the agent service is not required.	
	no snmp-server	Disables the agent function.
Setting SNMP Control Parameters	(Optional) It is used to set or change SNMP control parameters.	
	snmp-server contact	Sets the device contact mode.
	snmp-server location	Sets the device location.

Configuration	Description and Command	
	snmp-server logging	Sets the logging function.
	snmp-server chassis-id	Sets the serial number of the device.
	snmp-server net-id	Configures NE information about the device.
	snmp-server packetsize	Changes the maximum packet length.
	snmp-server udp-port	Changes the UDP port number of the SNMP service.
	snmp-server queue-length	Changes the length of a trap message queue.
	snmp-server trap-timeout	Changes the interval for sending a trap message.
Configuring SNMP MIB Cache Function	⚠ (Optional) It is used to configure or modify the SNMP MIB cache function.	
	snmp-server cache enable	Configures the global SNMP MIB cache function.
	snmp-server cache update-timer	Configures the global SNMP MIB cache update interval.
	snmp-server cache oid	Enables the cache function on a node with a specified OID and configures the cache update interval of this node.

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 configured 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 Step

↘ 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 Defense and Detection Function

- Optional.
- By default, the SNMP attack protection and detection function is disabled. When malicious attacks need to be prevented, the configuration item must be used on the agent.

Setting Password Dictionary Check for Community and User

- Optional.
- Password dictionary check for the SNMP community and user is disabled by default. To avoid using the weak community or user name that is easy to crack, you can enable this function. This configuration needs to be used with the **password policy** command in global configuration mode.

Configuring the SNMP Logging Function to Record Get, Get-Next, and Set Operations Performed by the NMS on the SNMP Agent

- Optional.
- The SNMP logging function records the Get, Get-Next, and Set operations performed by the NMS on the SNMP agent. When the Get and Get-Next operations are performed, the agent records the IP address of the NMS user, operation type, and OID of the operation node. When the Set operation is performed, the agent records the IP address of the NMS user, operation type, OID of the operation node, and set value. These logs will be sent to the device's information center with the informational level, which means that they serve as general notification messages for the device.

Verification

Run the **show snmp** command to check the SNMP function on the device.

Related Commands

Configuring an SNMP View

Command	**snmp-server view** *view-name oid-tree* { **include** | **exclude** }
Parameter Description	*view-name*: Specifies the view name. *oid-tree*: Specifies the 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**: Indicates that 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**: Indicates that 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**: Indicates that 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*: Specifies the 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*: Specifies the 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*: Specifies the 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 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* | **secret** [**0** | **8**] *string*} [**view** *view-name*] [[**ro** | **rw**] [**host** *ipaddr*]] [**ipv6** *ipv6-aclname*] [*aclnum* | *aclname*]
Parameter Description	*0*: Indicates that the input community string is a cleartext string. *7*: Indicates that the input community string is a ciphertext string. **secret**: Indicates the community name that needs to be encrypted, with the default encryption algorithm of SHA256. **0**: Indicates that the input community string is in cleartext mode, and will be encrypted using the default method. **8**: Indicates that the input community string is in ciphertext mode. *string*: Specifies the 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: Indicates that the NMS can read and write variables of the MIB. *aclnum*: Specifies the 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*: Specifies the 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*: Specifies the 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 pivotal for enabling the SNMP agent function because it defines community attributes and specifies the NMS scope where access to the MIB is permitted. 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** { *aclnum* | *aclname* | **ipv6** *ipv6_aclname* }]
Parameter Description	*username*: Specifies the user name. *groupname*: Specifies the group name for a user. **v1** | **v2c** | **v3**: Specifies the SNMP version. Only SNMPv3 supports security parameters. **encrypted:** Indicates that the specified password is in ciphertext mode. Otherwise, the cleartext mode is used. If the ciphertext mode is selected, enter a key consisting of contiguous hexadecimal digits. An MD5 authentication key consists of 16 bytes and an SHA authentication key consists of 20 bytes. Two characters stand for 1 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 password into the corresponding authentication key. **priv**: Specifies whether confidentiality is used. **des56**: Specifies 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*: Specifies the 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*: Specifies the 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*: Specifies the 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, SHA,

	SHA256, or SHA512), authentication password, encryption algorithm (DES or AES128), and encryption password.

Enabling the Agent Function

Command	**enable service snmp-agent**
Parameter Description	N/A
Configuration mode	Privileged mode.
Usage Guide	This command is used to enable the SNMP agent function of a device.

Enabling the SNMP Attack Defense and Detection Function

Command	**snmp-server authentication attempt** *times* **exceed** { **lock** | **lock-time** *minutes* | **unlock** }
Parameter Description	*times*: Specifies the number of continuous failed attempts. **lock**: Indicates that the source IP address is permanently forbidden to initiate authentication for access after continuous authentication fails. The administrator needs to manually unlock the IP address. **lock-time** *minutes*: Indicates that the source IP address is forbidden to initiate authentication for access in a period of time after continuous authentication fails. Beyond the period, the source IP address can be authenticated for access again. **unlock**: Indicates that the source IP address is allowed to access the MIB continuously after continuous authentication fails. This means that the SNMP attack defense and detection function is not configured.
Command Mode	Global configuration mode
Usage Guide	Configure the SNMP attack defense 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 Password Dictionary Check for the Community and User

Command	**snmp-server enable secret-dictionary-check**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command must be used with the **password policy** command in global configuration mode to set checking rules, such as a minimum password length of 6. Run the **no snmp-server enable secret-dictionary-check** command to disable the check function.

Setting the SNMP Logging Function to Record Get, Get-Next, and Set Operations Performed by the NMS on the SNMP Agent

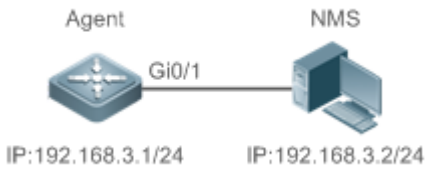
Command	**snmp-server logging** { **get-operation | set-operation** }
Parameter Description	**get-operation**: Enables logging of Get and Get-Next operations. **set-operation**: Enables logging of the Set operation.
Command Mode	Global configuration mode
Usage Guide	This command is used to record the 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.

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 the user configuration. **locked-ip**: Specifies the 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

Configuration Example

Configuring SNMPv3

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	● Configure a MIB view and a MIB group. Create a MIB view **view1**, which includes the

Steps	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 **view1** and write **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 Gi0/1 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 the device configuration. 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 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`

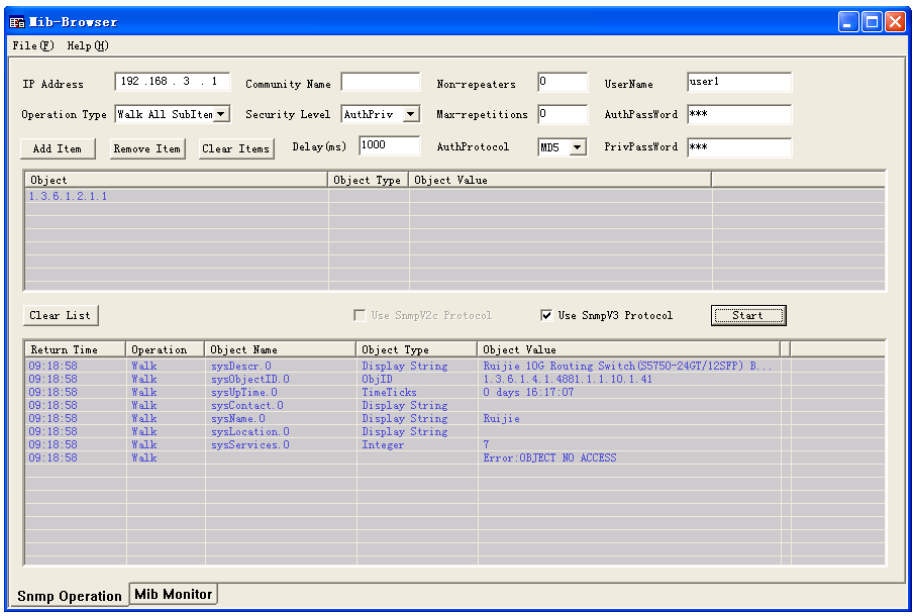
```
storage-type: permanent     active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

```
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

N/A

1.4.2 Enabling the Trap Function

Configuration Effect

Enable the agent to proactively send a trap message to the NMS.

Notes

N/A

Configuration Step

Configuring the SNMP Host Address

- Optional.
- Configure the host address of the NMS when the agent is required to proactively send messages.

Enabling the Agent to Proactively Send a Trap Message to the NMS

- Optional.
- Configure this item on the agent when the agent is required to proactively send a trap message to the NMS.

Enabling an Interface to Send a Link Trap Message

- Optional.
- Configure this item on the agent when a link trap message needs to be sent on an interface.

Enabling the Agent to Send a System Reboot Trap Message

- Optional
- Perform this configuration on the agent when the RGOS system is required to send a trap message to the NMS to notify system reboot before reloading or restarting the device.

Specifying the Source Address for Sending a Trap Message

- Optional
- Perform this configuration on the agent when a local IP address needs to be permanently used as the source SNMP address to facilitate management.

Enabling a Trap Message to Carry Private Fields When the Message Is Sent

- Optional
- Perform this configuration on the agent when private fields need to be carried in a trap message.

Configuring the Heartbeat Trap Function and Interval

- Optional.
- By default, the heartbeat trap function is enabled, and the heartbeat trap messages are sent at an interval of 5 minutes. Perform this configuration if the heartbeat trap function needs to be disabled or the interval for sending heartbeat trap messages needs to be changed.

Verification

Run the **show snmp** command to display the SNMP status.

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

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*: Specifies the address of the SNMP host. *ipv6-addr*: Specifies the IPv6address of the SNMP host. *domain-name*: Indicates the domain name of the SNMP host. **traps | informs**: Configures the host to send a trap message or an inform message. **version**: Configures an SNMP version, which can be set to **V1**, **V2C**, or **V3**. **auth** | **noauth** | **priv**: Sets the security level of V3 users. *community-string*: Specifies the community string or user name (v3). *port-num*: Configures the port number of the SNMP host. *notification-type*: Configures the type of trap messages that are proactively 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 proactively send trap messages to the NMS.

Enabling the Agent to Proactively 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: Enables authentication trap message. entity: Enables entity trap message. snmp: Enables trap notification for SNMP events. bridge: Enables trap notification for bridge events. mac-notification: Enables trap notification for MAC events. nfpp: Enables NFPP Traps message. ospf: Enables trap notification for OSPF events. vrrp: Enables trap notification for VRRP events. web-auth: Enables trap notification for web-based authentication events.
Command Mode	Global configuration mode
Usage Guide	This command must be used with the **snmp-server host** command to so that trap messages can be proactively sent.

Enabling an Interface to Send a Link Trap Message

Command	**snmp trap link-status**

Parameter Description	**-**
Configuration mode	Interface configuration mode
Usage Guide	For interfaces (Ethernet interface, aggregate interface, and SVI), when this function is enabled, a Link Trap message is sent if the link status on the interfaces changes. Otherwise, such a message is not sent.

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 restarting the device.

Specifying the Source Address for Sending a Trap Message

Command	**snmp-server trap-source** *interface*
Parameter Description	*interface*: Specifies the interface of which the address is 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, run this command to specify 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. Supported private fields include the alarm generation time. For more information about specific data types and data ranges of the fields, see RUIJIE-TRAP-FORMAT-MIB.mib.

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**

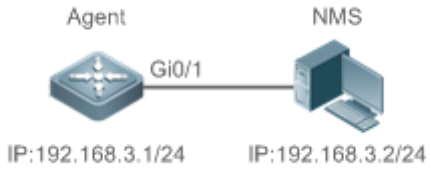
	command to disable this function.

Configuring the Interval for Sending Heartbeat Trap Messages

Command	**snmp-server heartbeat period** *time*
Parameter Description	*time*: Indicates the interval, in seconds.
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 proactively send messages to the NMS.
Configuration Steps	1. Perform the configuration to enable the agent to proactively 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 proactively send trap messages. 2. Set the IP address of the agent. Set the address of Gi0/1 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 the device configuration. ● 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 Hostname.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 Disabling the Agent Function

Configuration Effect

Disable 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 Step

↘ Disabling the SNMP Agent Function for the Device

- Optional.
- To disable the configuration of all SNMP agent services, perform this configuration.

Disabling the SNMP Agent Function for the Device

- Optional.
- To directly disable all services, perform this configuration.

Verification

Run the **show service** 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 the device configuration.

Related Commands

Disabling the SNMP Agent Function for the Device

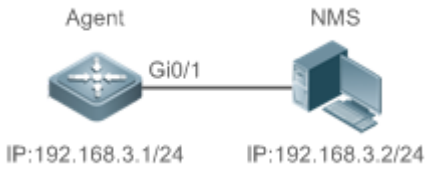
Command	**no snmp-server**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	By default, the SNMP agent function is disabled. When SNMP agent parameters (for example, NMS host address, authentication name, and access permission) are set, the SNMP agent service is automatically enabled. The **enable service snmp-agent** command must also be run simultaneously so that the SNMP agent service can take effect. If the SNMP agent service is disabled or the **enable service snmp-agent** command is not run, the SNMP agent service does not take effect. Run the **no snmp-server** command to disable SNMP agent services of all versions supported by the device. After this command is run, all SNMP agent service configurations are shielded (that is, after the **show running-config** command is run, no configuration is displayed. Configurations are restored after the SNMP agent service is enabled again). After the **enable service snmp-agent** command is run, the SNMP agent configurations are not shielded.

Disabling the SNMP Agent Function for the Device

Command	**no enable service snmp-agent**
Parameter Description	N/A
Configuration mode	Global configuration mode
Usage Guide	This command can be used to disable the SNMP service, but it will not shield SNMP agent parameters.

Configuration Example

Enabling the SNMP Service

Scenario **Figure 1-7**	 ● After the SNMP service is enabled and the SNMP agent server is set, the NMS can access devices based on SNMP.
Configuration Steps	1. Enable the SNMP service. 2. Set parameters for the SNMP agent server to make the SNMP service take effect.
A gent	`Hostname(config)#enable service snmp-agent`
Verification	● Run the **show service** 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. Based on the parameters, the NMS can obtain the contact and physical location of the device.

Notes

N/A

Configuration Step

↘ Setting the System Contact Mode

- Optional.
- When the contact mode of the system needs to be modified, perform this configuration on the agent.

↘ Setting the System Location

- Optional.
- When the system location needs to be modified, perform this configuration on the agent.

↘ Setting the System Serial Number

- Optional.

- When the system serial number needs to be modified, perform this configuration on the agent.

Setting NE Information about the Device

- Optional.
- When the NE code needs to be modified, perform this configuration 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, perform this configuration on the agent.

Setting the UDP Port Number of the SNMP Service

- Optional.
- When the UDP port number of the SNMP service needs to be modified, perform this configuration 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, perform this configuration on the agent.

Setting the Interval for Sending a Trap Message

- Optional.
- When the interval for sending a trap message needs to be modified, perform this configuration on the agent.

Configuring SNMP Flow Control

- Optional.
- If a large number of SNMP request packets result in a 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.

Configuring the Number of Attempts and Timeout for Sending Inform Packets

- Optional.

Verification

Run the **show snmp** command to display the SNMP status.

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

Related Commands

Setting the System Contact Mode

Command	**snmp-server contact** *text*
Parameter Description	*text*: Indicates the 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*: Indicates the 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*: Indicates the text of the system serial number, which may be digits or characters.
Configuration mode	Global configuration mode
Usage Guide	Typically, the device serial number is used as the SNMP serial number for the ease of identifying the device.

Configuring NE Information About the Device

Command	**snmp-server net-id** *text*
Parameter Description	*text*: Indicates the text that is used to set the device NE code. The text is a string that consists of 1 to 255 case-sensitive characters and may include spaces.
Configuration mode	Global configuration 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*: Indicates the packet size. The value range is from 484 bytes to 17876 bytes.
Configuration mode	Global configuration mode
Usage Guide	N/A

Setting the UDP Port Number of the SNMP Service

Command	**snmp-server udp-port** *port-num*
Parameter Description	*port-num*: Specifies the UDP port number of the SNMP service, that is, the number of the protocol port that receives SNMP packets.
Configuration mode	Global configuration mode

Usage Guide	Specify the protocol port number for receiving SNMP packets.

Setting the Length of a Trap Message Queue

Command	**snmp-server queue-length** *length*
Parameter Description	*length*: Specifies the queue length. The value range is from 1 to 1000.
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*: Specifies the interval for sending a trap message, which is expressed in the unit of 10 ms. The value range is from 1 to 1000.
Configuration mode	Global configuration mode
Usage Guide	Adjust the interval for sending a message to control the message sending speed.

Configuring SNMP Flow Control

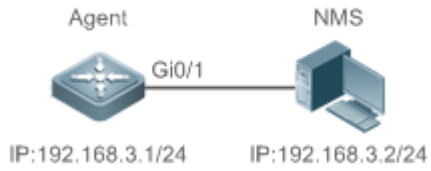
Command	**snmp-server flow-control pps** [*count*]
Parameter Description	*count*: Specifies the number of SNMP request packets processed per second. The value range is from 50 to 65535.
Command Mode	Global configuration mode
Usage Guide	If a large number of SNMP request packets result in a high CPU usage 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.

Configuring the Number of Attempts and Timeout for Sending Inform Packets

Command	**snmp-server inform** { **retries** *retry-num* | **timeout** *time* }
Parameter Description	*retry-num*: Indicates the number of attempts for sending inform packets. The value range is from 0 to 255. *time*: Indicates the timeout for sending inform packets, in seconds. The value range is from 0 to 21474836.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Setting SNMP Control Parameters

Scenario **Figure 1-8**	 ● The NMS manages network devices (agents) based on the community authentication mode and can obtain basic system information about the devices, for example, system contact mode, location, and serial number.
Configuration Steps	1. Set SNMP agent parameters, including the system location, contact mode, and serial number. 2. Set the IP address of the agent. Set the address of Gi0/1 to 192.168.3.1/24.

Agent	`Hostname(config)#snmp-server location fuzhou`
	`Hostname(config)#snmp-server contact Hostname.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	● Check the device configuration. ● 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 Hostname.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

1.4.5 Configuring SNMP MIB Cache Function

Configuration Effect

- Enable the SNMP MIB cache function to increase the speed of obtaining MIB data by the NMS. This function enables the master device to collect MIB variables on the standby/backup device in advance and cache the collected MIB variables. In this way, the NMS can directly read the cached MIB variables from the master device, avoid accessing the standby/backup device and reducing the consumed time.

Notes

- The SNMP MIB cache function applies only to MIB with specific table variables. To configure this function, only the OID of the root node of the MIB table variables needs to be configured.
- After the cache function is enabled, the cache is updated periodically, and the MIB data is not collected in real time. A short cache update interval may cause frequent cache update operations in the system, which consumes many CPU resources. On the contrary, a long cache update interval may delay MIB data updates, causing a failure to learn the system status in real time. Therefore, the cache update interval needs to be adjusted according to real-time performance of the MIB nodes and CPU resources.

Configuration Step

↘ Configuring the Global SNMP MIB Cache Function

- Optional.
- The SNMP MIB cache function is disabled by default. You can enable the MIB cache function globally.

↘ Configuring the Global SNMP MIB Cache Update Interval

- Optional.
- The global SNMP MIB cache update interval is 300s by default. You can configure the global cache update interval.

↘ Enabling Cache Function on Node with Specified OID and Configuring Cache Update Interval of This Node

- Optional.
- The cache function is disabled on all MIB nodes by default. You can enable the MIB cache function on a specified MIB node.

Verification

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

Related Commands

Configuring the Global SNMP MIB Cache Function.

Command	**snmp-server cache enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	

Configuring Global SNMP MIB Cache Update Interval

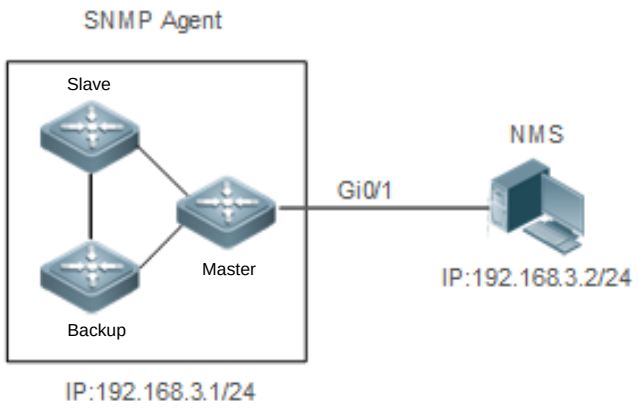
Command	**snmp-server cache update-timer** *seconds*
Parameter Description	*seconds*: Specifies the global SNMP MIB cache update interval, in seconds. The value range is from 60 to 86400.
Configuration Mode	Global configuration mode
Usage Guide	

Enabling the Cache Function on a Node with a Specified OID and Configuring the Cache Update Interval of This Node

Command	**snmp-server cache oid** *oid-string* [**update-timer** *seconds*]
Parameter Description	*oid-string*: Specifies the OID of a MIB node. *seconds*: Specifies the cache update interval, in seconds. The value range is from 60 to 86400.
Configuration Mode	Global configuration mode
Usage Guide	If the cache update interval of a MIB node is not configured, the global cache update interval is used.

Configuration Example

Setting SNMP Control Parameters

Scenario **Figure 1-9**	 ● The NMS manages the SNMP agent based on the community authentication mode. The NMS

	can obtain MIB node information about the SNMP agent, such as the connection status of the AP and STA.
Configuration Steps	● 1. Configure the global SNMP MIB cache function. ● 2. Configure the global SNMP MIB cache update interval. ● 3. Enable the cache function on a node with a specified OID.

Agent	`Hostname(config)# snmp-server cache enable`
	`Hostname(config)# snmp-server cache update-timer 600`
	`Hostname(config)# snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1`

Verification	● Display the device configuration.

Agent	`Hostname# show running-config | include snmp`
	`snmp-server cache enable`
	`snmp-server cache update-timer 600`
	`snmp-server cache oid 1.3.6.1.4.1.4881.1.1.10.2.56.2.1.1.1`
	`snmp-server enable traps`
	`snmp-server community public rw`

Common Errors

N/A

1.5 Monitoring

Clearing

Command	Description
clear snmp locked-ip [**ipv4** *ipv4-address* | **ipv6** *ipv6-address*]	Clears the list of source IP addresses that are locked after continuous authentication fails.

Displaying

Command	Description
show snmp [**mib** | **user** | **view** | **group| host | locked-ip | process-mib-time**]	Displays the SNMP status.

1 Configuring RMON

1.1 Overview

The Remote Network Monitoring (RMON) aims to address challenges of managing local area networks (LANs) and remote sites from a centralized point. In RMON, network monitoring data includes various statistics and performance indicators. These metrics are crucial for monitoring the network utilization, facilitating network planning, optimizing performance, and diagnosing network errors.

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
- RFC 4502: Remote Network Monitoring Management Information Base Version 2
- RFC 3919: Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)
- RFC 3737: IANA Guidelines for the Registry of Remote Monitoring (RMON) MIB Modules
- RFC 3434: Remote Monitoring MIB Extensions for High Capacity Alarms
- RFC 3395: Remote Network Monitoring MIB Protocol Identifier Reference Extensions
- RFC 3287: Remote Monitoring MIB Extensions for Differentiated Services
- RFC 3273: Remote Network Monitoring Management Information Base for High Capacity Networks
- RFC 2896: Remote Network Monitoring MIB Protocol Identifier Macros
- RFC 2895: Remote Network Monitoring MIB Protocol Identifier Reference

1.2 Applications

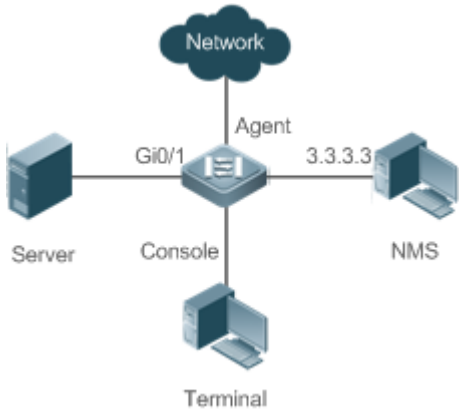
Application	Description
Collecting Statistics on Information of a Monitored Interface	Functions of RMON are utilized to an interface to monitor network communication.

1.2.1 Collecting Statistics on Information of a Monitored Interface

Scenario

The Ethernet statistics collection function of RMON is used to monitor accumulated information about an interface, the historical statistics collection function is used to monitor the packet count of an interface within each monitoring interval, and the alarm function is used to immediately obtain packet count exceptions of an interface. **Figure 1-1** shows the networking topology.

Figure 1-1



Deployment

An interface is monitored to accumulate statistics on packet counts and to collect data on packet counts and bandwidth utilization within the monitoring interval. If there's an abnormal packet count on the interface, an alarm is sent to the network management system (NMS). The key configuration points are outlined as follows:

- Configure the RMON Ethernet statistics collection function on the interface.
- Configure the RMON historical statistics collection 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 the 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

A 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. 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, so an administrator can easily query it.

History Group

A 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, bandwidth utilization, and collision count.

Alarm Group

An 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

An 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 logged so that an administrator can view it at any time.
- snmp-trap: A trap message is transmitted to the NMS to notify the NMS of event occurrence.
- log-and-trap: Event-relevant information is logged and a trap message is transmitted to the NMS.

Working Principle

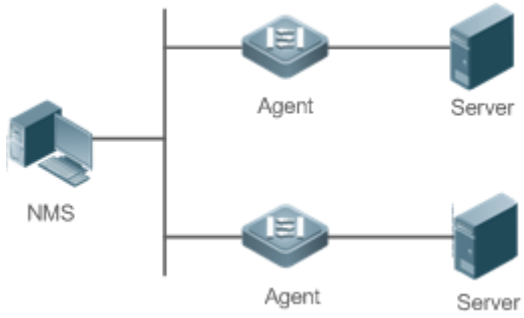
RMON allows multiple monitors and provides two data collection methods:

- Method 1: A dedicated RMON probe is used to collect data, and the NMS can directly obtain 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 network devices have the RMON probe function.

The NMS uses basic commands of the Simple Network Management Protocol (SNMP) to exchange data with RMON agents and collect network management information. This method, however, is limited by device resources and obtains information of only four groups but not all data of the RMON MIB.

Figure 1-2 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 an interface of a managed network device resides, thereby implementing remote management of network devices.

Figure 1-2



Overview

Feature	Description
RMON Ethernet Statistics Collection	Accumulates statistics on the packet count, byte count, and other data of a monitored Ethernet interface.

Feature	Description
RMON Historical Statistics Collection	Records the numbers of packets and bytes, and other communication data of 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, an event table is triggered to perform event processing or no processing is performed.

1.3.1 RMON Ethernet Statistics Collection

Working Principle

The RMON Ethernet statistics collection 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 collection 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 traffic information of the interface. The statistical items are variables defined in the RMON Ethernet statistical table, and recorded information is accumulated values of variables from the creation time of the RMON statistical table to the current time.

1.3.2 RMON Historical Statistics Collection

Working Principle

The RMON historical statistics collection function records accumulated statistics on traffic information about an Ethernet interface within each interval.

Related Configuration

↘ Configuring RMON Historical Control Entries

- The RMON historical statistics collection 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 limit or lower limit, a corresponding event is triggered for processing. For example, a trap message is

transmitted or one logTable entry record is generated. If the lower limit or upper limit is reached multiple times consecutively, only one corresponding event is triggered and another event is triggered till a reverse limit 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. 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 details on how to configure the SNMP agent, see *Configuring SNMP*.
- If a configured alarm object is a field node in the RMON statistics group or history group, the RMON Ethernet statistics collection function or RMON historical statistics collection function need to be configured on a monitored Ethernet interface first.

1.4 Configuration

Configuration	Description and Command	
Configuring RMON Ethernet Statistics Collection	⚠ (Mandatory) It is used to accumulatively collect statistics on traffic information about an Ethernet interface.	
	rmon collection stats	Configures Ethernet statistical entries.
Configuring RMON Historical Statistics Collection	⚠ (Mandatory) It is used to collect statistics on traffic information of an Ethernet interface and the bandwidth utilization within the interval.	
	rmon collection history	Configures historical control entries.
Configuring the 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 Collection

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 Step

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 stats** command to display Ethernet statistics.

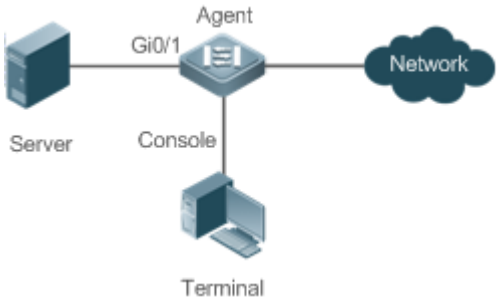
Related Commands

Configuring RMON Statistical Entries

Command	**rmon collection stats** *index* [**owner** *ownername*]
Parameter Description	*index*: Indicates the index of a statistical entry. The value range is from 1 to 65535. **owner** *ownername*: Indicates the entry creator. The value is a string of 1 to 63 case-sensitive characters.
Command Mode	Interface configuration mode
Usage Guide	The values of statistical entry parameters cannot be changed.

Configuration Example

Configuring RMON Ethernet Statistics Collection

Scenario **Figure 1-3**	
	As shown in Figure 1-3, the RMON agent is connected to the server, and the NMS requires the RMON statistics group to conduct performance statistics on received packets of Gi0/1. An administrator can view statistics at any time to learn 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 GigabitEthernet 0/1 to collect statistics on traffic of the 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 reconfigured or configured statistical table entries are modified.

1.4.2 Configuring RMON Historical Statistics Collection

Configuration Effect

Acquire accumulated statistics on 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 Step

- 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.

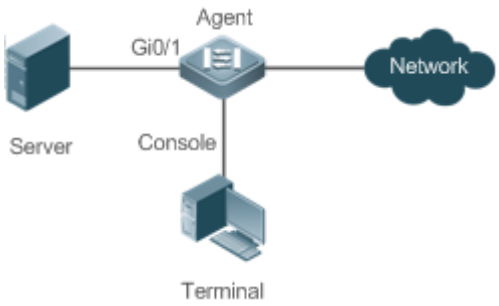
Related Commands

Configuring RMON Historical Control Entries

Command	**rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]
Parameter Description	*index*: Indicates the index of a history statistical entry. The value range is from 1 to 65535. **owner** *ownername*: Indicates the entry creator. The value is a string of 1 to 63 case-sensitive characters. **buckets** *bucket-number*: Sets the capacity of the history table in which a history statistical entry exists. The value range is from 1 to 65,535 and the default value is 10. **interval** *seconds*: Sets the statistics collection interval, in seconds. The value range is from 1 to 3600 and the default value is 1800.
Command Mode	Interface configuration mode
Usage Guide	The values of history statistical entry parameters cannot be changed.

Configuration Example

Configuring RMON History Statistics Collection

Scenario **Figure 1-4**	
	As shown in Figure 1-4, the RMON agent is connected to the server, and the NMS needs to collect statistics on received packets of Gi0/1 through the RMON history group at an interval of 60s, so as to monitor the network and learn emergency data.
Configuration Steps	● Configure the history control table on GigabitEthernet 0/1 to periodically collect statistics on 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 reconfigured or configured history control table entries are modified.

1.4.3 Configuring the 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 details on how to configure the SNMP agent, see *Configuring SNMP*.

If an alarm variable is a MIB variable defined in the RMON statistics group or history group, the RMON Ethernet statistics collection function or RMON historical statistics collection function must be configured on the monitored Ethernet interface. Otherwise, an alarm table fails to be created.

Configuration Step

Configuring Event Entries

- Mandatory.
- Perform the configuration in global configuration mode.

Configuring Alarm Entries

- Mandatory.
- Perform 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* [**description** *description-string* | **log** | **owner** *owner-name* | **trap** *community*] *
Parameter Description	*number*: Indicates the index of an event table. The value range is 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 of an event. The value is a string of 1 to 127 characters. **owner** *ownername*: Indicates the entry creator, which is a string of 1 to 63 case-sensitive 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.

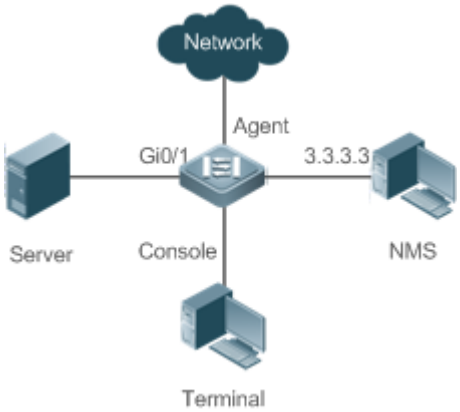
Configuring the RMON Alarm Group

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 of an alarm entry. The value range is from 1 to 65535.

	variable: Indicates an alarm variable. The value is a string of 1 to 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, in seconds. The value range is 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 reached. **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 reached. **rising-threshold** *value*: Sets the upper limit of the sampling quantity. The value range is from -2147483648 to +2147483647. *event-number:* Indicates the number of an event, which is triggered when the upper limit or lower limit is reached. **falling-threshold** *value*: Sets the lower limit of the sampling quantity. The value range is from -2147483648 to +2147483647. **owner** *ownername*: Indicates the entry creator The value is a string of 1 to 63 case-sensitive 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 or lower limit of the sampling quantity, and trigger events.

Configuration Example

Configuring the RMON Alarm

Scenario **Figure 1-5**	
	Assume that SNMPv1 runs on the NMS, the community name 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 GigabitEthernet0/3 is 1.3.6.1.2.1.2.2.1.15.3, the sampling mode is relative sampling, and the sampling interval is 60s. 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 GI0/1. The RMON agent needs to monitor the count of unknown protocol packets received by GI0/1. The sampling interval is 60s. 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 triggering. ● 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 input 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 limit is smaller than or equal to the lower limit.

1.5 Monitoring

Displaying

Command	Description
show rmon	Displays all RMON configuration.
show rmon statistics	Displays the Ethernet statistical table.
show rmon history	Displays the history control table.
show rmon alarm	Displays the alarm table.
show rmon event	Displays the event table.

1 Configuring NETCONF

1.1 Overview

The Network Configuration Protocol (NETCONF) is a new XML-based network configuration protocol developed by the NETCONF working group in 2003. It is used to configure and retrieve device parameters and monitor and manage the device. NETCONF uses the client/server mode for communication. The server program runs on the device, and the client program runs on a user device. The NETCONF protocol packets, including all configuration data and protocol messages are in Extensible Markup Language (XML) format. The NETCONF protocol consists of four layers: content layer, operation layer, remote procedure call (RPC) layer, and transmission layer. The content layer contains managed data objects, such as configuration data of the device. The operation layer defines a set of basic primitive operations of applications at the RPC layer, such as get, get-config, edit-config, and delete-config. The RPC layer provides a simple mechanism unrelated to the transport protocol, which contains regulations for elements of some error messages. The transmission layer provides a secure transmission channel using Secure Shell (SSH), Simple Object Access Protocol (SOAP), or Blocks Extensible Exchange Protocol (BEEP). SSH is mandatory. The following sections only describe the content related to NETCONF.

Protocols and Standards

- RFC 4741: NETCONF Configuration Protocol.
- RFC 4742: Using the NETCONF Configuration Protocol over Secure Shell (SSH)
- RFC 4743: Using NETCONF over the Simple Object Access Protocol (SOAP)
- RFC 4744: Using the NETCONF Protocol over the Blocks Extensible Exchange Protocol (BEEP)
- RFC 5277: NETCONF Event Notifications
- RFC 5381: Experience of Implementing NETCONF over SOAP
- RFC 5539: NETCONF Over Transport Layer Security (TLS)
- RFC 5717: Partial Lock RPC for NETCONF
- RFC 6022: NETCONF Monitoring Schema
- RFC 6241: Network Configuration Protocol
- RFC 6242: Using the Network Configuration Protocol over Secure Shell
- RFC 6243: With-defaults capability for NETCONF
- RFC 6470: NETCONF Notification Events
- RFC 6536: NETCONF Access Control Model (NACM)
- RFC 8071: NETCONF Call Home and RESTCONF Call Home

RFC 4741 and RFC 4742 are replaced by RFC 6241 and RFC 6242, respectively.

1.2 Applications

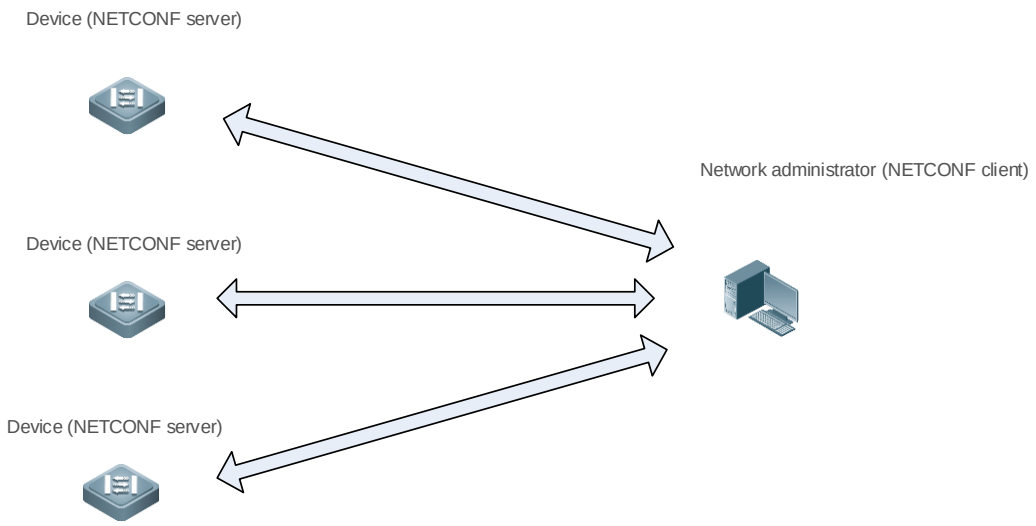
Application	Description
Configuring NETCONF Network Device Management	A user uses the network management software (NETCONF client) to send NETCONF configuration packets (XML format) to the device to configure and manage the device.

1.2.1 Configuring NETCONF Network Device Management

Scenario

As shown in Figure 1-1, the NETCONF client is used to manage and monitor network devices.

Figure 1-1



Deployment

The network management station connects to managed devices through a network, and the network management station and managed devices run SSH. On the network management station, the network administrator accesses the configuration database and status database on the network device and receives event messages proactively sent by the network devices through the NETCONF client to manage and monitor the network device.

1.3 Features

Basic Concepts

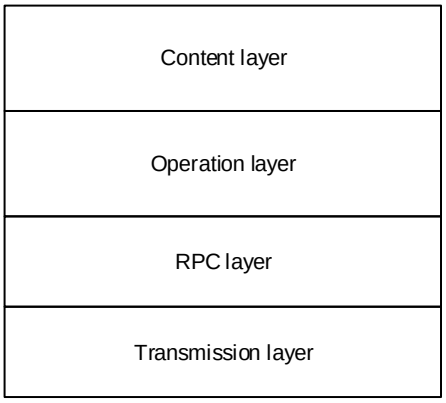
Definition of Terms

- RPC: Remote Procedure Call
- DM: data model

Network Structure of NETCONF

Figure 1-2 shows the structure of NETCONF.

Figure 1-2 Structure of NETCONF

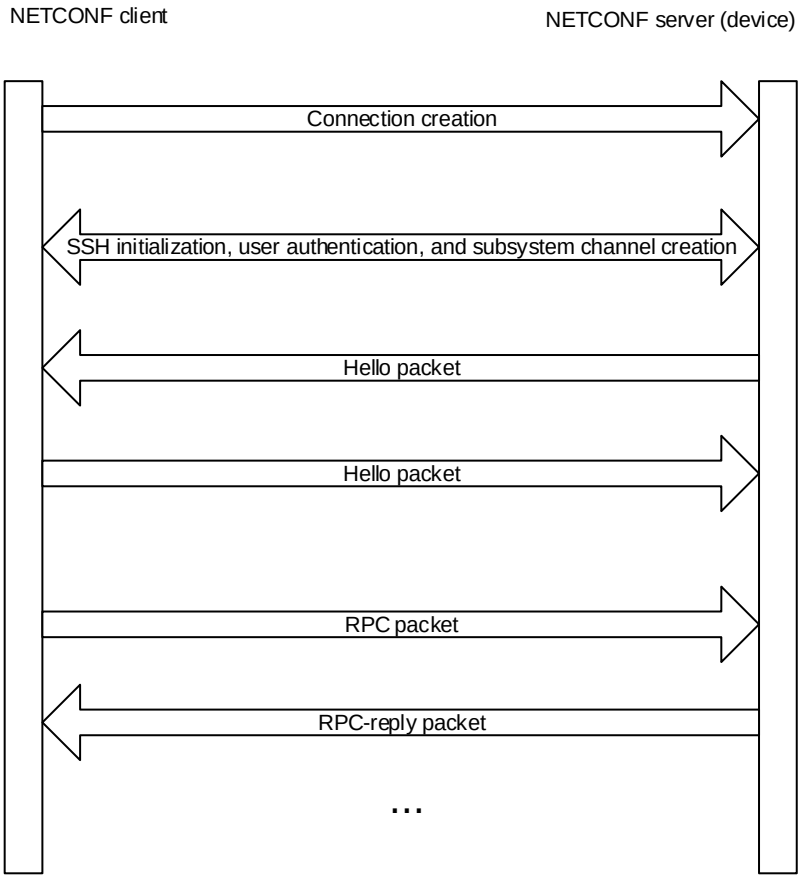


Session Creation

- NETCONF over SSH

The server is monitored over port 830. Before using the NETCONF protocol, an SSH channel (SSH subsystem, named netconf) needs to be established. The SSH channel is established through a series of transmission algorithm negotiations (including key negotiation, compression algorithm, hash algorithm, encryption algorithm, and signature algorithm) and user authentication.

Figure 1-3 Packet Exchange in a NETCONF Session



Capability Set Exchange

After the channel is established, the server and client need to exchange capability sets. Both parties provide their implemented capability sets and ignore capabilities they do not understand or implement. However, both parties must support at least basic protocol capabilities (urn:ietf:params:netconf:base:1.1). To be compatible with earlier protocol versions, both parties need to support basic capabilities of earlier versions (urn:ietf:params:netconf:base:1.0).

Protocol Operations

The operation layer of the NETCONF protocol defines nine basic operations. get and get-config are value acquisition operations, edit-config, copy-config, and delete-config are configuration operations, lock and unlock are lock protection during concurrent operations for unique device resources (such as the configuration file), and close-session and kill-session are session termination operations.

- get: Obtains the device status and configuration data.
- get-config: Obtains configuration data based on the configuration datastore.
- edit-config: Edits configuration based on the provided data model definition and operation attributes. One important attribute is **operation**, which includes merge, replace, create, delete, and remove options. The default value of the **default-operation** parameter is **merge**.
- copy-config: Copies configuration files. For example, copy the optional configuration to the configuration file, startup configuration to running configuration, or running configuration to startup configuration. To perform this operation, ensure that the target file is writable.
- delete-config: Deletes configuration files of the device. Running files of the device cannot be deleted.
- lock: Locks configuration data files to ensure that the current client can access (or modify) the files but other clients or non-NETCONF clients (such as SNMP or CLI) cannot access (or modify) the files.
- unlock: Unlocks configuration data files.
- close-session: Closes the current session, including resource and lock release and connection disconnection. To perform this operation, ensure that the current service is handled and no new request is handled.
- kill-session: Forcibly closes a session, including resource and lock release and connection disconnection. However, the current session cannot be closed. If a service is being handled, it must be stopped. Unfinished services must be rolled back to the initial state.

Overview

Feature	Description
Exchanging Capability Sets	The NETCONF server and client send capability sets to each other. The server (device) supports NETCONF 1.0 and 1.1.
Obtaining Data	The NETCONF client obtains configuration data or status data of the device.
Obtaining the Configuration	The NETCONF client obtains configuration data of the device.
Editing the Configuration	The NETCONF client modifies configuration data of the device.
Copying the Configuration	The NETCONF client copies a configuration file on the device to another configuration file.
Deleting the Configuration	The NETCONF client deletes a configuration file on the device.
Closing the Current Session	The NETCONF client proactively closes the NETCONF session with the device.

Feature	Description
Locking the Configuration	The NETCONF client locks a configuration file on the device.
Unlocking the Configuration	The NETCONF client unlocks a configuration file on the device.

1.3.1 Exchanging Capability Sets

After a connection is established between the client and server, they exchange their capability sets immediately. Subsequent data operations can be performed only after both parties support the same NETCONF version. The format of a sent packet is as follows.

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>
      urn:ietf:params:netconf:base:1.1
    </capability>
    <capability>
      Capability set 1
    </capability>
    <capability>
      Capability set 2
    </capability>
  </capabilities>
  <session-id>Session ID</session-id>
</hello>
```

⚠ Capability exchange messages sent from the NETCONF client to the NETCONF server cannot contain the session ID node (<session-id>).

Sample capability set exchange packet on the server:

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
    <capability>urn:ietf:params:netconf:base:1.1</capability>
    <capability>urn:ietf:params:netconf:capability:writable-running:1.0</capability>

  <capability>urn:ietf:params:xml:ns:yang:ietf-yang-types?module=ietf-yang-types&amp;re
  vision=2013-07-15</capability>

<capability>urn:rg:params:xml:ns:yang:rg-tacacs?module=rg-tacacs&amp;revision=2016-10-2
5</capability>

<capability>urn:rg:params:xml:ns:yang:rg-interfaces?module=rg-interfaces&amp;revision=2
016-10-25</capability>

<capability>urn:ietf:params:xml:ns:yang:ietf-inet-types?module=ietf-inet-types&amp;revi
sion=2010-09-24</capability>
```

```
<capability>urn:rg:params:xml:ns:yang:rg-openflow?module=rg-openflow&amp;revision=2016-09-26</capability>
  </capabilities>
  <session-id>28</session-id>
</hello>
```

Sample capability set exchange packet on the client:

```
<hello xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <capabilities>
    <capability>urn:ietf:params:netconf:base:1.0</capability>
  </capabilities>
</hello>
```

1.3.2 Obtaining Data

The get operation is used to obtain the device configuration or status data.

The format of packets sent from the client is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
  <filter type="subtree">
      Configuration data (or status data) filtering rule
  </filter>
  </get-config>
</rpc>
```

The format of packets returned by the server is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
     Obtained configuration data (or status data)
  </data>
</rpc-reply>
```

If none of status data subsets on the device matches filtering rules, the device returns an empty data node.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="Message ID " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
</rpc-reply>
```

1.3.3 Obtaining the Configuration

The get-config operation is used to obtain configuration data of the device. It obtains corresponding configuration data subsets based on various sub-tree filtering rules. However, it cannot obtain the device status data.

The format of packets sent from the client is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
 <rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <get-config>
   <source>
     <running/>
   </source>
   <filter type="subtree">
      Protocol-based filtering rule
    </filter>
  </get-config>
</rpc>
```

The format of packets returned by the server is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
 <rpc-reply message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      Obtained configuration data
   </data>
</rpc-reply>
```

If none of configuration data subsets on the device matches filtering rules, the device returns an empty data node.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
    <data xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"/>
</rpc-reply>
```

1.3.4 Editing the Configuration

The edit-config operation is used to edit configuration data based on the provided data model definition and operation attributes. The configuration editing packet contains five operation attributes, which are included in the operation attribute description of the configuration node in delivered XML packets. The five operation attributes are as follows:

- **merge**: Merges configuration data that contains this attribute in edit-config packets to the specified device configuration file (or database). If the configuration data does not exist, the device creates the configuration data based on the delivered content.
- **replace**: Replaces configuration data that contains this attribute in edit-config packets with the corresponding configuration data node in the specified device configuration file (or database). If the configuration data does not exist, the device creates the configuration data based on the delivered content. However, the device does not support this operation. If this attribute operation is delivered, the device performs the merge operation.
- **create**: Creates configuration data that contains this attribute in edit-config packets in the specified configuration data file (or database). If the configuration data does not exist, the device creates the configuration data based on the delivered content. If the configuration data already exists, the device returns an rpc-error packet, which carries error-tag whose content is data-exists.
- **delete**: Deletes configuration data that contains this attribute in edit-config packets from the specified configuration data file (or database). If the configuration data exists, the device directly deletes the corresponding configuration.

If the configuration data does not exist, the device returns an rpc-error packet, which carries error-tag whose content is data-missing.

- **remove**: Removes configuration data that contains this attribute in edit-config packets from the specified configuration data file (or database). If the configuration data exists, the device directly removes the corresponding configuration. If the configuration data does not exist, the device ignores this operation and returns OK.

The format of packets sent from the client is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target> <running/> </target>
      <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
        Configuration data
      </config>
  </edit-config>
</rpc>
```

If a packet does not carry the error-option node, the node is set to **stop-on-error** by default. When the configuration of a node is incorrect, subsequent configurations in the same packet are stopped and an error is returned (rpc-error). If a packet does not carry the test-option node, the node is set to **test-then-set** by default. If a packet does not carry the default-operation node, the node is set to **merge** by default.

The format of packets returned by the server is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="Message ID " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

When a packet carries the error-option node, the packet format is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
<edit-config>
  <target> <running/> </target>
  <error-option>Behavior option when a configuration error occurs</error-option>
  <config xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      Configuration data
  </config>
</edit-config>
</rpc>
```

The values of the error-option node are of enumerated type, including:

- **stop-on-error**: When an error occurs during an edit-config operation, the operation is stopped immediately. Data configured before this configuration packet (configuration before the error occurs) takes effect. This is the default value of the error-option node.

- **continue-on-error**: When a configuration error occurs during an edit-config operation, the error is recorded and remaining configurations are handled. However, error information is returned finally. That is, the final response packet is rpc-error in case of any configuration error.

1.3.5 Copying the Configuration

The copy-config operation is performed to synchronize the startup configuration to the running configuration.

The format of packets sent from the client is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx"  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <copy-config>
    <target>
      <startup/>
    </target>
    <source>
      <running/>
    </source>
  </copy-config>
</rpc>
```

The format of packets returned by the server is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx"  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

1.3.6 Deleting the Configuration

The delete-config operation is used to delete the startup configuration of the device. The running configuration of the device cannot be deleted.

The format of packets sent from the client is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <delete-config>
   <target>
     <startup/>
   </target>
 </delete-config>
</rpc>
```

The format of packets returned by the server is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

1.3.7 Closing the Current Session

The close-session operation is used to close the current session, release resources and lock, and disconnect the connection.

The format of packets sent from the client is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
   <close-session/>
</rpc>
```

The format of packets returned by the server is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx"  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

1.3.8 Locking the Configuration

As defined in RFC 6241, the lock operation is used to lock the configuration database (configuration file) to prevent multiple sources (such as CLI, SNMP, and multiple concurrent NETCONF sessions) from modifying the device configuration file concurrently and introducing other irrelevant configuration revisions. For this operation, the device can only prevent concurrent revision (running configuration) of multiple NETCONF sessions to ensure security of configuration data revision.

The format of packets sent from the client is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc message-id="xxx " xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <lock>
   <target>
     <running/>
   </target>
 </lock>
</rpc>
```

The format of packets returned by the server is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx "  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

1.3.9 Unlocking the Configuration

The unlock operation is used to unlock the configuration database (configuration file, running configuration here), which is opposite to the lock operation.

The format of packets sent from the client is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
```

```
<rpc message-id="xxx "  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <unlock>
   <target>
     <running/>
   </target>
 </unlock>
</rpc>
```

The format of packets returned by the server is as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<rpc-reply message-id="xxx "  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>
```

1.4 Configuration

Before NETCONF is used, the SSH channel authentication-related parameters need to be configured. For details about SSH configuration, see Configuring SSH.

Configuration	Description and Command	
Configuring NETCONF Call Home	⚠ (Optional) It is used to enable the NETCONF server to send a session establishment request to the NETCONF client.	
	netconf callhome { *hostname* | *ip-address* | **ipv6** *ipv6-address* } [**port** *port*]	Configures call home.
	netconf ch-reconnect interval *seconds*	Configures the call home reconnection interval.
	netconf source [**interface**] *interface-type interface-number*	Configures the source interface of call home.
	netconf source { **ip** *ip-address* | **ipv6** *ipv6-address* }	Configures the source IP address of call home.
Configuring the Candidate Capability of NETCONF	⚠ (Optional) It is used to configure the NETCONF server to report the candidate capability to the NETCONF client during capability set exchange.	
	netconf capability candidate	Enables the candidate and confirmed-commit capabilities of NETCONF.
Configuring the Rollback Capability of NETCONF	⚠ (Optional) It is used to configure the NETCONF server to report the rollback-on-error capability to the NETCONF client during capability set exchange.	
	netconf capability rollback	Enables the rollback-on-error capability of NETCONF.

Configuration	Description and Command	
Configuring the Validate Capability of NETCONF	(Optional) It is used to configure the NETCONF server to report the validate capability to the NETCONF client during capability set exchange.	
	netconf capability validate	Enables the validate capability of NETCONF.
Enabling the NETCONF Framework	(Optional) It is used to enable the NETCONF service on the device.	
	netconf enable	Enables the NETCONF framework service.
Disabling the Feature Attribute of NETCONF	(Optional) It is used to configure the NETCONF server not to report the feature attribute to the NETCONF client during capability set exchange.	
	netconf feature-disable	Disables the feature attribute of NETCONF.
Configuring the Maximum Number of Nodes Returned During NETCONF Session Query	(Optional) It is used to configure the maximum number of nodes returned during NETCONF session query.	
	netconf filter nodes-limit	Configures the maximum number of nodes returned during NETCONF session query.
Configuring the Maximum Number of NETCONF Session Connections	(Optional) It is used to configure the maximum number of NETCONF session connections with the NETCONF server.	
	netconf max-sessions	Configures the maximum number of NETCONF session connections.
Configuring the Port Monitored by the NETCONF Server	(Optional) It is used to configure the NETCONF server to monitor the port connected by the NETCONF client.	
	netconf port	Configures the port monitored by the NETCONF server.
Configuring the NETCONF Server to Advertise All Versions of All Supported YANG Modules to the NETCONF Client	(Optional) It is used by the NETCONF server to advertise all versions of all supported YANG modules to the NETCONF client during capability set exchange.	
	netconf yang multi-revision	Configures the NETCONF server to advertise all versions of all supported YANG modules to the NETCONF client.
Configuring the NETCONF Server to Preferentially Support the OpenConfig YANG Model	(Optional) It is used to configure the NETCONF server to preferentially support the OpenConfig YANG model.	
	netconf yang suite openconfig	Configures the NETCONF server to preferentially support the OpenConfig YANG model.

1.4.1 Configuring NETCONF Call Home

Configuration Effect

The NETCONF server proactively sends a session establishment request to the NETCONF client.

Notes

N/A

Configuration Step

Configuring NETCONF Call Home

Command	**netconf callhome** { *hostname* |*ip-address*	**ipv6** *ipv6-address* } [**port** *port*]
Parameter Description	*ip-address*: Specifies the remote IPv4 address of call home. *hostname*: Specifies the remote domain name of call home. **ipv6** *ipv6-address*: Specifies the remote IPv6 address of call home. **port** *port*: Specifies the remote port of call home. The default value is 4334.
Defaults	NETCONF call home is not configured by default.
Command Mode	Global configuration mode
Usage Guide	1. The call home configuration is affected by the **netconf enable** command. When the NETCONF service is unavailable, the call home configuration does not take effect. 2. Only one call home can be configured. If a call home already exists, run the **no netconf callhome** command to delete the existing configuration.

Configuring the NETCONF Call Home Reconnection Interval

Command	**netconf ch-reconnect interval** *seconds*
Parameter Description	*Seconds*: Specifies the call home reconnection interval, in seconds. The value range is from 5 to 3600.
Defaults	The default NETCONF call home reconnection interval is 5s.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Source Interface of NETCONF Call Home

- Optional. The source IP address of NETCONF call home is the IP address of the interface that sends packets by default.
- Run the **netconf source interface** *interface-type interface-number* command to configure the source interface. If the source interface is not configured on the device or no IP address is configured for the source interface, the source IP address of call home is still the IP address of the interface that sends packets.

Command	**netconf source interface** *interface-type interface-number*
Parameter Description	*interface-type*: Specifies the type of the interface. *interface-number*: Specifies the number of the interface.
Command	Global configuration mode

Mode	
Usage Guide	By default, the source IP address for initiating call home is the IP address of the interface that sends the packets. To facilitate tracing and management, you can use this command to specify an interface's IP address as the source IP address of call home. If the source interface is not configured on the device or no IP address is configured for the source interface, the source IP address of call home is still the IP address of the interface that sends the packets.

Configuring the Source IP Address of NETCONF Call Home

- Optional. The source IP address of NETCONF call home is the IP address of the interface that initiates call home by default.
- Unless otherwise specified, configure the source IP address of NETCONF call home on the device.
- Run the **netconf source** { **ip** *ip-address* | **ipv6** *ipv6-address* } command to configure the source IP address of call home. If the IP address is not configured on the device, the source IP address of NETCONF call home is still the IP address of the interface that initiates call home.

Command	**netconf source** { **ip** *ip-address*	**ipv6** *ipv6-address* }
Parameter Description	**ip** *ip-address*: Specifies the source IPv4 address that initiates call home to the remote PC with an IPv4 address. **ipv6** *ipv6-address*: Specifies the source IPv6 address that initiates call home to the remote PC with an IPv6 address.
Command Mode	Global configuration mode
Usage Guide	By default, the source IP address of call home is the IP address of the interface that initiates call home. To facilitate tracing and management, you can use this command to specify an interface's IP address as the source IP address of call home. If the source interface is not configured on the device, the source IP address of call home is still the IP address of the interface that sends the packets.

Verification

N/A

Configuration Example

Configuring NETCONF Call Home

Scenario Figure 1-4	
Configuration Steps	● Configure NETCONF call home.
NETCONF	`Hostname# configure terminal` `Enter configuration commands, one per line.  End with CNTL/Z.`

	Hostname(config)# netconf callhome 1.1.1.1 Hostname(config)# netconf source interface GigabitEthernet 0/1 Hostname(config)# netconf ch-reconnect interval 10
Verification	N/A

Common Errors

N/A

1.4.2 Configuring the Candidate Capability of NETCONF

Configuration Effect

The NETCONF server returns the candidate or confirmed-commit capability during capability set exchange with the NETCONF client (Hello packet and capabilities packet).

Notes

N/A

Configuration Step

Enabling the Candidate or Confirmed-commit Capability of NETCONF

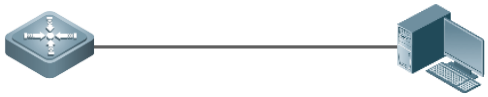
Command	**netconf capability candidate**
Parameter Description	N/A
Defaults	The candidate or confirmed-commit capability of NETCONF is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

Enabling the Candidate or Confirmed-commit Capability of NETCONF

Scenario **Figure 1-5**	NETCONF server NETCONF client 
Configuration Steps	● Enable the candidate or confirmed-commit capability of NETCONF.
NETCONF	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# netconf capability candidate

	`Hostname(config)#`
Verification	N/A

Common Errors

N/A

1.4.3 Configuring the Rollback Capability of NETCONF

Configuration Effect

The NETCONF server returns the rollback capability during capability set exchange with the NETCONF client (Hello packet and capabilities packet).

Notes

N/A

Configuration Step

↘ Enabling the Rollback Capability of NETCONF

Command	**netconf capability rollback**
Parameter Description	N/A
Defaults	The rollback capability of NETCONF is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

↘ Enabling the Rollback Capability of NETCONF

Scenario Figure 1-6	
Configuration Steps	● Enable the rollback capability of NETCONF.

NETCONF	`Hostname# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# netconf capability rollback`
	`Hostname(config)#`

Verification	N/A

Common Errors

N/A

1.4.4 Configuring the Validate Capability of NETCONF

Configuration Effect

The NETCONF server returns the validate capability during capability set exchange with the NETCONF client (Hello packet and capabilities packet).

Notes

N/A

Configuration Step

Enabling the Validate Capability of NETCONF

Command	**netconf capability validate**
Parameter Description	N/A
Defaults	The validate capability of NETCONF is disabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

Enabling the Validate Capability of NETCONF

Scenario Figure 1-7	
Configuration Steps	● Enable the validate capability of NETCONF.

NETCONF	`Hostname# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# netconf capability validate`
	`Hostname(config)#`

Verification	N/A

Common Errors

N/A

1.4.5 Enabling the NETCONF Framework

Configuration Effect

The NETCONF framework of the device allows the client to connect the configured port (port 830 by default).

Notes

N/A

Configuration Steps

↘ **Enabling the NETCONF Framework**

Command	**netconf enable**
Parameter Description	N/A
Defaults	The NETCONF framework is enabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

↘ **Enabling the NETCONF Framework**

Scenario Figure 1-8	
Configuration Steps	● Enable the NETCONF framework.

NETCONF	`Hostname# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# netconf enable`
	`Hostname(config)#`

Verification	N/A

Common Errors

N/A

1.4.6 Disabling the Feature Attribute of NETCONF

Configuration Effect

The NETCONF server does not return the feature attribute of YANG modules during capability set exchange with the NETCONF client (Hello packet and capabilities packet).

Notes

N/A

Configuration Step

↘ **Disabling the Feature Attribute of NETCONF**

Command	**netconf feature-disable**
Parameter Description	N/A
Defaults	The feature attribute of NETCONF is enabled by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

↘ **Disabling the Feature Attribute of NETCONF**

Scenario Figure 1-9	
Configuration Steps	● Disable the feature attribute of NETCONF.

NETCONF	`Hostname# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# netconf feature-disable`
	`Hostname(config)#`

Verification	N/A

Common Errors

N/A

1.4.7 Configuring the Maximum Number of Nodes Returned During NETCONF Session Query

Configuration Effect

When a user queries NETCONF sessions on the NETCONF client, only the number of XML nodes that does not exceed the upper limit can be returned. If the number of XML nodes returned exceeds the upper limit, an error is returned.

Notes

This configuration only affects query results with **target** set to **running**.

Configuration Step

↘ **Configuring the Maximum Number of Nodes Returned During NETCONF Session Query**

Command	**netconf filter nodes-limit** *num*
Parameter Description	*num*: Specifies the maximum number of nodes returned. The default value is 100000, and the value range is from 100 to 2147483647.
Defaults	The maximum number of nodes returned is 100000 by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

↘ **Configuring the Maximum Number of Nodes Returned During NETCONF Session Query**

Scenario Figure 1-10	
Configuration Steps	● Configure the maximum number of nodes returned during NETCONF session query.

NETCONF	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# netconf filter nodes-limit 101`
	`Hostname(config)#`

Verification	`Hostname (config)# show running-config | in filter nodes-limit` `netconf filter nodes-limit 101`

Common Errors

N/A

1.4.8 Configuring the Maximum Number of NETCONF Session Connections

Configuration Effect

When a NETCONF client connects to the NETCONF server, only the specified number of NETCONF session connections are allowed.

Notes

N/A

Configuration Step

Configuring the Maximum Number of NETCONF Session Connections

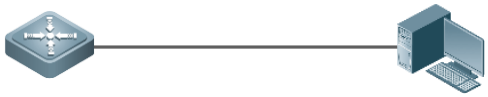
Command	**netconf max-sessions** *num*
Parameter Description	*num*: Specifies the maximum number of session connections. The default value is 1, and the value range is from 1 to 36.
Defaults	Only one session connection is supported by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

Configuring the Maximum Number of NETCONF Session Connections

Scenario **Figure 1-11**	NETCONF server NETCONF client 
Configuration Steps	● Configure the maximum number of NETCONF session connections.

NETCONF	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# netconf max-sessions 15`
	`Hostname(config)#`

Verification	`Hostname (config)#show running-config | in max-sessions` `netconf max-sessions 15`

Common Errors

N/A

1.4.9 Configuring the Port Monitored by the NETCONF Server

Configuration Effect

When the NETCONF client connects to the NETCONF server, the port with which the NETCONF client connects can be configured.

Notes

N/A

Configuration Step

Configuring the Port Monitored by the NETCONF Server

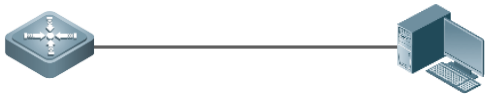
Command	**netconf port** *num*
Parameter Description	*num*: Specifies the monitored port number. The default value is 830, and the value range is from 1025 to 65535.
Defaults	The default monitored port number is 830.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

Configuring the Port Monitored by the NETCONF Server

Scenario **Figure 1-12**	NETCONF server NETCONF client 
Configuration Steps	● Configure the port monitored by the NETCONF server.

NETCONF	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# netconf port 1234`
	`Hostname(config)#`

Verification	`Hostname (config)#show running-config | in netconf` `netconf port 1234`

Common Errors

N/A

1.4.10 Configuring the NETCONF Server to Advertise All Versions of All Supported YANG Modules to the NETCONF Client

Configuration Effect

The NETCONF server advertises all versions of all supported YANG modules to the NETCONF client during capability set exchange with the NETCONF client (Hello packet and capabilities packet).

Notes

- The **netconf yang multi-revision** command must be configured before the capability packet (Hello packet) of the NETCONF server is advertised.
- The **no netconf yang multi-revision** command must be configured before the capability packet (Hello packet) of the NETCONF server is advertised and only the latest version of a YANG module is advertised in the capability notification packet.

Configuration Step

↘ Configuring the NETCONF Server to Advertise All Versions of All Supported YANG Modules to the NETCONF Client

- Optional.
- This configuration must be configured before the capability packet (Hello packet) of the NETCONF server is advertised.

Command	**netconf yang multi-revision**
Parameter Description	**N/A**
Defaults	The NETCONF server advertises all versions of all supported YANG modules to the NETCONF client by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

N/A

Configuration Example

↘ Configuring the NETCONF Server to Advertise All Versions of All Supported YANG Modules to the NETCONF Client

Scenario **Figure 1-13**	
Configuration	● Configure the NETCONF server to advertise all versions of all supported YANG modules to

Steps	the NETCONF client.
NETCONF	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# netconf yang multi-revision Hostname(config)#
Verification	N/A

↘

Common Errors

N/A

1.4.11 Configuring the NETCONF Server to Preferentially Support the OpenConfig YANG Model

Configuration Effect

When the NETCONF server starts, the device loads the OpenConfig YANG model.

Notes

- The **netconf yang suite openconfig** command takes effect after the device is restarted. If the command is configured, the OpenConfig YANG model is supported. Otherwise, the custom YANG model is supported.
- The **no netconf yang suite openconfig** command takes effect after the device is restarted. After the configuration takes effect, the OpenConfig YANG model is not supported.
- The **netconf yang suite openconfig** command takes effect after the device is restarted. The configuration after the CLI command is run is displayed in the **show running-config** command output.

Configuration Step

↘ **Configuring the NETCONF Server to Preferentially Support the OpenConfig YANG Model**

- Optional.
- The configuration takes effect after the device is restarted.

Command	netconf yang suite openconfig
Parameter Description	N/A
Defaults	The OpenConfig YANG model is not supported by default.
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

- Run the **show netconf yang-suite** command to display the effective YANG model configuration and configured YANG model of NETCONF (restart the device if the configuration does not take effect).

Configuration Example

Configuring the NETCONF Server to Preferentially Support the OpenConfig YANG Model

Scenario **Figure 1-14**	NETCONF server NETCONF client 
Configuration Steps	● Configure the NETCONF server to advertise all versions of all supported YANG modules to the NETCONF client.

NETCONF	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)#netconf yang suite openconfig`
	`This command will take effect after device restart.`
	`Hostname(config)#`

Verification	N/A

Common Errors

N/A

1.5 Monitoring

Displaying

Command	Description
show netconf yang-suite	Displays the current YANG model of NETCONF.

1 Configuring CWMP

1.1 Overview

The CPE WAN Management Protocol (CWMP) provides a general framework of unified device management, message specifications, management methods, and data models, realizing unified management and maintenance of widely distributed customer-premises equipment (CPEs), improving troubleshooting efficiency, and saving 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 reconfigure 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.
- Fault diagnosis: The ACE diagnoses or resolves connectivity or service problems based on information from CPEs, and can also perform pre-defined diagnosis tests.

Protocols and Standards

Major CWMP protocol specifications are outlined as follows:

- 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

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

1.2 Applications

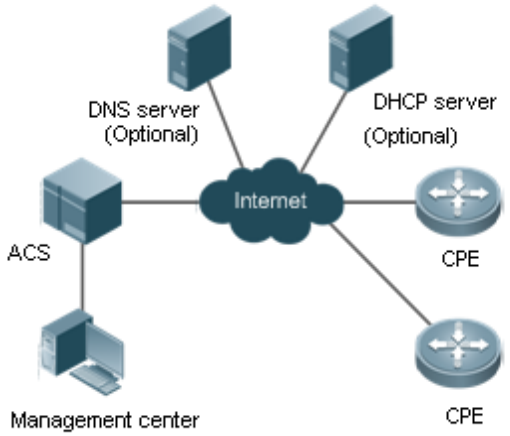
Typical Application	Scenario
CWMP Application Scenario	Initiate a CPE-ACS connection, so as to upgrade the CPE firmware, upload configuration files, restore the configuration, and realize other features.

1.2.1 CWMP Application Scenario

Application Scenario

A CWMP network architecture involves CPEs, an ACS, a management center, a Dynamic Host Configuration Protocol (DHCP) server, and a Domain Name System (DNS) server. The management center manages CPEs by controlling the ACS on a web browser.

Figure 1-1



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

Deployment

HTTP runs on both CPEs and the ACS.

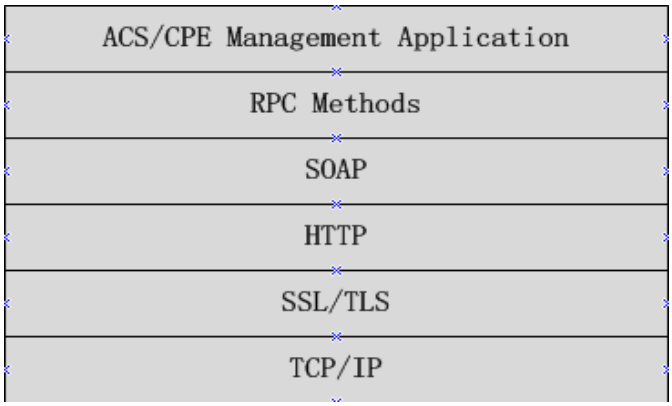
1.3 Features

Basic Concepts

↘ Protocol Stack

Figure 1-2 shows the protocol stack of CWMP.

Figure 1-2 CWMP Protocol Stack



As shown in Figure 1-2, CWMP defines six layers with respective functions.

- ACS/CPE Management Application

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

- RPC Methods

This layer provides various Remote Procedure Call (RPC) methods for interaction between the ACS and CPEs.

- SOAP

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

- HTTP

All CWMP messages are transmitted over the Hypertext Transfer Protocol (HTTP). Both the ACS and CPEs can behave as HTTP clients and servers. The server function is used to monitor reverse connections from the peer.

- SSL or TLS

The Secure Sockets Layer (SSL) or Transport Layer Security (TLS) layer guarantees CWMP security, including data integrity, confidentiality, and authentication.

- TCP/IP

The Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack is used.

RPC Methods

The ACS manages and monitors CPEs by calling the following main 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 data model (DM) parameters supported on CPEs.

- Set RPC Methods

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

- Inform RPC Methods

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

- Download RPC Methods

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

- Upload RPC Methods

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

- Reboot RPC Methods

The Reboot method enables the ACS to remotely reboot CPEs.

Session Management

CWMP works based on CWMP sessions or interactions. All CWMP interactions between the ACS and CPEs rely on these session exchanges. The ACS exchanges with CPEs to manages and monitors CPEs through session transmission, management, and maintenance. A typical session between ACS and CPE involves establishing a TCP connection, which starts from the Inform negotiation to TCP disconnection. Sessions are categorized into two types based on the initiator: those initiated by the CPE and those requested by the ACS.

↘ DM Management

CWMP operates based on the CWMP DM. CWMP manages all functional modules by a set of operations performed on DM. Each functional module registers and implements a respective data model, similar to 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 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 and multi-instance object nodes. A single-instance object node indicates that there is only one instance for this object node, whereas a multi-instance object node indicates that there are multiple instances for this object node.

DM nodes can be also classified into read and read-and-write nodes. A read node is a node whose parameter values can be read but cannot be modified, and a read-and-write 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 (not 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 (not the ACS), that is, whether the values of the parameters can be modified using other management modes such as Telnet. The ACS can modify attributes of the data models using RPC methods.

CWMP manages 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 similar to trap messages of SNMP or device logs. Using RPC methods, the ACS filters out unconcerned types of events. CWMP events are classified into two types: single (non-cumulative) events and cumulative events. A single event means that there is no quantitative change to the same event upon re-occurrence of the event, with old events discarded and the newest event kept. A cumulative event means that old events 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 Configuration Files	The ACS controls the upgrade of the configuration files of a CPE using the Download method.
Uploading 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 fails to be managed by the management center, this feature can be used to remotely restore the CPE to the previous status.

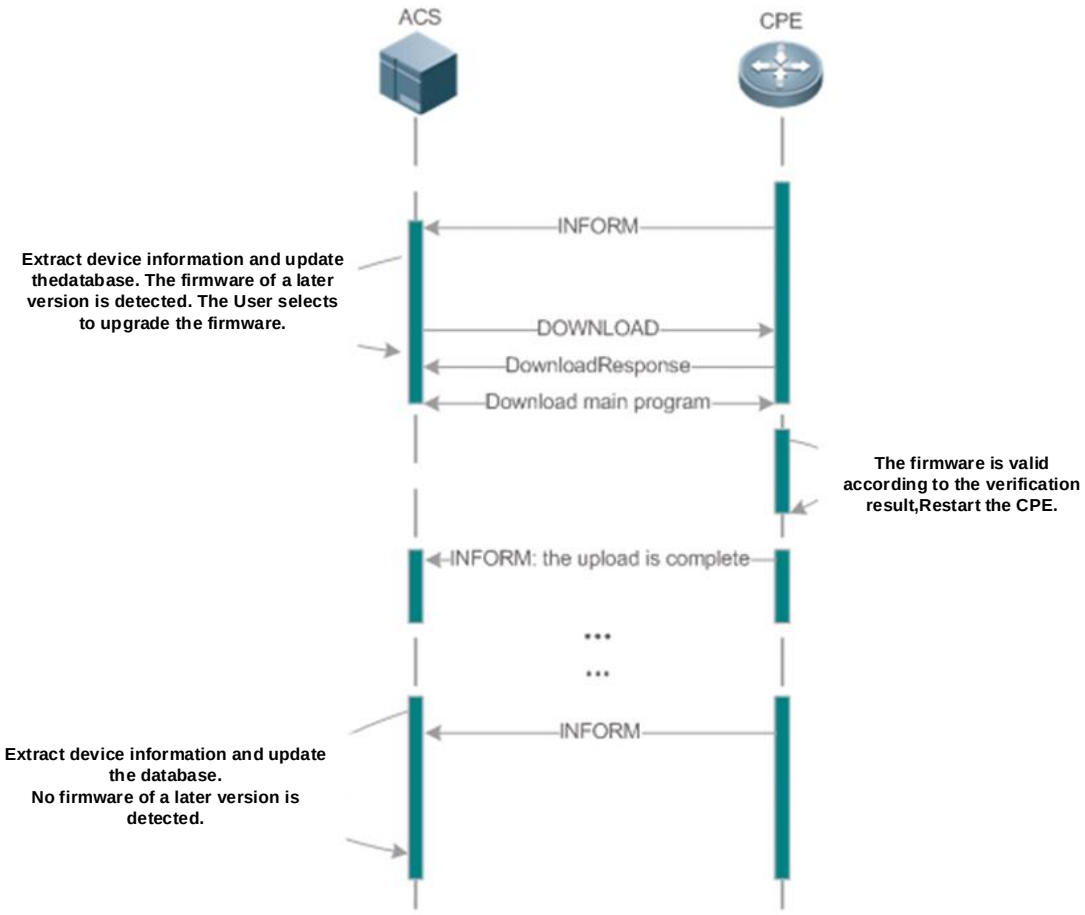
1.3.1 Upgrading the Firmware

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 1-3



You can 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. Then the CPE will notify the ACS of upgraded completed.

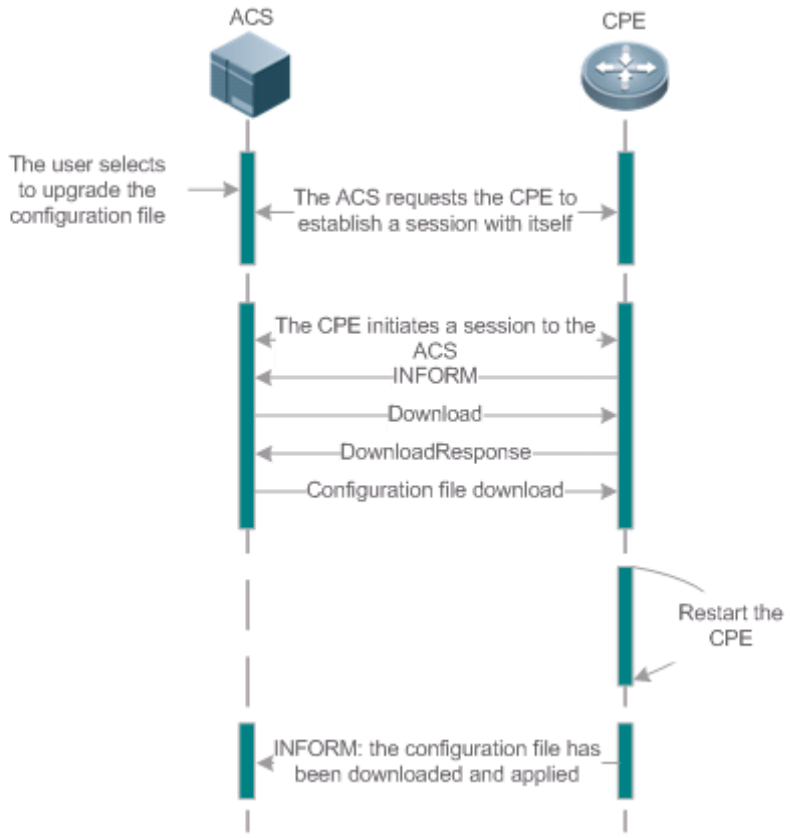
The file server can be the ACS or separately deployed.

1.3.2 Upgrading Configuration Files

Configuration files of a CPE can be replaced with specified configuration files, so that the new configuration files are used on the CPE after reset.

Working Principle

Figure 1-4



You can specify a CPE for the ACS to deliver the Download method for upgrading its configuration files. The CPE downloads the configuration files from the specified file server, upgrade configuration files, and then reboot. Then the CPE will notify the ACS of upgraded completed.

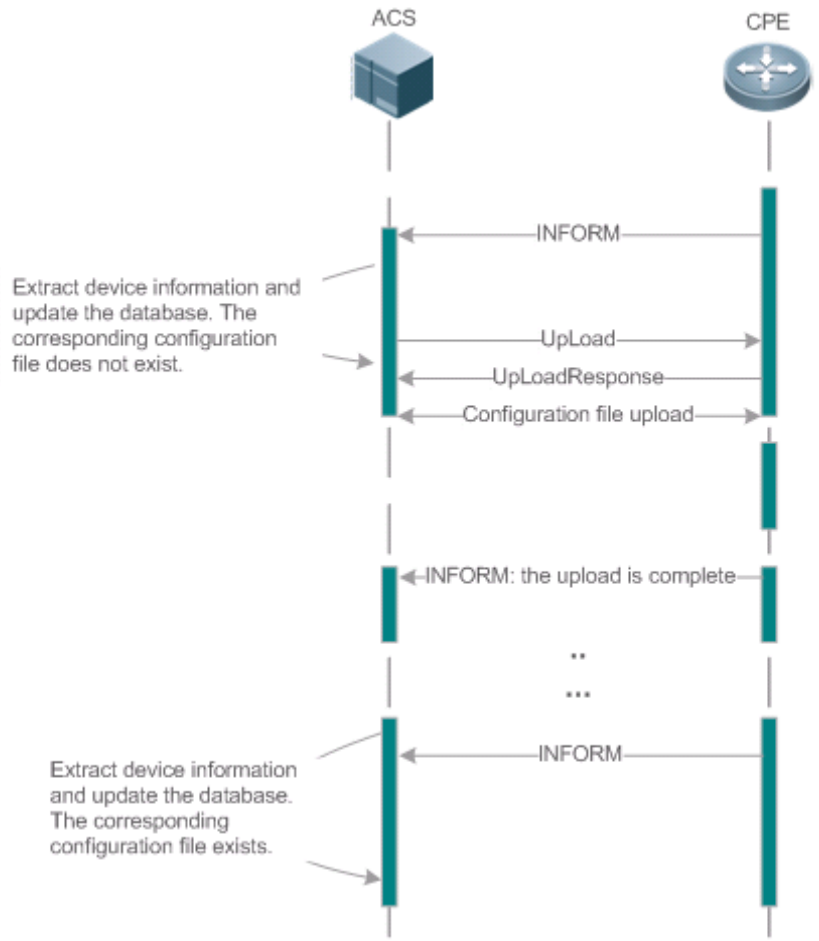
The file server can be the ACS or separately deployed.

1.3.3 Uploading Configuration Files

The ACS controls configuration files of CPEs by using the Upload method.

Working Principle

Figure 1-5



When a CPE initially connects to 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 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 notifies the ACS that the configuration files are uploaded.

1.3.4 Configuring Pre-registration

The unconfigured CPE automatically connects to the Ruijie Cloud server and automatically goes online based on the CWMP configuration delivered by Ruijie Cloud.

1.3.5 Backing Up and Restoring a CPE

When a remote CPE fails to be managed by the management center due to exceptions, the CPE backup and restoration feature helps restore the CPE to the previous status, so that the management center can remotely manage the CPE and take corresponding actions.

Working Principle

You can configure the restoration function on a CPE, so that the CPE can restore itself upon exceptions of its firmware or configuration files. When the CPE fails to connect to the ACS and fails to be managed by the management center after its firmware or configuration files are upgraded, the previous firmware or configuration files of the CPE can be restored in a timely manner for the ACS to manage the CPE. Such an exception occurs due to delivery of an incorrect version or configuration file.

Before the CPE receives a new firmware or configuration files for the 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.

1.4 Configuration

Configuration	Description and Command	
Establishing a Basic CWMP Connection	⚠ (Mandatory) It is used to configure the ACS or CPE username and password to be authenticated for a CWMP connection.	
	cwmp	Enables CWMP and enters the CWMP configuration mode.
	acs username	Configures the ACS username for establishing a CWMP connection.
	acs password	Configures the ACS password for establishing a CWMP connection.
	cpe username	Configures the CPE username for establishing a CWMP connection.
	cpe password	Configures the CPE password for establishing a CWMP connection.
	⚠ (Optional) It is used to configure URLs of the CPE and ACS.	
	acs url	Configures the URL of the ACS.
	cpe url	Configures the URL of the CPE.
Configuring CWMP-Related Attributes	⚠ (Optional) It is used to configure basic functions of the CPE, such as upload, backup, and restoration of the firmware, configuration files, or logs.	
	cpe inform	Configures the periodic notification function of the CPE.
	disable download	Disables the device from sending or downloading the firmware and configuration files from the ACS.
	disable upload	Disables the device from uploading configuration and log files to the ACS.
	cpe back-up	Configures the backup and restoration of the firmware and configuration file of the CPE.
	stun max-period	Configures the maximum STUN keepalive interval.

Configuration	Description and Command	
	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.
	register device	Enables pre-registration.

1.4.1 Establishing a Basic CWMP Connection

Configuration Effect

- A connection is established between the ACS and the CPE.

Notes

- N/A

Configuration Step

Enabling CWMP

- Mandatory.
- The CWMP function is enabled by default.
- Perform this configuration on the CPE.

Command	**cwmp**
Parameter Description	N/A
Command Mode	Global configuration guide
Usage Guide	N/A

Configuring the ACS Username for Establishing a CWMP Connection

- Mandatory.
- Perform this configuration on the ACS.
- Only one username can be configured for the ACS. If multiple usernames are configured, the latest username is used.

Command	**acs username** *username*
Parameter Description	**username** *username*: Indicates the ACS username for establishing a CWMP connection.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Password for Establishing a CWMP Connection

- Mandatory.
- Perform this configuration on the ACS.

- The password of the ACS can be in cleartext or ciphertext mode. Only one password can be configured for the ACS. If multiple passwords are configured, the latest password is used.

Command	**acs password** {*password* | *encryption-type encrypted-password*}
Parameter Description	*password*: Indicates the ACS password. *encryption-type*: Indicates the encryption mode. The value 0 indicates non-encryption and the value 7 indicates simple encryption. *encrypted-password:* Indicates the password text.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Username for Establishing a CWMP Connection

- Mandatory.
- Perform this configuration on the CPE.
- Only one username can be configured for the CPE. If multiple usernames are configured, the latest username is used.

Command	**cpe username** *username*
Parameter Description	*username*: Indicates the CPE username.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the CPE Password for Establishing a CWMP Connection

- Mandatory.
- Perform this configuration on the CPE.
- The password of the CPE can be in cleartext or ciphertext mode. Only one password can be configured for the CPE. If multiple passwords are configured, the latest password is used.

Command	**cpe password** {*password* | *encryption-type encrypted-password*}
Parameter Description	*password*: Indicates the CPE password. *encryption-type*: Indicates the encryption mode. The value 0 indicates non-encryption and the value 7 indicates simple encryption. *encrypted-password:* Indicates the password text.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to configure the CPE user password to be authenticated for the ACS to connect to the CPE. Typically, the encryption mode does not need to be specified. The encryption mode needs to be specified only when the encrypted password of this command is copied or pasted. A valid password should meet the following requirements: - It must contain 1 to 26 characters including letters and numerals. - The leading spaces will be ignored, while the trailing and middle spaces are valid.

Configuring the URL of the ACS for Establishing a CMWP Connection

- Optional.
- Perform this configuration on the CPE.
- Only one URL of the ACS can be configured. If multiple URLs are configured, the latest URL is used. The URL must be in HTTP format.

Command	**acs url** *url*
Parameter Description	*url*: Indicates the URL of the ACS.
Command Mode	CWMP configuration mode
Usage Guide	If the URL of the ACS is not configured but obtained through DHCP, CPEs will use this dynamic URL to initiate a connection to the ACS. The ACS URL must be in the format of http://ip [: port]/path and contains up to 255 characters.

Configuring the URL of the CPE for Establishing a CMWP Connection

- Optional.
- Perform this configuration on the CPE.
- Only one URL of the CPE can be configured. If multiple URLs are configured, the latest URL is used. The CPE URL must be in HTTP format but not the domain name format.

Command	**cpe url** *url*
Parameter Description	*url:* Indicates the URL of the CPE.
Command Mode	CWMP configuration mode
Usage Guide	If the URL of the CPE is not configured, it is obtained through DHCP. The the URL of the CPE must be in the format of http://ip [: port]/path and contains up to 255 characters.

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

The following configuration examples describe CWMP-related configuration only.

Configuring Usernames and Passwords on the CPE

Network Environment Figure 1-6	
Configuration Method	● Enable CWMP. ● On the CPE, configure the ACS username and password to be authenticated for the CPE to connect to the ACS. ● On the CPE, configure the CPE username and password to be authenticated for the ACS to connect to the CPE.

CPE	`Hostname# configure terminal`
	`Enter configuration commands, one per line.  End with CNTL/Z.`
	`Hostname(config)# cwmp`
	`Hostname(config-cwmp)# acs username USERB`
	`Hostname(config-cwmp)# acs password PASSWORDB`
	`Hostname(config-cwmp)# cpe username USERB`
	`Hostname(config-cwmp)# cpe password PASSWORDB`

Verification	● Run the **show** command on the CPE to check whether commands have been successfully executed.

CPE	`Hostname# show cwmp configuration`
	`CWMP Status                    : enable`
	`ACS URL                         : http://10.10.10.1:7547/acs`
	`ACS username                    : USERA`
	`ACS password                    : ******`
	`CPE URL                         : http://10.10.10.2:7547/`
	`CPE username                    : USERB`
	`CPE password                    : ******`

Configuring the URLs of the ACS and the CPE

Network Environment	See Figure 1-6.
Configuration Method	● Configure the URL of the ACS. ● Configure the URL of the CPE.

CPE	`Hostname# configure terminal`
	`Hostname(config)# cwmp`
	`Hostname(config-cwmp)# acs url http://10.10.10.1:7547/acs`
	`Hostname(config-cwmp)# cpe url http://10.10.10.1:7547/`

Verification	● Run the **show** command on the CPE to check whether commands have been successfully executed.

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://10.10.10.1:7547/`

Common Errors

- The input encrypted password is shorter than two characters or longer than 254 characters, or the length of the password is not an even number.
- The input cleartext password is longer than 126 characters.
- The input cleartext password contains invalid 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 of the CPE, such as the backup and restoration of its firmware or configuration file, whether to enable the CPE to download firmware and configuration files from the ACS, and whether to enable the CPE to upload its configuration and log files to the ACS.

Configuration Step

↘ Configuring the Periodic Notification Function of the CPE

- Optional.
- The value range is from 30 to 3600, in seconds. The default value is 600s.
- Perform this configuration to reset the periodical notification interval of the CPE.
- Perform this configuration on the CPE.

Command	**cpe inform** [**interval** *seconds*] [**starttime** *time*]
Parameter Description	*seconds*: Specifies the periodical notification interval of the CPE. The value range is from 30 to 3600, in seconds.

	time: Specifies the date and time for starting periodical notification in *yyyy-mm-ddThh:mm:ss* format.
Command Mode	CWMP configuration mode
Defaults	The default value is 600 seconds.
Usage Guide	Use this command to configure the periodic notification function of the CPE. ● If the time for starting periodical notification is not specified, periodical notification starts after the periodical notification function is enabled. The notification is performed once within every notification interval. ● If the time for starting periodical notification is specified, periodical notification starts at the specified start time. For instance, if the periodical notification interval is set to 60s and the start time is 12:00 am next day, periodical notification will start at 12:00 am next day and once every 60s.

Disabling the Device from 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.
- Perform this configuration on the CPE.

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 device from downloading the main program and configuration files from the ACS. ● This command is invalid for configuration script files. The configuration scripts can still be executed even if this function is disabled.

Disabling the Device from 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.
- Perform this configuration on the CPE.

Command	**disable upload**
Parameter Description	N/A
Defaults	The CPE can upload configuration and log files to the ACS by default.
Command Mode	CWMP configuration mode
Usage Guide	Use this command to disable the function of uploading configuration and log files to the ACS.

Configuring the Backup and Restoration of the Firmware and Configuration Files of the CPE

- Optional.
- The backup and restoration of the firmware and configuration files of the CPE is enabled by default. The value range is from 30 to 10000, in seconds. The default value is 60s.
- Perform this configuration to change the time for backup and restoration of the firmware and configuration files of the CPE.
- Perform this configuration on 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 60s.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the Maximum STUN Keepalive Interval

- Optional.
- Configure the maximum STUN keepalive interval in the range of 0s to 3600s. The default value is 60s.

Command	**stun max-period** *seconds*
Parameter Description	*seconds*: Configures the maximum STUN keepalive interval, in seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the Minimum STUN Keepalive Interval

- Optional.
- Configure the minimum STUN keeaplive interval in the range of 0s to 3600s. The default value is 20s.

Command	**stun min-period** *interval*
Parameter Description	*seconds*: Configures the minimum STUN keepalive interval, in seconds.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the STUN Server Port

- Optional.
- The STUN server port range is from 0 to 65535.

Command	**stun port** *port-number*
Parameter	*port-number*: Configures the STUN server port.

Description	
Command Mode	CWMP configuration mode
Usage Guide	N/A

Configuring the ACS Response Timeout Interval

- Optional.
- The value range is from 10 to 600, in seconds. The default value is 30s.
- Perform this configuration to change the ACS response timeout interval on the CPE.
- Perform this configuration on the CPE.

Command	**timer cpe- timeout** *seconds*
Parameter Description	*seconds*: Specifies the timeout interval, in seconds. The value range is from 10 to 600.
Defaults	The default value is 30s.
Command Mode	CWMP configuration mode
Usage Guide	N/A

Enabling the Pre-registration Function

- The function is enabled by default.
- Run the **no register device** command to disable the pre-registration function in global configuration mode.

Command	**register device**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	This command takes effect only on devices where the pre-registration macro is enabled. In scenarios where Ruijie Cloud is not required or there are high requirements on information security, you can use this command to disable the pre-registration function.

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 of the CPE

Scenario	See Figure 1-6.
Configuration Steps	● Enable the CWMP function and enter the CWMP configuration mode. ● Set the periodical notification interval of the CPE to 60s.
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 commands have been successfully configured.
CPE	Hostname# show cwmp configuration CWMP Status : enable …… CPE inform interval : 60s

Disabling the Device from Sending or Downloading Firmware and Configuration Files from the ACS

Scenario	See Figure 1-6.
Steps	● Enable the CWMP function and enter the CWMP configuration mode. ● Disable the device from sending or downloading the firmware and configuration files from the ACS.
CPE	Hostname# config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# cwmp Hostname(config-cwmp)# disable download
Verification	● Run the **show** command on the CPE to check whether commands have been successfully configured.
CPE	Hostname#show cwmp configuration CWMP Status : enable

	…… CPE download status : disable

Disabling the Device from Uploading Configuration and Log Files to the ACS

Scenario	See Figure 1-6.
Configuration Steps	● Enable the CWMP function and enter the CWMP configuration mode. ● Disable the device from 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 commands have been successfully configured.
CPE	Hostname# show cwmp configuration CWMP Status : enable …… CPE upload status : disable

Configuring the Delay for Backup and Restoration

Network Environment	See Figure 1-6.
Configuration Steps	● Enable the CWMP function and enter the CWMP configuration mode. ● Set the delay for backup and restoration to 100s.
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 commands have been successfully configured.
CPE	Hostname# show cwmp configuration CWMP Status : enable …… CPE back up delay time : 30s

Configuring the ACS Response Timeout of the CPE

Scenario	See Figure 1-6.
Configuration Steps	● Enable the CWMP function and enter the CWMP configuration mode. ● Set the response timeout of the CPE to 100s.
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 commands have been successfully configured.

CPE	Hostname# show cwmp configuration CWMP Status : enable …… CPE wait timeout : 100s

Common Errors

N/A

1.5 Monitoring

Displaying

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

1 Configuring gRPC

1.1 Overview

Google Remote Procedure Calls (gRPC) is a Google-developed RPC protocol. It is widely used in server program design. When Local Procedure Call (LPC) is used, a code snippet needs to be executed on the local host for performing an operation. When RPC is used, the service user and provider can be located on different computers. The client notifies the server by sending a request to the server over the network. The server returns the result to the client after the request is executed.

gRPC uses the protocol buffer for data serialization and deserialization and uses HTTP 2 as the data transmission protocol, ensuring better performance.

Protocols and Standards

- https://github.com/grpc/grpc

1.2 Applications

Application	Description
One-to-One Topology	One device reports gRPC information to one server.
One-to-Multi Topology	One device reports gRPC information to multiple servers.

1.2.1 One-to-One Topology

Scenario

A tested device (device S) is connected to a server and reports gRPC data to the server, as shown in Figure 1-1.

Figure 1-1 One-to-One Topology



Deployment

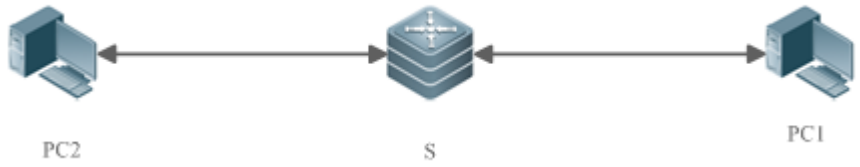
- Ensure that the network between device S and PC1 is reachable.
- Enable the gRPC function on device S.
- Configure events that need to be reported to the server on device S.

1.2.2 One-to-Multi Topology

Scenario

A tested device (device S) is connected to multiple servers and reports gRPC data to servers simultaneously, as shown in Figure 1-2.

Figure 1-2 One-to-Multi Topology



Deployment

- Ensure that the network between device S and PC1 and between device S and PC2 is reachable.
- Configure different IP addresses for PC1 and PC2.
- Enable the gRPC function on device S.
- Configure events that need to be reported to the server on device S.

1.3 Features

Basic Concepts

gRPC

gRPC is a cross-platform open-source high-performance RPC framework that was initially created by Google. It is based on HTTP2 and Protobuf 3.x.

Channel

A channel is established between the device and a server.

Stub

The stub is used to execute RPC.

For details about gRPC terms, see https://github.com/grpc/grpc.

Overview

Feature	Description
Enabling gRPC	Enables gRPC on the device. The device can serve as the gRPC server to receive authentication requests and obtain messages. It can also serve as the client to report gRPC data.
Supporting Login and Logout Operations	Supports login and logout operations initiated by a server.
Configuring Event Types Supported by gRPC	Configures event types supported by gRPC. Events include real-time, periodic, and obtainment events.
Specifying the Source Interface for Sending gRPC Data	Specifies the source interface for sending gRPC data.
Pre-configuring the Subscribing Server and Events to Be Subscribed to	Pre-configures the subscribing server and events to be subscribed to.

Feature	Description
Pre-configuring Server Login User Information	Pre-configures server login user information.
Configuring YANG Model Data Subscription (Defined in openconfig-telemetry.yang)	Configures YANG model data subscription.
Supporting RPC Methods Defined by a Third Party	Supports RPC methods defined by a third party.

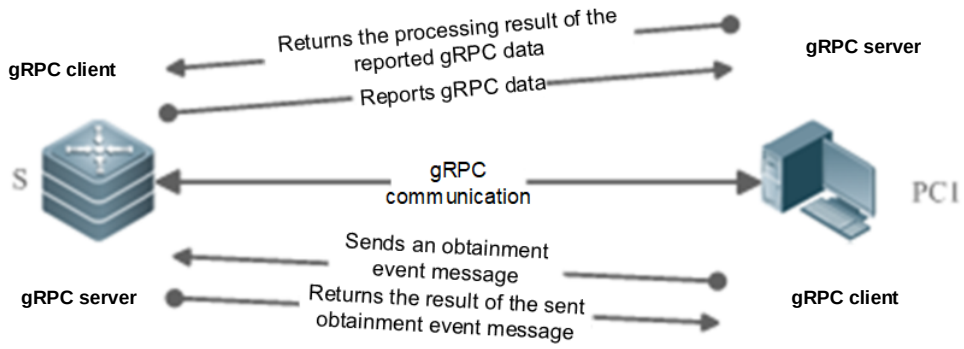
1.3.1 Enabling gRPC

Enable gRPC on the device. The device can serve as the gRPC server to receive authentication requests and obtain messages. It can also serve as the client to report gRPC data.

Working Principle

gRPC communication is implemented over the HTTP2 protocol. After a gRPC client initiates a request and a server returns a response, one data interaction is completed. Only the client can initiate a request, and then the server sends a response. Figure 1-3 shows the process.

Figure 1-3 gRPC communication



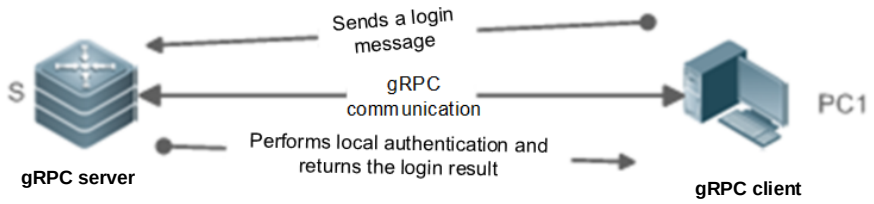
- After gRPC is configured on device S, the gRPC client and server are enabled on device S.
- The gRPC server of device S receives an obtainment event message from the server and returns a response to the obtainment event to the server.
- The gRPC client of device S reports gRPC data to the gRPC server based on the events subscribed to and waits for a response.

1.3.2 Supporting Login and Logout Operations

gRPC supports login and logout operations initiated by a server.

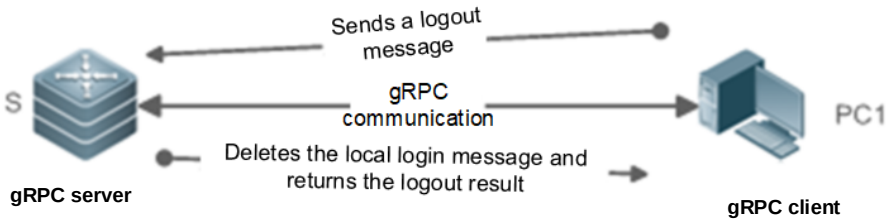
Working Principle

Figure 1-4 gRPC Login



- gRPC is configured on device S, and the gRPC server service is enabled.
- After device S receives a login request from the server, it authenticates the server locally and returns a login result to the server.
- The gRPC server of device S only receives the obtainment events initiated by the server that has logged in.

Figure 1-5 Logout Flow



- gRPC is configured on device S, and the gRPC server is enabled.
- After device S receives a logout request from the server, it deletes local matched login information and returns a logout result to the server.
- The gRPC server of device S no longer receives the obtainment events initiated by the server that has logged out.

1.3.3 Configuring Event Types Supported by gRPC

gRPC supports real-time , periodic, and obtainment events.

Working Principle

Real-time event: Is triggered when a specified threshold is met, irrespective of time. When the threshold is met, the device collects information once and reports it to the server.

Periodic events: Is reported regularly. When the time is reached, the device collects information once and reports it to the server.

Obtainment events: Is initiated by the server to query data. After the device receives a query request, the device collects information and reports it to the server.

1.3.4 Specifying the Source Interface for Sending gRPC Data

Working Principle

After gRPC is configured on the device and a channel with the server is created, the device creates a socket and attempts to send some ping packets to check whether the path is reachable. If the path is reachable, the device sends gRPC packets. By default, the created socket is bound randomly to the source address of a device port to send ping packets. If the server receives only packets from the specified source address, the default behavior of the device with gRPC enabled does not make the path reachable. As a result, gRPC packets cannot be uploaded.

If the specified source address is bound when a socket is created, the reachable path can ensure that gRPC packets are correctly uploaded.

1.3.5 Pre-configuring the Subscribing Server and Events to Be Subscribed to

Working Principle

The device can use a configuration command, NETCONF, or other methods to pre-create a server to be subscribed to and an event of concern.

The device can use a configuration command, NETCONF, or other methods to configure a standby server. When the active server malfunctions, the device automatically sends data to the standby server.

The device can use a configuration command to delete a server and an event that have been subscribed to and simulate the controller to notify the server of server and event unsubscription through NETCONF.

1.3.6 Pre-configuring Server Login User Information

Working Principle

By running a configuration command, the device can pre-create login user information about the server that passes authentication, simulate the server to initiate a login request, pass authentication, and save user information.

By running a configuration command, the device can delete login user information about the server that passes authentication, simulate the server to initiate a logout request, and delete login user information.

1.3.7 Configuring YANG Model Data Subscription (Defined in openconfig-telemetry.yang)

Working Principle

The device can use a configuration command, NETCONF, or other methods to deliver the configuration defined in **openconfig-telemetry.yang** to collect YANG model data of the device.

The device can use a configuration command, NETCONF, or other methods to delete the configuration defined in **openconfig-telemetry.yang**.

1.3.8 Supporting RPC Methods Defined by a Third Party

Working Principle

The device can use configuration commands to enable relevant functions defined in **gnmi.proto**. It can also collect device data by using RPC methods defined in **gnmi.proto**, such as Get, Set, and Subscribe.

The device can use configuration commands to disable relevant functions defined in **gnmi.proto**.

1.4 Configuration

Configuration	Description and Command	
Enabling gRPC	(Mandatory) It is used to enable the gRPC function. The device supports data subscription and reporting only after the gRPC function is enabled.	
	grpc	Creates the gRPC mode and enables the gRPC function.
Configuring Authentication Modes and AAA Server Authentication Attributes for gRPC Login and Logout	(Optional) It is used to configure server login authentication as required.	
	authen login { **local | authentication** *mlist* }	Configures the authentication mode of server login.
	authen aaa-config { **retry** *times* **| timeout** *second* }	Configures the number of retries and timeout interval during AAA server authentication.
Configuring Event Types Supported by gRPC	(Mandatory) It is used to configure events subscribed to.	
	subscr realtime enable	Enables the device to focus on all subscribed-to real-time events.
	subscr sample enable	Enables the device to focus on all subscribed-to periodic events.
	subscr-sample-interval *interval* [**millisecond** *millisecond*]	Changes the timer value of periodic events, which can be set to milliseconds.
	subscr-realtime-interval {all *interval* **| realtime** *json-event interval***}**	Configures the suppression time of real-time events.
Specifying the Source Interface for Sending gRPC Data	**subscr-source-interface**	Configures the source interface for sending real-time data and periodic data.
Configuring the Response Timeout Interval for gRPC Data	**reply-timeout**	Configures the response timeout interval for Get/Set data.
Pre-configuring the Subscribing Server and Events to Be Subscribed to	**user-server** *ip-address port-id*	Pre-configures the subscribing server.
	standby-server *ip-address port-*	Pre-configures the standby server of the subscribing server.
	type *json-event* **value** *value* [**value-extend** *value-extend*]	Pre-configures the subscribed-to event of the specified server.
Pre-configuring the Server Login User Information	**user-client** *id user-name ip-address*	Pre-configures server login user information.
Configuring a gRPC YANG Model Path and Its Group	**sensor-group** *group-id*	Configures a YANG model path.
	sensor-path *path*	
Configuring the gRPC Destination Server	**destination-group** *group-id*	Configures the destination server address.
	ip *ip-address* **port** *port-id*	
	protocol grpc {**tls | no-tls**}	Configures the protocol used by the destination server.

Configuration	Description and Command	
Configuring a gRPC Subscription Association	**sensor-group** *group-id* **sample-interval** *interval*	Configures the subscription association relationship.
	destination-group *group-id*	
Supporting RPC Methods Defined by a Third Party	**rpc gnmi enable**	Configures RPC methods defined in **gnmi.proto**.

1.4.1 Enabling gRPC

Configuration Effect

- Enable the gRPC client and gRPC server.

Notes

- The device and server must be reachable to each other.
- The port number of the local gRPC server is 50051.

Configuration Step

Enabling gRPC

- Mandatory.
- Unless otherwise specified, enable gRPC in the global configuration mode of each device.

Command	**grpc**
Parameter Description	N/A
Defaults	gRPC is disabled by default.
Command Mode	Global configuration mode
Usage Guide	This command is used to create a gRPC instance, enable the gRPC function, and enter the gRPC process configuration mode. When the gRPC function is enabled, the gRPC client and gRPC server are created. The gRPC client uploads data to the server, and the gRPC server parses authentication messages and obtainment messages sent from the server.

Verification

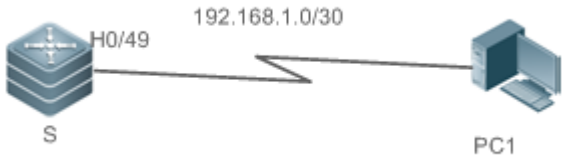
- Run the **show grpc status** command to display the running time after the gRPC function is enabled.

Configuration Example

Only gRPC-related configuration is described.

Enabling gRPC

Scenario	The network communication between device S and PC1 is normal.

Figure 1-6 One-to-One Topology	
Configuration Steps	● Enable the gRPC function. ● Configure a WAN port.

S	`S(config)# grpc`
	`S(config-grpc)# exit`
	`S(config)# interface HundredGigabitEthernet 0/49`
	`S(config-if-HundredGigabitEthernet 0/49)# ip address 192.168.1.1 255.255.255.252`

Verification	● Ping the server address to check whether the address is reachable. ● Check whether the gRPC function is enabled.
S	`S# show grpc status`

Common Errors

N/A

1.4.2 Configuring Authentication Modes and AAA Server Authentication Attributes for gRPC Login and Logout

Configuration Effect

- The authentication mode of the gRPC login and logout function is configured as non-authentication, AAA local authentication, or AAA server authentication (timeout interval and retry count).

Notes

- If AAA server authentication is configured, the new-model mode must be enabled.
- You are not advised to configure the non-authentication mode.
- You are not advised to modify the timeout interval or retry count.

Configuration Step

↘ Configuring the Authentication Mode for gRPC Login and Logout

- Optional.
- Perform this configuration as needed.
- Unless otherwise specified, configure authentication login in gRPC process configuration mode of the device where this configuration needs to be performed.

Command	**authen login** { **local** | **authentication** *mlist* }
Parameter Description	**local**: Enables authentication based on the local username database. It is the default configuration. **authentication**: Uses the specified AAA server list for authentication. *mlist*: Specifies the name of the AAA list.

Defaults	Local login is used by default, that is, **authen login local**.
Command Mode	gRPC process configuration mode
Usage Guide	Upon receiving a login request from the server, the device selects AAA local authentication, AAA server authentication, or non-authentication based on the configured authentication mode. After the server passes authentication, login user information, namely, the IP address and username of the server, is recorded. The device only returns responses to the obtainment event requests from the server that passes authentication.

Configuring AAA Server Authentication Attributes for gRPC Login and Logout

- Optional. The configuration relies on AAA configuration and takes effect only after the AAA configuration (**aaa new-model**) is completed.
- Perform this configuration as needed.
- Unless otherwise specified, do not change the device configuration.

Command	**authen aaa-config** { **retry** *times* **| timeout** *second* }
Parameter Description	**retry**: Configures the retry count during AAA server authentication. *times*: Specifies the retry count. The value range is from 1 to 100. The default retry count is 1. **timeout**: Configures the timeout interval of AAA server authentication. *second:* Specifies the timeout interval, in seconds. The value range is from 0 to 300. The value 0 indicates that waiting for the AAA server times out. The default timeout interval is 4s.
Command Mode	gRPC process configuration mode
Usage Guide	This command is used to configure the retry count and timeout interval of AAA server authentication during server login. You are not advised to modify the retry count or timeout interval. If the retry count exceeds a limit or an improper timeout time is configured, AAA users may be locked for 15 minutes. The lock time can be canceled by running the **clear aaa local user lockout all** command.

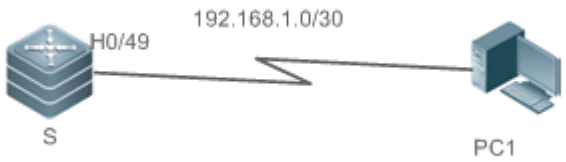
Verification

- Run the **show running** command to check whether the configuration is correct.

Configuration Example

Only gRPC-related configuration is described.

Configuring the Authentication Mode for gRPC Login and Logout

Scenario	The network communication between device S and PC1 is normal.
Figure 1-7 One-to-One Topology	
Configuration Steps	● Enable the gRPC function. ● Configure the new-model and mlist test.

S	S(config)# grpc S(config-grpc)# authen login authentication test
Verification	● Check whether the configuration is saved correctly. ● Check whether the PC client can ping the device. ● Check whether the PC client can be authenticated and record the authentication information.
S	S# show running S# show grpc client

Common Errors

N/A

1.4.3 Configuring Event Types Supported by gRPC

Configuration Effect

- Enable the device to focus on all subscribed-to real-time events on the device.
- Enable the device to focus on all subscribed-to periodic events on the device.
- Change the timer value of periodic events.

Notes

- An event that the server subscribes to takes effect only when the event is configured on the device.

Configuration Steps

↘ Enabling the Device to Focus on Subscribed-to Events on the Device

- Mandatory.
- Run the **subscr realtime enable** command to enable the device to focus on all subscribed-to real-time events on the device.
- Run the **subscr sample enable** command to enable the device to focus on all subscribed-to periodic events on the device.
- Run the **show grpc channel [counter]** command to display information about real-time or periodic events that the server registers and subscribes to or various statistics.

Command	**subscr** [**realtime** | **sample**] **enable**
Parameter Description	**realtime**: Specifies the subscribed-to real-time events that need to be concerned. The function of concerning subscribed-to real-time or periodic events is disabled by default. **sample**: Specifies the subscribed-to periodic events that need to be concerned.
Command Mode	gRPC process configuration mode
Usage Guide	After the gRPC process configures the function of concerning subscribed-to events, the gRPC process waits for the NETCONF manager to send the subscribed-to events. When the received subscription message matches the locally subscribed-to event, the gRPC process enables the corresponding event and reports gRPC data to the server. When the NETCONF manager sends an event unsubscription message to the gRPC process and the received unsubscription message matches the locally subscribed-to event, the gRPC process disables the event and reports gRPC

	data to the server. If the function of concerning subscribed-to events is not configured on the gRPC process, the gRPC process ignores the event subscription and unsubscription messages sent by the NETCONF manager.

Configuring the Timer Value of Periodic Events

- Optional.
- Perform this configuration as needed.
- Unless otherwise specified, run the **subscr-sample-interval** command in gRPC process configuration mode of the device that requires this configuration to change the timer value of periodic events.

Command	**subscr-sample-interval** *interval* [**millisecond** *millisecond*]
Parameter Description	*interval*: Indicates the second part in the locally configured interval for reporting periodic events. The value range is from 0 to 65535. The default value is 10s. The default timer value for periodic events is used by default. *millisecond*: Indicates the millisecond part in the locally configured interval for reporting periodic events. The value range is from 0 to 999, and the default value is 0. This value plus *interval* is the actual reporting interval, which should not be smaller than 100 milliseconds.
Command Mode	gRPC process configuration mode
Usage Guide	When the function of concerning subscribed-to periodic events is enabled on the device and the NETCONF manager sends a subscribed-to periodic event, the periodic event timer starts and gRPC data is sent to the subscribing server. If the periodic event sent by the NETCONF manager does not carry the timer value, the timer value is determined by the **subscr-sample-interval** command. If the periodic event sent by the NETCONF manager carries the timer value, the timer value sent by the NETCONF manager is used.

Configuring the Suppression Time of Real-Time Events

- Optional.
- Perform this configuration as needed.
- Unless otherwise specified, run the **subscr-realtime-interval** command in gRPC process configuration mode of the device that requires this configuration to change the suppression time of real-time events.

Command	**subscr-realtime-interval {all** *interval* **| realtime** *json-event interval***}**
Parameter Description	**all**: Configures the suppression time for all real-time events. realtime: Configures the suppression time for real-time events. Real-time events are not suppressed by default. *json-event:* Indicates the type of the configured real-time event. *interval:* Indicates the suppression interval for real-time event reporting, in milliseconds. The value range is from 1 to 1000000. No suppression interval is configured by default.
Command Mode	gRPC process configuration mode
Usage Guide	When the device subscribes to a real-time event and the threshold of the real-time event is reached, real-time packets are generated and sent to the subscribing server. If the threshold of the real-time

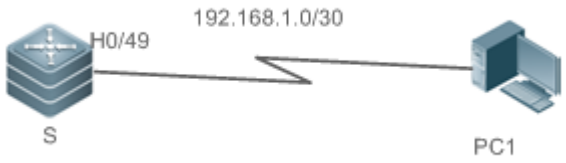
	event is triggered frequently, many packets are generated within a short time and sent to the subscribing server. These packets may be the same, and processing these packets will increase the overhead of the device and the server. To address this issue, run the **subscr-realtime-interval** command.

Verification

- Run the **show grpc subscr realtime** command to display registered real-time events.
- Run the **show grpc subscr sample** command to display registered periodic events.
- Run the **show grpc channel** [**counter**] command to display the server IP address, port number, and registered events or various statistics.

Configuration Example

Enabling the Function of Concerning Subscribed-to Real-Time Events on the Device

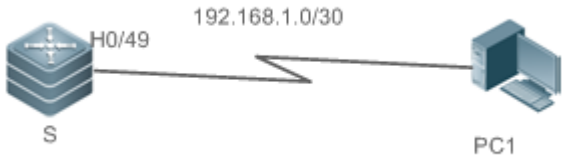
Scenario	The network communication between device S and PC1 is normal.
Figure 1-8 One-to-One Topology	
Configuration Steps	• Enable the gRPC function. • Configure the device to concern the subscribed-to CLI configuration modification real-time events. • Configure the NETCONF manager to subscribe to the CLI configuration modification real-time events.
S	`S(config)# grpc` `S(config-grpc)# subscr realtime enable`
Verification	• Run the **show grpc subscr realtime** command to display the status and statistics of the CLI configuration modification real-time event. • Run the **show grpc channel** [**counter**] command to display the server IP address, port number, and registered events or various statistics.
S	`S# show grpc subscr realtime` `S# show grpc channel counter`

Common Errors

N/A

Enabling the Function of Concerning Subscribed-to Periodic Events on the Device

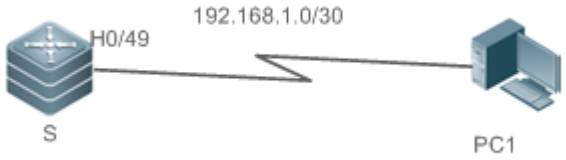
Scenario	The network communication between device S and PC1 is normal.

Figure 1-9 One-to-One Topology	
Configuration Steps	● Enable the gRPC function. ● Configure the device to concern subscribed-to DCB and PFC periodic events. ● Configure the NETCONF manager to subscribe to the DCB and PFC periodic events.
S	`S(config)# grpc` `S(config-grpc)# subscr sample enable`
Verification	● Run the **show grpc subscr sample** command to display the status and statistics of DCB and PFC periodic events. ● Run the **show grpc channel** [**counter**] command to display the server IP address, port number, and registered events or various statistics.
S	`S# show grpc subscr sample` `S# show grpc channel counter`

Common Errors

N/A

Configuring the Timer Value of Periodic Events

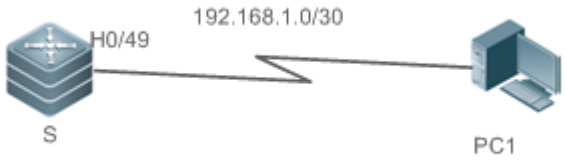
Scenario	The network communication between device S and PC1 is normal.
Figure 1-10 One-to-One Topology	
Configuration Steps	● Enable the gRPC function. ● Set the timer value for obtaining subscribed-to periodic events that need to be concerned to 10 seconds.
S	`S(config)# grpc` `S(config-grpc)# subscr-sample-interval 10`
Verification	● Run the **show grpc subscr sample** command to display the expiration time of all subscribed-to periodic events.
S	`S# show grpc subscr sample`

Common Errors

N/A

Configuring the Suppression Time of Real-Time Events

Scenario	The network communication between device S and PC1 is normal.

Figure 1-11 One-to-One Topology	
Configuration Steps	● Enable the gRPC function. ● Set the suppression time of all subscribed-to real-time events that need to be concerned to 500 milliseconds.
S	`S(config)# grpc` `S(config-grpc)# subscr-realtime-interval all 500`
Verification	● Run the **show grpc subscr realtime** command to display the suppression time of all subscribed-to real-time events.
S	`S# show grpc subscr realtime`

Common Errors

N/A

1.4.4 Specifying the Source Interface for Sending gRPC Data

Configuration Effect

- Use the IP address of the specified interface to send gRPC packets.

Notes

- The bound interface must be Up and be configured with an IP address.

Configuration Step

↘ Configuring the Source Interface for Sending Real-Time Data and Periodic Data

- Optional.
- Perform this configuration as needed.
- Unless otherwise specified, run the **subscr-source-interface** command in gRPC process configuration mode of the device that requires this configuration.

Verification

- Run the **show running** command to check whether the configuration is correct.

Related Commands

↘ Configuring the Source Interface for Sending Real-Time Data and Periodic Data

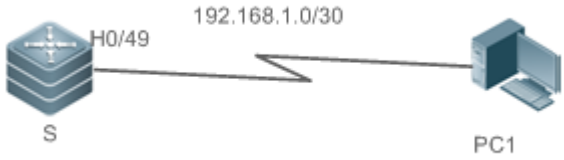
Command	**subscr-source-interface** *interface-type interface-number*
Parameter Description	*interface-type interface-number*: Specifies the type and number of a specified interface. The source interface for sending real-time data and periodic data is selected at random by default.
Command	gRPC process configuration mode

Mode	
Usage Guide	A source interface is bound at random to send real-time data and periodic data. If a server receives only packets from a specified source address, this command can be used to configure the specified source interface.

Configuration Example

Only gRPC-related configuration is described.

Binding a Specified Interface for Sending gRPC Packets

Scenario	The network communication between device S and PC1 is normal.
Figure 1-12 One-to-One Topology	
Configuration Steps	● Enable the gRPC function. ● Configure a WAN port.

S	`S(config)# interface HundredGigabitEthernet 0/49`
	`S(config-if-HundredGigabitEthernet 0/49)# ip address 192.168.1.1 255.255.255.252`
	`S(config-if-HundredGigabitEthernet 0/49)# exit`
	`S(config)# grpc`
	`S(config-grpc)# subscr-source-interface HundredGigabitEthernet 0/49`

Verification	● Check whether the configuration is saved correctly. ● Ping the server address to check whether the address is reachable. ● Check whether the communication between the device and server is normal.
S	`S# show running` `S# show grpc channel`

Common Errors

N/A

1.4.5 Configuring the Response Timeout Interval for gRPC Data

Configuration Effect

- Configure the data response timeout interval for the device serving as the gRPC server.

Notes

- The value can be set as needed. A smaller value may result in a timeout error when the GET operation involves time-consuming data.

Related Commands

Configuring the Response Timeout Time for gRPC Data

- Mandatory.

Command	**reply-timeout** *interval*
Parameter Description	*interval:* Specifies the data response timeout interval of the device serving as the gRPC server, in seconds. The value ranges from 1 to 300 and the default value is 10.
Command Mode	gRPC process configuration mode
Usage Guide	After a timeout interval is configured for the gRPC process and the collector initiates a GET/SET operation, the device returns a timeout error to the collector if it fails to obtain data within the timeout interval.

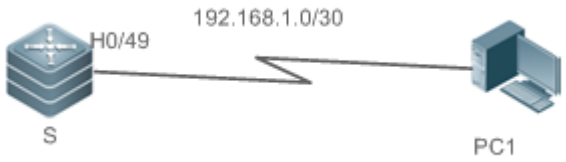
Verification

- Run the **show running** command to check whether the configuration is correct.

Configuration Example

Only gRPC-related configuration is described.

Configuring the Response Timeout Interval for gRPC Data

Scenario	The network communication between device S and PC1 is normal.
Figure 1-13 One-to-One Topology	
Configuration Steps	• Enable the gRPC function. • Configure the response timeout interval for gRPC data.
S	`S(config)# grpc` `S(config-grpc)# reply-timeout 30`
Verification	• Check whether the configuration is saved correctly. • Check whether the displayed timeout interval is the same as the configured value.
S	`S# show running`

Common Errors

N/A

1.4.6 Pre-configuring the Subscribing Server and Events to Be Subscribed to

Configuration Effect

- After the subscribing server and subscribed-to events are pre-configured, gRPC packets of corresponding events can be reported to the server.

- After the standby server is pre-configured for the subscribing server, the standby server becomes the new active server when the active server malfunctions and packets are automatically sent to the new active server.

Notes

- The IP address and port number of the subscribing server must be valid.
- The subscribed-to events and parameters must be correct and valid.

Configuration Step

Pre-configuring the Subscribing Server

- Mandatory.

Command	**user-server** *ip-address port-id*
Parameter Description	*ip-address:* Specifies the IPv4 address of the subscribing server. *port-id*: Specifies the port number of the server.
Command Mode	gRPC process configuration mode
Usage Guide	This configuration relies on the configuration described in 1.4.3 Configuring Event Types Supported by gRPC. The configuration takes effect only after the supported real-time events or periodic events are enabled. This command is used to pre-create a channel for a specified server and enter the gRPC subscribing server mode. The subscription events of this channel can be configured in this mode. By running a configuration command, the device can pre-create the subscribing server and events concerned. The device can use a configuration command to delete a server and an event that have been subscribed to, and to simulate the controller to notify the server of server and event unsubscription through NETCONF.

Pre-configuring Events to Be Subscribed to

- Mandatory.

Command	**type** *json-event* **value** *value* [**value-extend** *value-extend*]
Parameter Description	*json-event:* Specifies the type of the configured event. For details, see the **show grpc subscr | include json** command. *value:* Specifies the parameter value, that is, the threshold of real-time events and the period time of periodic events. *value-extend*: Specifies the extension field of *value*. This parameter is used to set the millisecond part in the interval for reporting periodic events. The value range is from 0 to 999. This value plus *value* should not be smaller than 100 milliseconds.
Command Mode	gRPC subscription server mode
Usage Guide	This command is used to configure subscription events and parameters of this channel and ensure that the configuration is consistent with the NETCONF configuration.

Configuring the Heartbeat Detection Mechanism

- Optional.

Command	**heartbeat inform** [**interval** *interval*] [**keepalive-times** *times*]
Parameter Description	**inform:** Enables the heartbeat detection mechanism. *interval:* Specifies the heartbeat detection interval, in seconds. The value range is from 1 to 3600. *times:* Specifies the number of heartbeat keepalive times. If the number of keepalive failures exceeds this value, it is determined that the server malfunctions. The value range is from 1 to 300. When the active server malfunctions and the standby server operates properly, data will be sent to the standby server.
Command Mode	gRPC process configuration mode
Usage Guide	This command is used to enable the heartbeat detection mechanism, and configure the heartbeat detection interval and number of heartbeat keepalive times. After the number of keepalive failures exceeds the configured value, it is determined that the server malfunctions.

Pre-configuring the Standby Server of the Subscribing Server

- Optional.

Command	**standby-server** *ip-address port-id*
Parameter Description	*ip-address*: Specifies the IPv4 address of the server. *port-id*: Specifies the port number of the server.
Command Mode	gRPC subscription server mode
Usage Guide	This command is used to configure a standby server. You need to enable the heartbeat detection mechanism first so that the device can automatically send data to the standby server when the active server malfunctions.

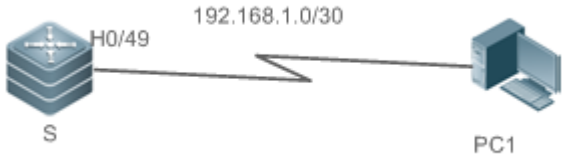
Verification

- Run the **show running** command to check whether the configuration is correct.
- Run the **show grpc channel** command to check whether the subscribing server and subscribed-to events are correct.

Configuration Example

Only gRPC-related configuration is described.

Pre-configuring the Subscribing Server and Events to Be Subscribed to

Scenario	The network communication between device S and PC1 is normal.
Figure 1-14 One-to-One Topology	
Configuration Steps	● Enable the gRPC function. ● Enable the heartbeat detection mechanism, and configure the heartbeat detection interval

	and the number of keepalive times. ● Configure the specified channel. ● Configure the specified subscription type. ● Configure the standby server.

S	`S(config)# grpc`
	`S(config-grpc)# heartbeat inform interval 1 keepalive-times 1`
	`S(config-grpc)# user-server 192.168.0.1 12345`
	`S(config-grpc-us)# type 0x10000000 value 10`
	`S(config-grpc-us)# standby-server 192.168.0.2 12345`

Verification	● Check whether the configuration is saved correctly. ● Ping the server address to check whether the address is reachable. ● Check whether the communication between the device and server is normal. ● Check whether the heartbeat link is normal, and whether data is automatically sent to the standby server when the active server malfunctions.
S	`S# show running` `S# show grpc channel`

Common Errors

The threshold range of real-time events is from –1 to +100. The period range of periodic events is from –1 to +65535. The selected event type must be available. Otherwise, the configuration is invalid and not reserved.

1.4.7 Pre-configuring the Server Login User Information

Configuration Effect

- After login user information is pre-configured for a server, the server can obtain correct information for sent obtainment event requests.

Notes

- The IP address of the server must be valid.
- The sequence number of the login user must be unique.

Related Commands

↘ Pre-configuring Server Login User Information

- Mandatory.

Command	**user-client** *id user-name ip-address*
Parameter Description	*id:* Sequence number of the login user. *user-name:* Specifies the username (which may not exist in the AAA library). *ip-address:* Specifies the allowed address.
Command Mode	gRPC process configuration mode
Usage Guide	By running a configuration command, the device can pre-create the login user information of the server that passes authentication, simulate the server to initiate a login request, pass the authentication, and save the user information.

	By running a configuration command, the device can delete login user information of the server that passes authentication, simulate the server to initiate a logout request, and delete login user information.

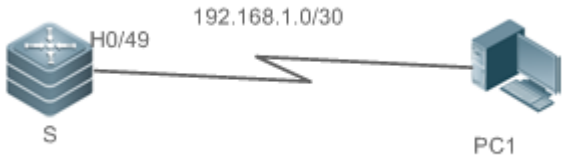
Verification

- Run the **show running** command to check whether the configuration is correct.
- Run the **show grpc client** command to display login user information.

Configuration Example

Only gRPC-related configuration is described.

Pre-configuring Server Login User Information

Scenario	The network communication between device S and PC1 is normal.
Figure 1-15 One-to-One Topology	
Configuration Steps	• Enable the gRPC function. • Configure login user information of the specified server.
S	`S(config)# grpc` `S(config-grpc)# user-client 12345 test-user 192.168.0.1`
Verification	• Check whether the configuration is saved correctly. • Ping the server address to check whether the address is reachable. • Check whether the server can obtain correct information for sent obtainment event requests.
S	`S# show running` `S# show grpc client`

Common Errors

N/A

1.4.8 Configuring a gRPC YANG Model Path and Its Group

Configuration Effect

- Configure a YANG model path (data collection source) for data collection. Then the device sends relevant data to the server configured in a subscription association.

Notes

- The YANG model path must be valid and data exists in this path.

Configuration Steps

Configuring a YANG Model Path Group

- Mandatory.

Command	**sensor-group** *group-id*
Parameter Description	*group-id*: Specifies the ID of a group.
Command Mode	gRPC process configuration mode
Usage Guide	This command is used to create a gRPC YANG model path group and switch to the gRPC YANG model group configuration mode. In this mode, you can configure multiple YANG model paths in this group.

Configuring a gRPC YANG Model Path and Its Group

- Mandatory.

Command	**sensor-path** *path*
Parameter Description	*path*: Specifies the YANG model path.
Defaults Command Mode	N/A gRPC YANG model group configuration mode
Usage Guide	This command is used to configure a YANG model path in a YANG model path group. For details on how to compile a path, refer to the output of the **show grpc yang tree/node-path** command.

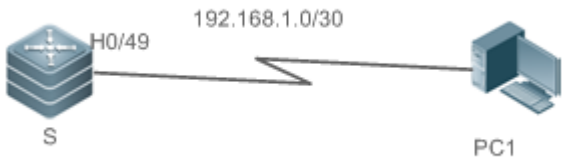
Verification

- Run the **show running** command to check whether the configuration is correct.

Configuration Example

Only gRPC-related configuration is described.

Configuring a gRPC YANG Model Path and Its Group

Scenario	The network communication between device S and PC1 is normal.
Figure 1-16 One-to-One Topology	
Configuration Steps	• Enable the gRPC function. • Configure a YANG model path group. • Configure a YANG model path.

S	`S(config)# grpc`
	`S(config-grpc)# sensor-group 1`
	`S(config-grpc-us)# sensor-path /rg-bridge:bridge/vlan/entry[id='1']/swport-list`

Verification	• Check whether the configuration is saved correctly.

S	S# show running

Common Errors

The configured YANG model path is invalid. You must check the YANG file and compile the path based on the output of the **show grpc yang tree/node-path** command.

1.4.9 Configuring the gRPC Destination Server

Configuration Effect

- Configure the address of the destination server so that the destination server subscribes to a YANG model path based on the subscription association.

Notes

- The server address and port number must be valid.

Configuration Step

Configuring a gRPC Destination Group

- Mandatory.

Command	**destination-group** *group-id*
Parameter Description	*group-id*: Specifies the ID of a group.
Command Mode	gRPC process configuration mode
Usage Guide	This command is used to create a gRPC destination group and switch to the gRPC destination group configuration mode. In this mode, you can configure multiple destination addresses in this group.

Configuring a gRPC IPv4 Destination Address

- Mandatory.

Command	**ip** *ip-address* **port** *port-id*
Parameter Description	*ip-address*: Specifies the IPv4 address of the server. *port-id*: Specifies the port number of the server.
Command Mode	gRPC destination group configuration mode
Usage Guide	This command is used to configure the IP address of the gRPC server.

Verification

- Run the **show running** command to check whether the configuration is correct.

Configuring the Protocol Used by the Destination Server

- Mandatory.

Command	**protocol grpc** {**tls** | **no-tls**}

Parameter Description	**tls**: Configures TLS encryption for gRPC. The gRPC protocol that uses TLS encrypted transmission is enabled by default. **no-tls**: Configures cleartext transmission for gRPC.
Command Mode	gRPC destination group configuration mode
Usage Guide	This command is used to configure the protocol used by the destination server.

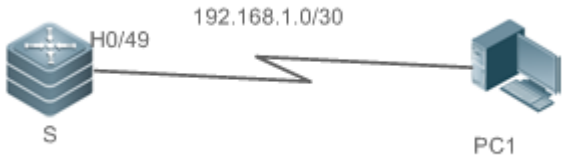
Verification

- Run the **show running** command to check whether the configuration is correct.

Configuration Example

Only the gRPC-related configuration is described.

Configuring the gRPC Destination Server and Its Group

Scenario	The network communication between device S and PC1 is normal.
Figure 1-17 One-to-One Topology	
Configuration Steps	• Enable the gRPC function. • Configure a destination group. • Configure the destination address and port number. • Configure cleartext transmission for gRPC.

S	`S(config)# grpc`
	`S(config-grpc)# destination-group 1`
	`S(config-grpc-destination)# ip 192.168.0.1 port 12345`
	`S(config-grpc-destination)# protocol grpc no-tls`

Verification	• Check whether the configuration is saved correctly. • Ping the server address to check whether the address is reachable. • Check whether the communication between the device and server is normal.
S	`S# show running`

Common Errors

N/A

1.4.10 Configuring a gRPC Subscription Association

Configuration Effect

- Configure a subscription association to enable the device to collect data of the associated YANG model path group and send the data to a destination server in the associated destination group.

Notes

- A YANG model path group must have been configured.
- A destination group must have been configured.

Configuration Step

Configuring a Subscription Association

- Mandatory.

Command	**subscription** *subscription_id*
Parameter Description	*subscription_id*: Specifies the ID of a group.
Command Mode	gRPC process configuration mode
Usage Guide	This command is used to create a gRPC subscription association and switch to the gRPC subscription association mode. In this mode, you can configure subscription associations between multiple YANG model path groups and multiple destination groups.

Configuring an Associated YANG Model Path Group and Its Data Collection Interval

- Mandatory.

Command	**sensor-group** *group_id* [**sample-interval** *interval*]
Parameter Description	*group_id*: Specifies the ID of a YANG model path group. *interval*: Specifies the interval for periodic data collection. It is not required for collection of triggered data.
Command Mode	gRPC subscription association configuration mode
Usage Guide	This command is used to configure the data source of a subscription association. If ***sample-interval*** is configured, data needs to be collected periodically. If it is not configured, triggered data needs to be collected.

Configuring an Associated Destination Group

- Mandatory.

Command	**destination-group** *group_id*
Parameter Description	*group_id*: Specifies the ID of a group.
Command Mode	gRPC subscription association configuration mode
Usage Guide	This command is used to configure the destination group of a subscription association.

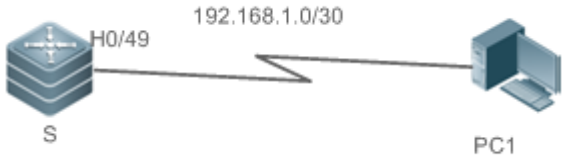
Verification

- Run the **show running** command to check whether the configuration is correct.
- Run the **show grpc openconfig subscription** command to check whether the configuration is correct.

Configuration Example

Only gRPC-related configuration is described.

Pre-configuring the Subscribing Server and Events to Be Subscribed to

Scenario	The network communication between device S and PC1 is normal.
Figure 1-18 One-to-One Topology	
Configuration Steps	● Enable the gRPC function. ● Configure a subscription association. ● Configure an associated YANG model path group and data collection interval. ● Configure an associated destination group.

S	`S(config)# grpc`
	`S(config-grpc)# subscription 1`
	`S(config-grpc-us)# sensor-group 1 sample-interval 1000`
	`S(config-grpc-us)# destination-group 1`

Verification	● Check whether the configuration is saved correctly. ● Ping the server address to check whether the address is reachable. ● Check whether the communication between the device and server is normal.
S	`S# show running` `S# show grpc openconfig subscription`

Common Errors

The YANG model path is invalid and no data exists in this path.

1.4.11 Supporting RPC Methods Defined by a Third Party

Configuration Effect

- Support RPC methods defined in **gnmi.proto**. Defined RPC methods such as Get, Set, and Subscribe can be used to collect device data.

Notes

- The device and server must be reachable to each other.

Configuration Step

Supporting RPC Methods Defined by a Third Party

- Mandatory.

Command	**rpc gnmi enable**
Parameter Description	N/A RPC methods defined by a third party are not supported by default.
Command	gRPC process configuration mode

Mode	
Usage Guide	This command is used to use RPC methods defined in **gnmi.proto**.

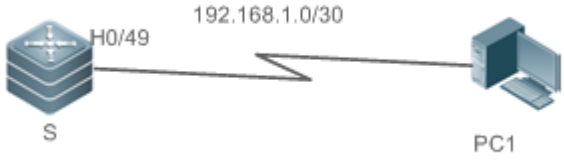
Verification

- Run the **show running** command to check whether the configuration is correct.

Configuration Example

Only gRPC-related configuration is described.

Pre-configuring the Subscribing Server and Events to Be Subscribed to

Scenario	The network communication between device S and PC1 is normal.
Figure 1-19 One-to-One Topology	
Configuration Steps	• Enable the gRPC function. • Enable the gNMI function.
S	`S(config)# grpc` `S(config-grpc)# rpc gnmi enable`
Verification	• Check whether the configuration is saved correctly.
S	`S# show running`

Common Errors

N/A

1.5 Monitoring

Clearing

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

Command	Description
clear grpc channel [*ip-address port-id*] [**counter**]	Clears statistics about the server which gRPC subscribes to.
clear grpc subscr [**sample**] [**counter**]	Clears data about periodic events and real-time events of gRPC.

Displaying

Command	Description
show grpc channel [**counter**]	Displays the server IP address, port number, and subscribed-to events or various statistics.
show grpc client	Displays gRPC server login information.
show grpc status	Displays gRPC running status information.

show grpc subscr [**realtime | sample**]	Displays status and statistics of events which are subscribed to.
show grpc openconfig subscription	Displays information about static subscription associations of the device (defined in **openconfig-telemetry.proto**).
show grpc gnmi subscription	Displays information about subscription associations generated through RPC methods defined in **gnmi.proto** on the client.
show grpc yang node-path [*module_name*]	Displays the path of a YANG node.
show grpc yang tree [*module_name*]	Displays the YANG model tree defined in the RG-gRPC YANG file.

Debugging



Debugging occupies system resources, so disable it immediately if not required.

Command	Description
debug grpc { all | **event }**	Debugs gRPC information.

1 Configuring INC

1.1 Overview

In the Simplified Optical Ethernet (SOE) Solution, the Intent-Business Network Commander (INC) function enables the device to monitor network devices in real time and manage basic services. After this function is enabled, the Google Remote Procedure Calls (gRPC) transmission protocol and YANG model data structure can make information collection and transmission between the device and the INC more efficient and convenient.

Protocols and Standards

N/A

1.2 Features

Basic Concepts

↘ INC

INC is the next-generation integrated network management platform for perception-free replacement, optical link O&M, real-time monitoring, and information collection of network devices.

↘ gRPC

gRPC uses coding in protocol buffer format and HTTP/2 as the transport layer protocol, ensuring efficient, real-time, and accurate information transmission.

Overview

Feature	Description
Enabling INC	Enables the INC function and configures gRPC-related configuration.

1.2.1 Enabling INC

Enable the INC function on the device. The device serves as the gRPC client, and the INC serves as the gRPC server. After a subscription relationship is established through gRPC, the device and INC can exchange network data.

Working Principle

After the INC function is enabled on the device, the device sends a request to the gRPC server to establish a subscription relationship. To simplify the configuration process of network administrators, the device automatically executes key configurations before exchanging data with the gRPC server. The key configurations include:

- IP address and port number of the gRPC server

  The device sends a request to this server address to try to establish a subscription relationship.
- Data sources in the YANG data model

The data source is reported by the device (gRPC client) to the INC (gRPC server).

- Association between the gRPC server and YANG model

  After the association between the gRPC server and YANG model is configured, data in the YANG model is reported only to the associated gRPC server. The device presets different sending periods for different gRPC data sent to the gRPC server. These sending periods prevent network congestion caused by simultaneous reporting of a large amount of data.

Based on the preceding pre-configured key information, the device periodically collects data based on the data paths in the YANG model and sends gRPC data requests to the INC, ensuring real-time device monitoring by the INC.

1.3 Configuration

Configuration	Description and Command	
Enabling INC	(Optional) It is used to enable INC.	
	inc-config grpc-config	Configures the gRPC server address and the subscription relationship for reporting data.

1.3.1 Enabling INC

Configuration Effect

- Configure the gRPC server address and the subscription relationship for reporting data.

Notes

N/A

Configuration Step

- Optional.
- Configure the IPv4 address of the gRPC server and the subscription relationship for reporting data in the global configuration mode of the access controller (AC).

Command	**inc-config grpc-config** *ipv4-address port*
Parameter Description	*ipv4-address*: Indicates the IPv4 address of the gRPC server. *port*: Indicates the port number of the gRPC server. The value range is from 1024 to 65535, and the default value is 30001.
Defaults	N/A
Command Mode	Global configuration mode

Usage Guide	This command is used to establish a subscription relationship between the AC and the INC and complete key configurations for message transmission between the AC and INC. The key configurations are as follows:
	1. IP address and port number of the gRPC server
	`destination-group 1`
	`  ip 1.1.1.1 port 1024`

2. Data sources in the YANG data model

```
sensor-group 1
  sensor-path /rg-interfaces:interfaces-state
  sensor-path /rg-interfaces:interfaces
  exit-sensor-group
 sensor-group 2
  sensor-path /rg-inc-wlan-dev-info:devinfo/wlan-dev-info
  exit-sensor-group
 sensor-group 3
  sensor-path /rg-inc-wlan-ap-list:aplist/wlan-ap-list
  exit-sensor-group
 sensor-group 4
  sensor-path /rg-inc-wlan-am-list:amlist/wlan-am-list
  exit-sensor-group
 sensor-group 5
  sensor-path /rg-inc-wlan-sta-list:stalist/wlan-sta-list
  exit-sensor-group
 sensor-group 6
  sensor-path
/rg-inc-wlan-statistics-info:dev-total-count/wlan-statistics-info
  exit-sensor-group
 sensor-group 7
  sensor-path /rg-inc-wlan-ap-list:netconf-ap-event/wlan-ap-list
  sensor-path /rg-inc-wlan-am-list:netconf-am-event/wlan-am-list
  sensor-path /rg-inc-wlan-sta-list:netconf-sta-event/wlan-sta-list
  exit-sensor-group
```

In the preceding pre-configuration, the device collects specified data from different data paths in the YANG model.

YANG Data Model Group	Data Path	Description
1	interfaces-state/interfaces	Interface status and information of the AC
2	wlan-dev-info	Host information of the AC
3	wlan-ap-list	List of online access points (APs)
4	wlan-am-list	List of online all-optical i-Share hosts
5	wlan-sta-list	List of online STAs
6	wlan-statistics-info	Device statistics, including the number of online APs, number of offline APs, number of all-optical i-Share hosts, and number of online STAs

3. Association between the gRPC server and YANG model and default period for reporting messages, in milliseconds

```
subscription 1
  sensor-group 1 sample-interval 300000
```

	sensor-group 2 sample-interval 300000 sensor-group 3 sample-interval 120000 sensor-group 4 sample-interval 1800000 sensor-group 5 sample-interval 60000 sensor-group 6 sample-interval 1800000 sensor-group 7 destination-group 1 ● Use the **no** form of this command on the AC to delete the configuration of a single server or all servers. After all server configurations are deleted, the gRPC function is disabled.

Verification

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

Configuration Example

↘ Enabling INC on the AC

Configuration Steps	● Enable the Network Configuration Protocol (NETCONF) on the AC. Because gRPC relies on NETCONF, NETCONF must be enabled first.
AC	Hostname # configure terminal Hostname(config)#crypto key generate dsa Hostname(config)#enable service ssh-server Hostname(config)#username admin privilege 15 password Hostname123 Hostname(config)#line vty 0 35 Hostname(config-line)#login local Hostname(config-line)#exit Hostname(config)#netconf enable Hostname(config)#netconf max-sessions 32
	● Configure the IP address and port number of the gRPC server and enable the INC function.
AC	Hostname(config)#inc-config grpc-config 172.29.4.102 30001
	● Delete the configuration of a gRPC server.
AC	Hostname(config)#no inc-config grpc-config 172.29.4.102 30001
	● Delete the configuration of all gRPC servers.
AC	Hostname(config)#no inc-config grpc-config all
Verification	● Run the **show running-config** command to display the AC configuration.
AC	Hostname#show running-config ! inc-config grpc-config 172.29.4.102 30001 ! grpc no authen login rpc gnmi enable sensor-group 1 sensor-path /rg-interfaces:interfaces-state sensor-path /rg-interfaces:interfaces

```
 exit-sensor-group
 sensor-group 2
  sensor-path /rg-inc-wlan-dev-info:devinfo/wlan-dev-info
  exit-sensor-group
 sensor-group 3
  sensor-path /rg-inc-wlan-ap-list:aplist/wlan-ap-list
  exit-sensor-group
 sensor-group 4
  sensor-path /rg-inc-wlan-am-list:amlist/wlan-am-list
  exit-sensor-group
 sensor-group 5
  sensor-path /rg-inc-wlan-sta-list:stalist/wlan-sta-list
  exit-sensor-group
 sensor-group 6
  sensor-path
/rg-inc-wlan-statistics-info:dev-total-count/wlan-statistics-info
  exit-sensor-group
 sensor-group 7
  sensor-path /rg-inc-wlan-ap-list:netconf-ap-event/wlan-ap-list
  sensor-path /rg-inc-wlan-am-list:netconf-am-event/wlan-am-list
  sensor-path /rg-inc-wlan-sta-list:netconf-sta-event/wlan-sta-list
  exit-sensor-group
 destination-group 1
  ip 172.29.4.102 port 30001
  exit-destination-group
 subscription 1
  sensor-group 1 sample-interval 300000
  sensor-group 2 sample-interval 300000
  sensor-group 3 sample-interval 120000
  sensor-group 4 sample-interval 1800000
  sensor-group 5 sample-interval 60000
  sensor-group 6 sample-interval 1800000
  sensor-group 7
  destination-group 1
  exit-grpc-subscription
!
```

Common Errors

N/A

1.4 Monitoring

Clearing

N/A

Displaying

N/A

Debugging

N/A

1 Configuring MQTT

1.1 Overview

Message Queuing Telemetry Transport (MQTT) is a transmission protocol of the International Organization for Standardization (ISO) standard (ISO/IEC PRF 20922). MQTT messages occupy low bandwidth and apply to low-bandwidth and low-power devices. Based on machine-to-machine (M2M) communication, MQTT is a lightweight messaging protocol in binary format. Based on the MQTT publish/subscribe messaging system, most operations are performed on the intermediate broker. MQTT has low requirements for performance of remote devices. Therefore, it is applied to the Internet of Things (IoT), M2M, Instance Messaging (IM), and Hypertext Transfer Protocol (HTTP).

Protocols and Standards

N/A

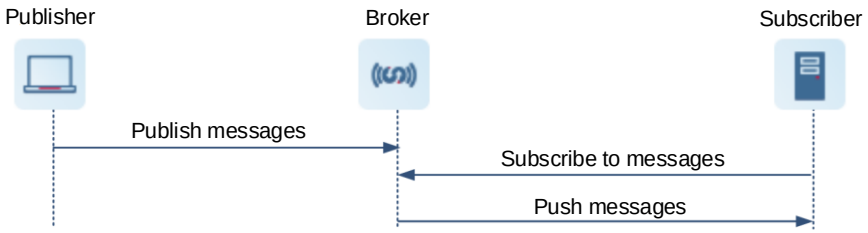
1.2 Features

Basic Concepts

↘ MQTT

Figure1-1 shows the network architecture of MQTT.

Figure 1-1 Architecture of MQTT



The MQTT protocol requires three roles: publisher, broker, and subscriber. The MQTT clients include the publisher and subscriber who publishes and subscribes to messages respectively. The server serves as a message broker. The subscriber can also publish messages as the publisher.

Messages transmitted by MQTT include the topic and payload:

- Topic: Indicates the message type. After a subscriber subscribes to a topic, the subscriber will receive the payload of this topic.
- Payload: Indicates the message content, that is, the detailed content used by a subscriber.

MQTT Client

An application or a device needs to establish a network connection with the server when using MQTT. You can perform the following operations on an MQTT client:

- Publish messages that other clients may subscribe to.
- Subscribe to messages published by other clients.
- Unsubscribe to or delete application messages.
- Disconnect from the server.

MQTT Server

The MQTT server is the broker, which can be an application or a device between the message publisher and subscriber. The MQTT server can take the following actions:

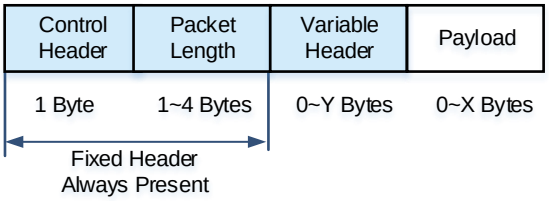
- Accept network connection requests from clients.
- Receive application information published by clients.
- Process subscription and unsubscription requests from clients.
- Forward application messages to subscribers.

MQTT Control Packets

Name	Value	Packet Flow	Description
Reserved	0	Disabled	Packet reserved
CONNECT	1	Client ---> Server	Client connecting to the server
CONNACK	2	Server ---> Client	Connection request acknowledged
PUBLISH	3	Client <--> Server	Publishing messages
PUBACK	4	Client <--> Server	Publishing request acknowledged
PUBREC	5	Client <--> Server	Message received (QoS 2 phase 1)
PUBREL	6	Client <--> Server	Message released (QoS 2 phase 2)
PUBCOMP	7	Client <--> Server	Publishing ends (QoS 2 phase 3)
SUBSCRIBE	8	Client ---> Server	The client sends a subscription request to the server.
SUBACK	9	Server ---> Client	The server confirms the subscription request.
UNSUBACRIBE	10	Client ---> Server	The client sends an unsubscription request to the server.
UNSUBACK	11	Server ---> Client	The server confirms the unsubscription request.
PINGREQ	12	Client ---> Server	Heartbeat message sent by the client

Name	Value	Packet Flow	Description
PINGRESP	13	Server ---> Client	Heartbeat response from the server
DISCONNECT	14	Client ---> Server	Disconnection request sent by the server
Reserved	15	Disabled	Packet reserved

Figure 1-2 Format of MQTT Messages



Overview

Feature	Description
MQTT Connection	Establishes a basic MQTT connection.

1.2.1 MQTT Connection

MQTT enables communication between remote sensors and control devices in a low-bandwidth and unstable network environment.

Working Principle

MQTT provides the following functions:

1 Uses the publish/subscribe messaging mode to broadcast messages to multiple clients.

Compared with a similar messaging mode, Extensible Messaging and Presence Protocol (XMPP), MQTT eliminates information redundancy and transmits data more efficiently.

2 Transmits messages with the payload content blocked.

3 Provides network connections based on TCP/IP.

Typically, MQTT is based on a TCP connection. Some MQTT versions are based on User Datagram Protocol (UDP), such as MQTT-SN. Different connection modes have their advantages and disadvantages.

4 Supports three message publishing modes to flexibly control the service quality.

- At most once

Message push completely relies on the underlying TCP/IP network. Messages may be lost, and repeated messages may occur. This mode can be used for ambient sensor data because the lost data will soon be transmitted for the second time. In this mode, messages are usually pushed through common apps. If a client is disconnected from the network when a message is pushed, the message will be lost and the client will not receive the message after reconnecting to the network.

- At least once

This mode ensures that messages can reach the destination. However, repeated messages may occur.

- Only once

This mode ensures that messages can reach the destination only once. If messages are repeated or lost, the result may be incorrect in some systems, such as the billing system. The message publishing service of the highest quality applies to these systems with strict requirements. This mode can also be used to push messages of IM apps.

5 Minimize protocol exchange to reduce network traffic.

In IoT and other environments, the computing capability of clients is poor and the network bandwidth is low, making it difficult to ensure normal network transmission. The transmission overhead of MQTT is small, and the header has a fixed length of only 2 bytes, which ensure transmission in a low-power and low-bandwidth environment.

6 Inform clients when the connection is interrupted.

Use the Last Will and Testament mechanisms to notify other devices subscribing to the same topic that the device sending the last will is disconnected.

1.3 Configuration

Configuration	Description and Command	
Establishing a Basic MQTT Connection	**mqtt-server enable**	Enables the MQTT broker service.
	mqtt-server authen login { **default-user** | **local** }	Configures the authentication mode for MQTT server login.
	mqtt-server authen aaa-config	Configures the number of attempts and timeout interval for AAA server authentication.
	mqtt-server port	Configures the port number used by MQTT.
	mqtt-server tls-port	Configures the TLS port number used by MQTT.
	mqtt-client broker username	Configures the username for the MQTT broker.
	mqtt-client broker password	Configures the password for the MQTT broker.
	mqtt-client use-tls	Configures TLS encryption for the MQTT client.

1.3.1 Establishing a Basic MQTT Connection

Configuration Effect

The server configured with MQTT enables an ordered, reliable, and bidirectional transmission connection with clients to realize topic subscription and message push.

Notes

N/A

Configuration Step

Enabling the MQTT Broker Service

- Enable the MQTT broker service on the server in global configuration mode.

Command	**mqtt-server enable**
Parameter Description	N/A
Defaults	The MQTT broker service is disabled.
Command Mode	Global configuration mode
Usage Guide	After the MQTT broker service is enabled, MQTT clients can connect to the broker to subscribe to topics and publish messages.

Configuring an Authentication Mode for MQTT Server Login

- Configure an authentication mode for MQTT server login on the broker in global configuration mode.

Command	**mqtt-server authen login** { **default-user** | **local** }
Parameter Description	N/A
Defaults	Local login is employed.
Command Mode	Global configuration mode
Usage Guide	Upon receiving a login request from the broker, the device selects AAA local authentication, AAA server authentication, or authentication exemption based on the configured authentication mode.

Configuring the Number of Attempts and Timeout Interval for AAA Server Authentication

- Configure the number of attempts and timeout interval for AAA server authentication on the broker in global configuration mode.

Command	**mqtt-server authen aaa-config** { **retry** *times* | **timeout** *second* }
Parameter Description	*times*: Indicates the number of attempts for AAA server authentication. The value range is from 1 to 100. *second:* Indicates the timeout interval, in seconds. The value range is from 0 to 300. The value 0 indicates waiting for the AAA server to time out.
Defaults	The number of attempts is 1 and the timeout interval is 4s.
Command Mode	Global configuration mode
Usage Guide	This command is used to configure the number of attempts and timeout interval for AAA server authentication during server login. You are advised not to change the number of attempts and timeout interval. If the number of attempts exceeds a limit or an improper timeout interval is configured, AAA authentication may be locked for 15 minutes. The lock can be canceled by running the **clear aaa local user lockout all** command.

Configuring the Port Number Used by MQTT

- Configure the port number used by MQTT on the server in global configuration mode.

Command	**mqtt-server port** *port*
Parameter Description	*port*: Indicates the port number. The value range is from 1025 to 65535.
Defaults	The port number is 1883.
Command Mode	Global configuration mode
Usage Guide	The default port number is 1883. The port number can be reconfigured.

Configuring the TLS Port Number Used by MQTT

- Configure the TLS port number used by MQTT on the server in global configuration mode.

Command	**mqtt-server tls-port** *port*
Parameter Description	*port*: Indicates the port number. The value range is from 1025 to 65535.
Defaults	The TLS port number is 8883.
Command Mode	Global configuration mode
Usage Guide	The default TLS port number is 8883. The port number can be reconfigured.

Configuring the Username for the MQTT Broker

- Configure the username for the MQTT broker on the client in global configuration mode.

Command	**mqtt-client broker username** *username*
Parameter Description	*username*: Indicates the username of the MQTT broker.
Defaults	The username is **ruijie**.
Command Mode	Global configuration mode
Usage Guide	The username and password are required for MQTT broker authentication. Configure the username before connecting to the server.

Configuring the Password for the MQTT Broker

- Configure the password for the MQTT broker on the client in global configuration mode.

Command	**mqtt-client broker password** *password*
Parameter Description	*password*: Indicates the password of the MQTT broker.
Defaults	The password is **Ruijie_mosquitto_pwd**.
Command Mode	Global configuration mode
Usage Guide	The username and password are required for MQTT broker authentication. Configure the password

	before connecting to the server.

Configuring TLS Encryption for the MQTT Client

- Configure TLS encryption for the MQTT client in global configuration mode.

Command	**mqtt-server enable**
Parameter Description	N/A
Defaults	TLS encryption is configured.
Command Mode	Global configuration mode
Usage Guide	TLS encryption is employed for the MQTT client by default. To disable TLS encryption, run the **no** form of the command.

Verification

N/A

Configuration Examples

Enabling the MQTT Broker

Configuration Steps	• Use this command to enable the MQTT broker.

Server	`Hostname> enable`
	`Hostname# configure terminal`
	`Hostname(config)# mqtt-server enable`

Verification	• N/A

Common Errors

- N/A

1.4 Monitoring

Clearing

N/A

Displaying

Command	Description
show mqtt clients	Displays information about the connected MQTT client.

Debugging

N/A

1.5 Configuration Examples

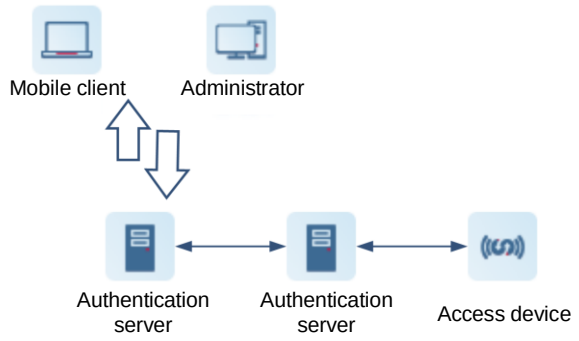
1.5.1 Configuring Basic MQTT Functions

1.5.1.1 Requirements

Enable the MQTT function and establish an MQTT message channel.

1.5.1.2 Topology

Figure 1-3 Topology for Basic MQTT Functions



1.5.1.3 Notes

- The link between the MQTT server and device is reachable.
- The MQTT broker service is enabled on the MQTT server.

1.5.1.4 Procedure

Enable the MQTT broker.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# mqtt-server enable
```

Configure AAA local authentication with the username and password for the MQTT broker.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# mqtt-server login local
DeviceA(config)# username mqtt_user password Mqtt_password
```

Configure the username and password for the client.

```
DeviceA> enable
DeviceA# configure terminal
```

```
DeviceA(config)# mqtt-client broker username mqtt_user
DeviceA(config)# mqtt-client broker password Mqtt_password
```

1.5.1.5 Verification

Run the **show mqtt clients** command on the MQTT client to display MQTT client information.

```
DeviceA#show mqtt clients
count: 2

id: ac-001a.2c18.82af
    sock: 580
    username: DeviceA
    address: 127.0.0.1
    sub_count: 5
    last_msg_in: 408672
    next_msg_out: 408687

id: am/c0b8.e64e.e374/2
    sock: 1415
    username: DeviceA
    address: 16.30.49.1
    sub_count: 4
    last_msg_in: 408672
    next_msg_out: 408687
```

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

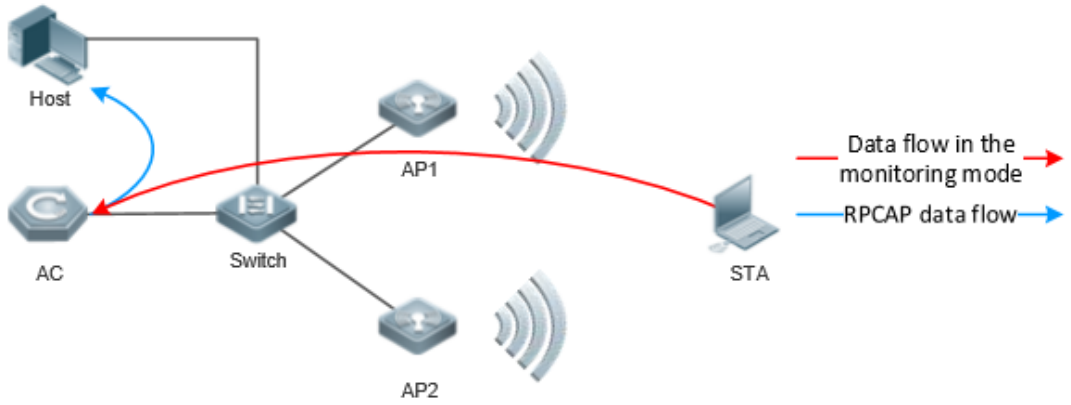
Application	Description
Remote Packet Capture in Fit AP Mode	In fit AP mode, enable the wireless sniffing service on the access controller (AC). The remote host sniffs packets on the radio port of the fit AP through packet sniffing tools.

1.2.1 Remote Packet Capture in Fit AP Mode

Scenario

In fit AP mode, the remote host enables the monitoring mode on the radio 1 port of the AP 1 through packet sniffing tools that support RPCAP and captures wireless packets (including packets between the STA and the radio 1 port of the AP 2 which shares the same channel with the radio 1 port of the AP 1).

Figure 1-1 RPCAP Remote Packet Capture in Fit AP Mode



Note: Switch: Indicates a switch.
AC: Indicates a wireless controller.
Host: Indicates a remote host.

Deployment

- Enable the remote packet capture service on the AC.
- Configure the radio 1 port of the AP 1 as the port for packet capture in the AP 1 configuration mode on the AC.
- 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.

CAPWAP Tunnel

On the fit AP network, the AC manages all APs through a Control and Provisioning of Wireless Access Points (CAPWAP) tunnel. Control policies sent to the APs do not need to be independently configured on the APs. The CAPWAP protocol establishes the control channel and data channel between the APs and the AC. The control channel is used by the AC to configure the APs and used by the APs to send event advertisements to the AC. The data channel is used to send data packets between the APs and the AC.

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

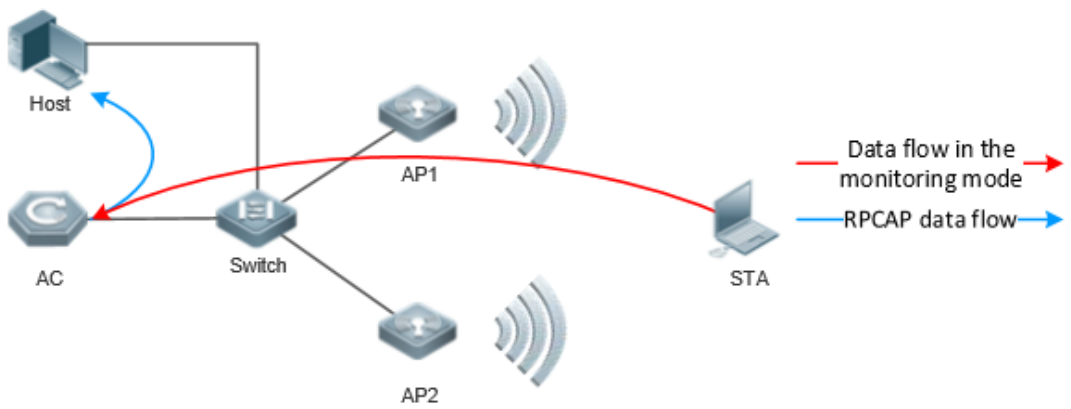
The remote packet capture function is based on the RPCAP protocol. RPCAP uses the control channel and data channel to communicate with the packet sniffing tool. The control channel is used to transmit signaling based on reliable TCP connection. The data channel is used to transmit captured data based 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 ACs. This enables remote hosts to control the wireless sniffing process on the radio port of APs which are managed by ACs 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 sends them to the AC through the CAPWAP tunnel.
3. The AC encapsulates the wireless packets with the RPCAP protocol header and sends them to the remote host.
4. 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.
AC: Indicates a wireless controller.
Host: Indicates a remote host.

1.4 Configuration

Configuration	Description and Command	
Configuring the Wireless Sniffing Function	(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.
Configuring the Packet Sniffing Policy	(Optional) It is used to configure the channel for packet capture and the forwarding mode for sniffed packets.	
	forward	Configures the forwarding mode for sniffed packets.
Enabling Wireless Sniffing	(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 fit AP.

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	AP configuration mode and AP group 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 Fit AP Mode

Configuration Steps	Use this command to enable the wireless sniffing function on radio 1 of online AP 1. The wireless sniffing function on radio 1 of offline AP 2 fails to be enabled.
AC	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# ap-config AP1 Hostname(config-ap)# wlan-cap enable radio 1 Hostname(config-ap)# exit Hostname(config)# ap-config AP2 Hostname(config-ap)# wlan-cap enable radio 1 The ap is not online.
Verification	Run the following command to display wireless sniffing configuration on a specified port.
AC	Hostname# show wlan-cap interface Wlan capture interface info: Total Interface : 2 Total capturing Interface : 0 Total Idle Interface : 2 AP Name MAC Address Type Index Channel Status Users ----- --------- -------------- ----- ----- ------- ------- ----- AP1 00d0.f822.33d0 radio 1 11 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.
- When RPCAP packets are being captured in listening mode, connection status and packet interaction of users associated with the corresponding RF port cannot be guaranteed.

Configuration Steps

Entering the Wireless Sniffing Configuration Mode

- Optional.
- The listening port and login information can be configured only on the AC.

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 AC.

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 AC.

- Configuring RPCAP remote access information includes configuring the port to be accessed and the username and password used for remote host login.

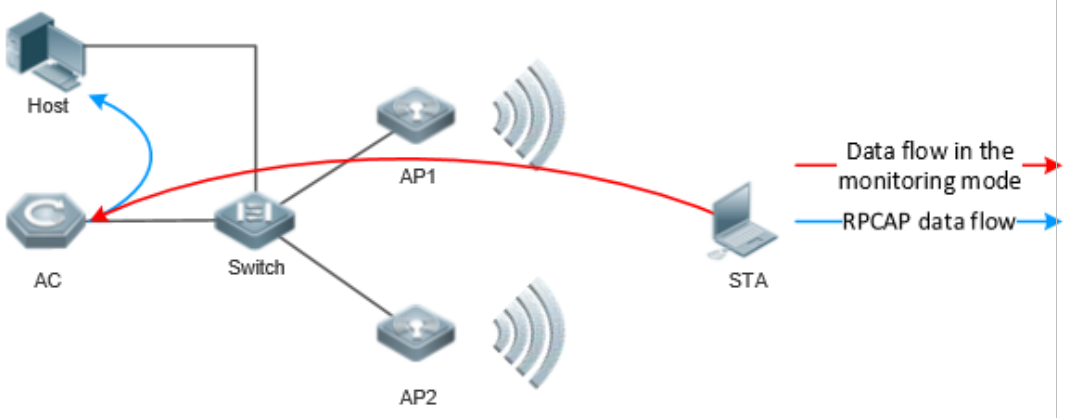
Command	**rpcap login** *username password*
Parameter Description	*username*: Indicates the username used for login. *password*: Indicates the password used for login.
Defaults	No username and password are configured by default.
Command Mode	Wireless sniffing configuration mode
Usage Guide	N/A

Verification

Run the **show wlan-cap config** command to display wireless sniffing configuration.

Configuration Example

Setting the Listening Port Number of the AC to 65535 in the Fit AP Mode

Scenario **Figure** 1-2	
Configuration Steps	● Use this command to enter the wireless sniffing configuration mode and set the listening port to 65535 for RPCAP remote access.
AC	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#wlan-cap Hostname(wlan-cap)#rpcap port 65535
Verification	Run the following command to display wireless sniffing configuration.
AC	Hostname#show wlan-cap config ========================== Wlan-cap-config ====================== Listen port: 65535 Login info: Anonymous Forward: Central Service enable: No

Configuring Login Information for the AC

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**.
AC	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# wlan-cap Hostname(wlan-cap)# rpcap login wlan-capture wlan-capture
Verification	Run the following command to display wireless sniffing configuration.
AC	Hostname# 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 Configuring the Packet Sniffing Policy

Configuration Effect

- A packet sniffing policy can be configured to obtain packets from the channel of the current AP radio and to specify whether the packets obtained by the AP are forwarded to the remote host directly by the AP or forwarded by the AC.

Notes

- N/A

Configuration Steps

↘ Configuring the Forwarding Mode

- Optional.
- The forwarding mode can be configured only when wireless sniffing is disabled. It is configured on the AC.
- Configure a packet sniffing policy for the remote host to specify the AP channel for sniffing and determine whether the packets captured by the AP are forwarded to the host by the AC or directly by the AP.

Command	**forward** { **central** | **local** }
Parameter Description	**central**: Indicates centralized forwarding. Packets captured by the AP are forwarded to the remote host by the AC. **local**: Indicates local forwarding. Packets captured by the AP are directly forwarded to the remote host.
Defaults	The forwarding mode is centralized forwarding by default.
Command Mode	Wireless sniffing configuration mode
Usage Guide	N/A

Verification

- Display wireless sniffing configuration to check the configured packet sniffing policy.

Configuration Example

Configuring the Forwarding Mode

Configuration Steps	• Use this command to enter the wireless sniffing configuration mode • and set the forwarding mode to local forwarding on the AC.
AC	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# wlan-cap Hostname(wlan-cap)# forward local
Verification	Run the following command to display wireless sniffing configuration on the AC.
AC	Hostname#show wlan-cap config ========== Wlan-cap-config ========== Listen port: 2002 Login info: Anonymous Forward: Local Service enable: No

Common Error

N/A

1.4.4 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 AC, 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	Wireless sniffing configuration mode

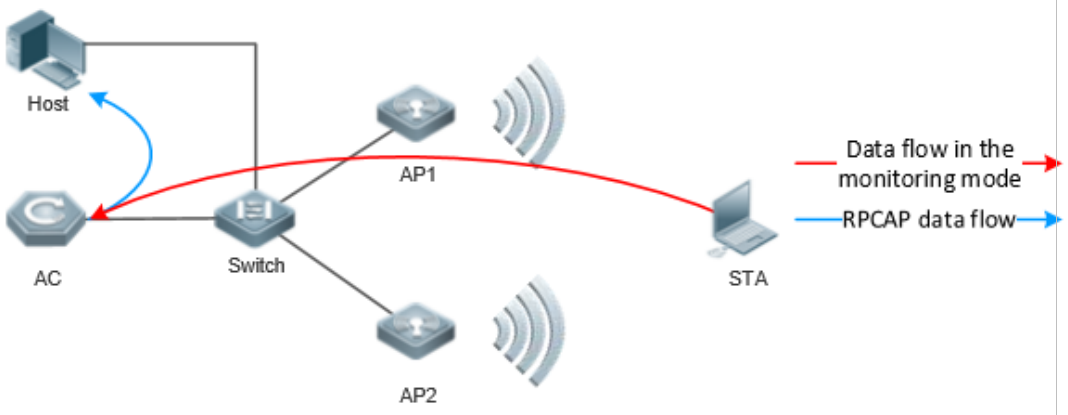
Mode	
Usage Guide	After wireless sniffing is enabled, only the sniffed channel can be modified, and the other configurations cannot be modified in this configuration mode.

Verification

Run the **show wlan-cap config** command to check whether wireless sniffing is enabled.

Configuration Example

Configuring Wireless Sniffing on the AC

Scenario **Figure** 1-3	
Configuration Steps	● Use this command to enter the wireless sniffing configuration mode and enable wireless sniffing on the AC.
AC	Hostname# configure terminal Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)# wlan-cap Hostname(wlan-cap)# service enable
Verification	Run the following command to display wireless sniffing configuration on the AC.
AC	Hostname#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 Gateway

1. Configuring Application Identification
2. Configuring AEM
3. Configuring QoS-based Key Service Assurance
4. Configuring DNS-CACHE
5. Configuring RNFP

1 Configuring Application Identification

1.1 Overview

Application identification refers to classification and identification of a network data flow based on application characteristics. Application identification analyzes packet payload and flow characteristics to obtain the application protocol type of the data flow. It detects and identifies content at layers 4 to 7 of a packet and some protocols (such as HTTP, TCP, and RTP). The application identification technology classifies and identifies specific applications by matching feature codes in data packets.

Application identification provides application class information for other functional modules, such as key service assurance, flow control, and traffic audit. The service module can be used for application quality analysis and application assurance policy control based on the service flow identification result.

At present, APP-ROUTE distributes application traffic depending on the initial packet identification technology. For the TCP flow, due to a lack of payload in the handshake packet, initial packet identification cannot be implemented based on the Deep Packet Inspection (DPI) rule.

1.2 Applications

Application	Description
Egress Gateway Deployment	Deploys application identification on the egress gateway.

1.2.1 Egress Gateway Deployment

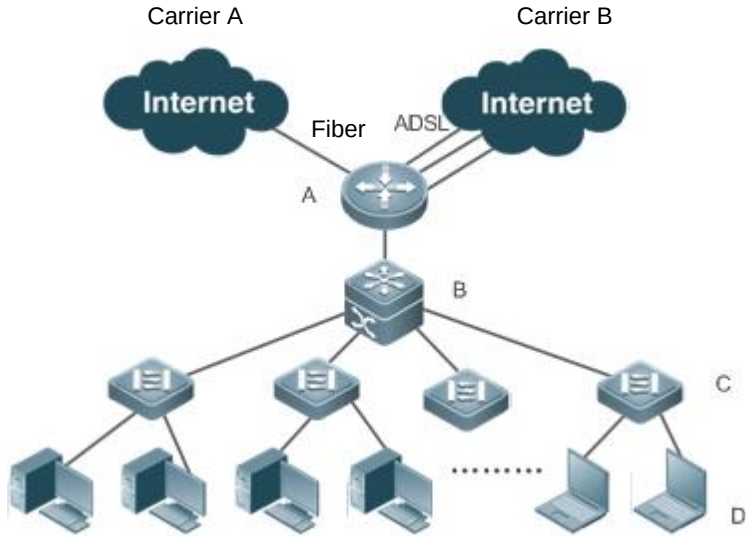
Scenario

An egress gateway can connect to lines of different operators, for example, one fiber line of China Telecom and one Asymmetric Digital Subscriber Line (ADSL) of China Unicom, or one fiber line of China Telecom and multiple ADSLs of China Unicom.

Functions that rely on application identification include:

- Flow control
- Flow audit
- Application routing
- Content audit

Figure 1-1 Typical Application Scenario of Egress Gateway



Remarks	A indicates an egress gateway. B indicates a core switch. C indicates an access switch. D indicates an intranet PC.

Deployment

Basic NAT: Implement basic network address translation (NAT) to ensure that clients access the Internet normally.

Application identification: Indentify the application with traffic forwarding, and cooperate with the flow control module to implement application-based flow control.

Application routing: Enable traffic of heavy-traffic applications or key applications to be transmitted via specified egress ports based on application identification.

Multi-link load balancing: Distribute traffic of data flows to multiple links to ensure proper utilization of bandwidth.

Flow control: Implement rate limitation on P2P download traffic and realize functions such as traffic guarantee of key applications in combination with application identification.

Flow audit: Provide application-based traffic reports in combination with application identification, so that users can learn whether the egress bandwidth is sufficient and whether capacity expansion is needed.

1.3 Features

Basic Concepts

Data Flow

A data flow is a flow of packets with the same 5-tuple. According to protocols, data flows fall into three types: TCP flow, UDP flow, and IP flow (specific for non-TCP/UDP applications). The following table describes the 5-tuple of different data flows:

Flow Type	5-tuple Identifier

TCP flow	Source IP address|destination IP address|IP|TCP source port|TCP destination port
UDP flow	Source IP address|destination IP address|IP|UDP source port|UDP destination port
IP flow	Source IP address|destination IP address

Application Routing

To ensure effective utilization of network resources, it is proposed that enterprises or Internet cafes rent two (or multiple) WAN links and use one high-quality line for transmitting data of key applications that are sensitive to transmission delay and jitter and use the other low-quality line for transmitting data of P2P and other download applications. To realize the method, the egress gateway should be able to route packets based on applications. Different from the conventional IP routing technology that is based on the destination IP address of a packet, application-based routing (also referred to as application routing for short) is a routing and forwarding technology that is based on application types of data flows. With the application routing technology, traffic of data flows of different application types can be distributed to different egress ports, to separate data flows of key services from data flows of rate-limited services and to minimize impact. The major problem of application routing is how to identify the initial packet of data flows. For details about application routing, refer to relevant descriptions.

Initial Packet Identification

The capability of identifying the first packet of each flow is initial packet identification. This function ensures the application routing effect. If packet identification starts from the midway of a data flow, the flow will be transmitted along at least two lines, which will cause flow interruption. For the TCP flow, the initial packet is a handshake packet, and the first payload packet is a request packet.

Overview

Feature	Description
Signatures Database Upgrade	Upgrades the signature database of the gateway.
Application Protocol Object Management	Manages application protocol objects.
Application	Identifies the application with traffic forwarding, and cooperates with the flow control module to implement application-based flow control.
Application Identification of the AP with the Assistance of the AC	The AC assists the AP in performing application identification.
URL Identification	Enables URL identification.

1.3.1 Signatures Database Upgrade

As software is upgraded, packet characteristics of the software may change. With signature database upgrade, packet characteristics are updated to ensure accurate and effective application identification without software upgrade.

Working Principle

The professional signature database analysis team of Ruijie Networks formulates a mature characteristics analysis procedure. According to the procedure, the team analyzes packet characteristics of different applications and constantly update the characteristics to the signature database.

Users can download the signature database from the provided URL or obtain the signature database from the customer service center and then upgrade the local signature database on a Web portal. Alternatively, the signature database can be automatically updated to the latest version via Web settings from the Ruijie signature database server, which is convenient and ensures automatic and timely update.

Signatures database upgrade is a procedure of analyzing and processing the compressed signature database package (app_signature.upd) to form matching rules relevant to application identification.

After the signature database is upgraded successfully, application identification will store the signature database to the flash memory. After the gateway restarts, the signature database in the flash memory is automatically upgraded.

1.3.2 Application Protocol Object Management

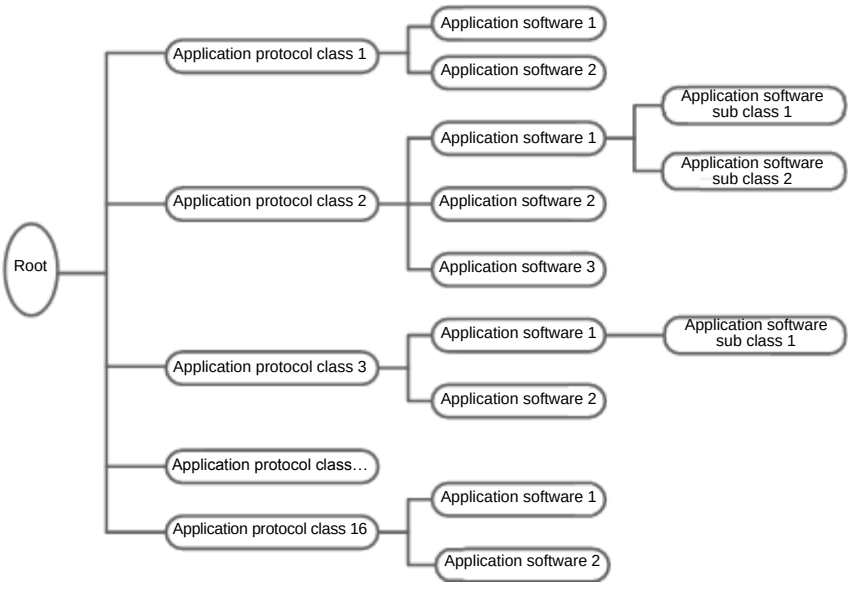
By grouping application protocol objects, application protocol object management is simplified. By defining applications, users can define application protocol objects according to the 5-tuple information and add the user-defined application protocol objects into groups for management.

Working Principle

Protocol Objects of Signatures Database

By parsing the signature database, class objects are generated and a protocol tree is formed. Figure 1-2 shows the organization form.

Figure 1-2 Protocol tree



Applications are organized at three levels (application protocol class, application software, and application software sub class) to form a protocol tree in the system.

User-defined Application

Packets compliant with specific 5-tuple attributes are defined as one type of user-defined application.

Matching of user-defined applications is dedicated for TCP, UDP, and IP packets. Users extract the source and destination IP addresses, source and destination ports, and protocol ID from packets and query the data structures of the user-defined applications to determine whether there is a matched user-defined application.

User-defined applications are added to the same tree as other applications. The entire system has only one protocol tree, which contains all applications, including user-defined applications.

Application Grouping

Applications can be grouped by the default classes of the system, preset groups of the system, or user requirements.

According to the default classes of the system, applications are classified into the following types: instant messaging, VoIP, network game, video streaming, P2P, stock, Internet file transfer, email, database, network management protocol, routing protocol, security protocol, tunnel application, remote access protocol, network application update, online banking, network hard disk, software update, mobile Internet downloader, mobile Internet video/audio, mobile Internet web disk, mobile Internet software update, mobile Internet instant messaging, mobile Internet game, mobile Internet social network, mobile Internet web browsing, mobile Internet stock, and RFC. The classification is based on the actual signature database.

According to the preset groups of the system, applications are classified into the following groups: key application group, rate-limited application group, blocked application group, Other application group, Web_Group, Online_Video_Group, P2p_Video_Group, Download_Group, P2p_Group, Update_Group, Upload_Group, High_Group, Middle_Group, and Low_Group. The names of these application groups cannot be modified, but users can add the default classes of the system or an application of a class into the groups. Some system applications (with the index of x-0-0-0) belong to the other application group by default.

Applications can be grouped according to user requirements as well. Users can add the default classes of the system or an application of a class into the user-defined group.

1.3.3 Application Identification

Application identification identifies application attributes of data flows so that other modules execute policy actions according to the application attributes.

Working Principle

Application identification identifies the application attributes of data flows using technologies such as predictive identification, DPI, detective identification, Deep/Dynamic Flow Inspection (DFI), and length sequence identification.

Predictive Identification

Some application protocols have distinct flow characteristics. For example, a flow may contain information such as an IP address and a port for subsequent sessions. With an analysis on the flow information, flow characteristics are extracted and recorded. Subsequent flows that comply with the characteristics can be identified as flows of the application. The predicted characteristics will age after a period of time. Users can configure the aging time.

Detective Identification

Some application protocols may generate unknown encrypted data flows. The Ruijie gateway can identify the application type corresponding to this type of encrypted data flows using detection mechanisms.

DPI

DPI is specific for payloads of packets. By parsing the packet payloads based on the protocol layer, the DPI identifies the protocol type and port of the packets, encodes the payloads, and then matches the payload content with the strings in the signature database. Multiple models are used to match and identify the payload characteristics. If different match

results are obtained, the DPI selects a final result based on priorities. If the protocol type of an application has to be determined by identifying payloads of multiple packets, the status tracking module will trace the status.

QUIC Identification

Quick UDP Internet Connections (QUIC) identification is a part of DPI identification used to identify QUIC packets. After decoding QUIC packets, the system matches the decoding content with the feature string in the feature library to obtain the corresponding identification result.

DFI

DFI is a technology that identifies applications based on flow characteristics. Generally, session connections or data flow statuses vary with the specific application type, for example, the P2P download flow and voice flow. DFI identifies the characteristics of the data flows, builds flow classifiers, and then classifies the data flows using the classifiers, thereby implementing smart identification of application types.

QUIC Identification

When application identification is enabled, QUIC identification is enabled by default.

Run the **identify-application quic enable** command to disable QUIC identification.

After QUIC identification is disabled, applications that use QUIC packets cannot be identified. Typically, you are advised to enable QUIC identification.

Length Sequence Identification

Packet payloads generated by some applications, though encrypted, feature a fixed length. Based on this characteristic, encrypted P2P download flows can be identified. A typical example is the eDonkey encrypted download flow.

1.3.4 Application Identification of the AP with the Assistance of the AC

The AP performs application identification with the assistance of the AC.

Working Principle

In local forwarding mode, the AP mirrors some initial packets of a data flow to the AC (the number of mirrored packets vary with different protocols). The AC identifies the application based on the packets and sends the identification result to the AP to assist the AP in performing application identification.

1.3.5 URL Identification

Identify data stream attributes of users' Uniform Resource Locator (URL) access requests, so other modules can enforce corresponding policies based on the attributes.

Working Principle

HTTP identifies URL attributes corresponding to a data flow based on URL information in GET, POST, PUT, and HEAD request packets.

HTTPS identifies URL attributes corresponding to a data flow based on host information in client and server Hello packets.

Related Configuration

Enabling URL Identification

Run the **identify-url enable** command to enable URL identification globally.

Adding an HTTP port

Run the **identify-url http-port** *port-num* command to add the HTTP port used by a website whose URL is not identified by default port 80 or 8080 to the port identification list so that the website URL can be identified.

Adding an HTTPS port

Run the **identify-url https-port** *port-num* command to add the HTTPS port used by a website whose URL is not identified by default port 443 or 8080 to the port identification list so that the website URL can be identified.

Adding a URL Group

Run the **identify-url url-group** *group-id* [**name** *group-name*] command to add a custom URL group for a control policy, such as the ACL function.

Adding a URL Object

Run the **identify-url url-name** *url-name* **regexp** *regexp* command to add a custom URL object.

Adding the URL Object to the Custom URL Group

Run the **url** *url-name* command in URL group configuration mode to add the URL object to the custom URL group.

1.4 Configuration

Configuration	Description and Command	
Upgrading Signatures Database	(Mandatory) It is used to build a protocol tree and rules of the signature database.	
	Identify-application signature update	Triggers signature database upgrade.
Defining Applications	(Optional) It is used to define application rules.	
	identify-application custom name	Defines application rules.
Grouping Applications	(Optional) It is used to manage application protocol objects.	
	identify-application clear key-inhibitive-block-other group	Clears all the applications in the key application group, rate-limited application group, and blocked application group.
	identify-application custom-group	Defines a group.
	app-add	Adds applications to the user-defined group.
	app-del	Deletes applications from the user-defined group.

	identify-application block	Blocks applications from the user-defined group.
	identify-application key	Adds an application to the key application group.
	identify-application inhibitive	Adds an application to the rate-limited application group.
	identify-application other	Adds an application to the Other application group.
	identify-application web-group	Adds an application to Web_Group.
	identify-application online-video-group	Adds an application to Online_Video_Group.
	identify-application p2p-video-group	Adds an application to P2p_Video_Group.
	identify-application download-group	Adds an application to Download_Group.
	identify-application p2p-group	Adds an application to P2p_Group.
	identify-application update-group	Adds an application to Update_Group.
	identify-application upload-group	Adds an application to Upload_Group.
	identify-application high-group	Adds an application to High_Group.
	identify-application middle-group	Adds an application to Middle_Group.
	identify-application low-group	Adds an application to Low_Group.
Configuring A	(Mandatory) It is used to enable application identification.	
	identify-application enable	Enables application identification.
	identify-application proto-detect enable	Enables detective identification.
	identify-application proto-expect enable	Enables predictive identification.
	identify-application proto-expect timeout	Sets aging time of protocol information.
	identify-application dpi enable	Enables DPI.
	identify-application quic enable	Enables QUIC identification.
	identify-application dfi enable	Enables DFI.
	identify-application len-seq enable	Enables length sequence identification.
	identify-application app-db enable	Enables the application collection function.
Configuring the L2 Application Identification Feature of the AC	(Optional) It is used to enable the L2 application identification feature on the AC.	
	identify-application ac-enable compatible	Enables the L2 application identification feature on the AC.
Configuring Application Identification of the AP with the Assistance of the AC	**identify-application ap-enable**	Enables application identification of the AP with the assistance of the AC.
	identify-application ap-db	Configures information about application groups that can be identified by the AP.
Configuring URL Identification	(Mandatory) It is used to enable URL identification.	
	identify-url enable	Enables URL Identification
	identify-url http-port	Adds an HTTP port for URL identification.
	identify-url https-port	Adds an HTTPS port for URL identification.
	identify-url url-group	Adds a custom URL group.

	identify-url url-name	Configures a custom URL object.
	url	Adds a URL object to a custom URL group.
Configuring the Language in Which Application Identification Information Is Displayed	**identify-application signature language**	Configures the language in which application identification information is displayed.

1.4.1 Upgrading Signatures Database

Configuration Effect

Build a protocol tree of the signature database.

Create or update the signature database rules.

Notes

If the current database version of the gateway is consistent with the target database version, the upgrade fails.

Configuration Step

Upgrading Signatures Database

Mandatory.

Upgrade the signature database on the egress gateway. Obtain the signature database from the official website to the local PC, download the compression package of the signature database to the gateway, and then upgrade the local signature database on the web portal. Alternatively, the signature database can be updated in HTTP mode.

⚠ For details about HTTP upgrade, refer to relevant documents. This document mainly describes the configuration method of local upgrade. If the upgrade is implemented via a web portal or automatic update, users do not need to run relevant commands to trigger signature database parsing.

Verification

Check the version number of the signature database to determine whether the signature database is upgraded successfully.

Related Commands

Upgrading Signatures Database

Command	**Identify-application signature update**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Download the compression package of the signature database to the gateway and run this command to trigger signature database upgrade.

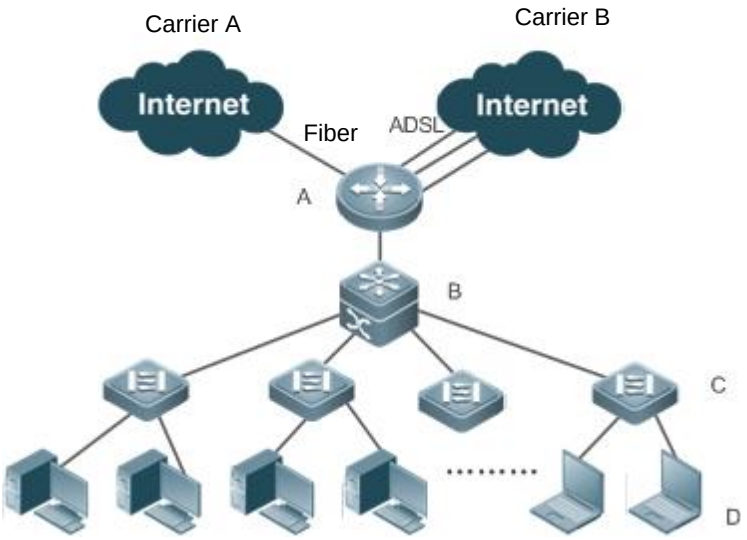
Displaying Version Number of Signatures Database

Command	**show identify-application version**

Parameter Description	N/A
Command Mode	Privileged EXEC mode, global configuration mode, and interface configuration mode
Usage Guide	N/A

Configuration Example

Upgrading Signatures Database

Scenario Figure 1-3	
Configuration Steps	1. Choose **Advanced** > **System Upgrade** > **Signatures Database Download** > **Download Application Database** to download the signature database package to the gateway. 2. Decompress the package, choose **Advanced** > **System Upgrade** > **Local Upgrade** to select the **app_signature.upd** file in the package directory, and click **Start** to upgrade the signature database. The system will prompt upgrade success after the upgrade.
A	`Hostname#*Apr 25 14:08:55: %DPI-5-LOCAL_UPDATE: Local signature database upgrading.` `Hostname#*Apr 25 14:10:14: %DPI-5-SIGNATURE_UPDATE: Signature database is upgraded successfully!`
Verification	3. Run the **show identify-application version** command to display the version number of the signature database.
A	`Hostname#show identify-application version` `Version:2013.05.22.13.05.22(V2.0)`

Common Errors

The current database version of the gateway is consistent with the target database version.

1.4.2 Defining Applications

Configuration Effect

Define applications and identify application traffic based on the 5-tuple information.

⚠ If the gateway does not have a signature database, user-defined applications cannot be identified.

Notes

User-defined applications fall into the following types:

Protocol type and source and destination ports

Protocol type, source IP address, and source port

Protocol type and source and destination IP addresses

Protocol type, destination IP address, and destination port

Pay attention to the following limits during configuration:

For the first type of applications, the source and destination ports cannot be set to **any** at the same time.

For the second type of applications, neither the source IP address nor the source port can be set to **any**.

For the third type of applications, the source and destination IP addresses cannot be set to **any** at the same time.

For the fourth type of applications, neither the destination IP address nor the destination port can be set to **any**.

A single IP address or an IP address segment can be configured. In the IP address segment, the number of IP addresses cannot be greater than 32 and the IP addresses must be consecutive.

Users can add characteristics to an existing application or application class. The original characteristics of the existing application or application class are not affected but are less prioritized than the user-defined application characteristics.

The name of a user-defined class contains no more than 31 characters, and the name of a user-defined application contains no more than 27 characters.

If user-defined applications share a source or destination IP address, a maximum of 16 port configurations can be configured for the applications. For example, for the combination of destination IP address + destination port, the possible configurations are IP:1.1.1.1 + port:80, IP:1.1.1.1 + port:100, and IP:1.1.1.1 + port:200.

Both the source IP address and the destination IP address cannot be 0.

Configuration Step

Run relevant commands in global configuration mode to create applications.

Verification

Check whether the user-defined applications are created successfully.

Related Commands

Defining Rules

Command	**identify-application custom name** *software-name* **class** *class-name* { **ip sip** { **any any** | *sip-low sip-high* } **dip** { **any any** | *dip-low dip-high* } **|** { **tcp** | **udp** } { **sport** { **any any** | *sport-low sport-high* } **dport** { **any any** | *dport-low dport-high* } | **sip** { **any any** | *sip-low sip-high* } { **sport** { **any any** | *sport-low sport-high* } | **dip** { **any any** | *dip-low dip-high* } } | **dip** { **any any** | *dip-low dip-high* } **dport** { **any any** | *dport-low dport-high* } } }
Parameter Description	*software-name*: Indicates an application name. *class-name*: Indicates an application class name. *sport-low*: Indicates the start source port. The value ranges from 0 to 65,535 or is **any**.

	sport-high: Indicates the end source port. The value ranges from 0 to 65,535 or is **any**. *dport-low*: Indicates the start destination port. The value ranges from 0 to 65,535 or is **any**. *dport-high*: Indicates the end destination port. The value ranges from 0 to 65,535 or is **any**. *sip-low*: Indicates the start source IP address (IPv4). *sip-high*: Indicates the end source IP address (IPv4). *dip-low*: Indicates the start destination IP address (IPv4). *dip-high*: Indicates the end destination IP address (IPv4).
Command Mode	Global configuration mode
Usage Guide	N/A

Displaying Defined Rules

Command	**show identify-application custom- rule**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Defining Rules

Configuration Steps	Define a rule.
	Hostname# configure terminal Hostname(config)#identify-application custom name XLgame class Custom Game tcp sport 1 10 dport 1 100
Verification	Display the defined rule on the gateway.
	Hostname#show identify-application custom-rule TYPE NAME CLASS SPL SPH DPL DPH SIPL SIPH DIPL DIPH ---- ---------- ---------- ----- ----- ----- ----- ---------- ---------- ---------- ---------- TCP XLgame Custom Game 1 10 1 100 any any any any

Common Errors

The specified limit conditions are not met. For details about the limit conditions, refer to the preceding Notes.

1.4.3 Grouping Applications

Configuration Effect

- Group applications so that the flow control and application routing modules can associate policies with the application groups.

Notes

An application cannot be added to two system groups at the same time, but the application and corresponding class can be added to different system groups. For example, for Tencent QQ (a type of instant messaging software) and the class of instant messaging software, the class of instant messaging software can be added to the key application group while Tencent QQ is added to the rate-limited application group. Without manual intervention, Tencent QQ will be added to the same system group (that is, the key application group) as the class of instant messaging software by default.

Application identification protocols fall into user-defined protocols and signature database protocols. The user-defined protocols prevail over the signature database protocols. If a protocol is self-defined by users and also exists in the signature database, the system prefers the user-defined protocol.

A maximum of 100 classes of application groups can be defined.

Configuration Step

Decide a grouping mode.

Create groups.

Add applications or application classes to the groups.

Verification

Check the current application grouping mode.

Display groups and confirm that the groups are created successfully.

Display the applications or application classes in the groups.

Related Commands

Configuring Grouping Mode

Command	**identify-application clear key-inhibitive-block-other group**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Use this command to delete applications from system groups.

Creating Groups

Command	**identify-application custom-group** *group-name*
Parameter Description	group-name: Indicates a group name.
Command Mode	Global configuration mode
Usage Guide	Use this command to add user-defined groups. A maximum of 100 classes of application groups can be defined. After the command is run, enter the group-group mode.

Adding Applications to Groups

Command	**app-add** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	application group configuration mode
Usage Guide	Use this command to add applications (including applications and application classes) to the groups.

Deleting Applications from Groups

Command	**app-del** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	application group configuration mode
Usage Guide	Use this command to delete applications from the groups.

Configuring Blocked Application Group

Command	**identify-application block** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Key Application Group

Command	**identify-application key** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Rate-limited Application Group

Command	**identify-application inhibitive** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Adding a Specified Application to Other Application Group

Command	**identify-application other** *app-name*
Parameter Description	app-name: Indicates an application name.
Command	Global configuration mode

Mode

Usage Guide (1) This command is used to add a specified application to other application group.

(2) If you delete the application that is not added to another application group, the following situations will occur:

(a) If the application belongs to another application group by default, this command is successfully executed and the system does not display the message that the application is not added to another application group.

(b) If this application is a custom application (not belonging to any other application group by default), the command fails to be executed and a prompt is displayed, indicating that the application is not added to another application group.

Configuring Web_Group

Command	**identify-application web-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Online_Video_Group

Command	**identify-application online-video-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring P2p_Video_Group

Command	**identify-application p2p-video-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Download_Group

Command	**identify-application download-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring P2p_Group

Command	**identify-application p2p-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Update_Group

Command	**identify-application update-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Upload_Group

Command	**identify-application upload-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring High_Group

Command	**identify-application high-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Middle_Group

Command	**identify-application middle-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring Low_Group

Command	**identify-application low-group** *app-name*
Parameter Description	app-name: Indicates an application name.
Command	Global configuration mode

Mode	
Usage Guide	N/A

Displaying Protocol Tree

Command	**show identify-application**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Application Classes

Command	**show identify-application class [class-name]**
Parameter Description	**class-name**: Indicates a class name.
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Current Application Grouping Mode

Command	**show identify-application group-state**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Groups and Applications or Application Classes in Groups

Command	**show identify-application custom-group**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Blocked Application Group

Command	**show identify-application block**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Key Application Group

Command	**show identify-application key**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Rate-limited Application Group

Command	**show identify-application inhibitive**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Other Application Group

Command	**show identify-application other**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Web_Group

Command	**show identify-application web-group**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Online_Video_Group

Command	**show identify-application online-video-group**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying P2p_Video_Group

Command	**show identify-application p2p-video-group**
Parameter Description	N/A
Command	Privileged EXEC mode

Mode	
Usage Guide	N/A

Displaying Download_Group

Command	**show identify-application download-group**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying P2p_Group

Command	**show identify-application p2p-group**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Update_Group

Command	**show identify-application update-group**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Upload_Group

Command	**show identify-application upload-group**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Configuration Example

Creating Groups and Adding Applications to Groups

Configuration Steps	1. Create a group. 2. In application group configuration mode, add applications to the group.

	Hostname# configure terminal Hostname(config)#identify-application custom-group mygroup Hostname(config-custom-group)#app-add BQQ Hostname(config-custom-group)#app-add MSN Hostname(config-custom-group)#exit
Verification	Display the groups and applications in the groups.
	Hostname#show identify-application custom-group system-group: Key_Group system-group: Unkey_Group system-group: Block_Group application: HTTP-single thread system-group: Other_Group custom-group: mygroup application: BQQ application: MSN (group)

Configuring System Groups

Configuration Steps	Add applications or application classes to the key application group.
	Hostname# configure terminal Hostname(config)#identify-application key BQQ
Verification	Display the groups and applications in the groups.
	Hostname#show identify-application key BQQ Hostname#

Common Errors

- The specified limit conditions are not met. For details about the limit conditions, refer to the preceding Notes.

1.4.4 Configuring Application Identification

Configuration Effect

- After application identification is configured, application types of different data flows can be identified and application information can be collected.

Notes

- If application identification is disabled, all application identification functions are invalid.
- The application identification functions rely on the signature database. If the gateway does not have a signature database, application identification is invalid.
- The application identification functions are enabled by default provided that application identification is enabled.
- If application identification is enabled during application use, applications may not be accurately identified. To ensure accurate identification, enable application identification first.

Configuration Steps

In global configuration mode, run relevant commands to enable application identification and application identification functions.

Verification

- Check the module status and statuses of different application identification functions.

Related Commands

Enabling Application Identification

Command	**identify-application enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Detective Identification

Command	**identify-application proto-detect enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Predictive Identification

Command	**identify-application proto-expect enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Setting Aging Time of Protocol Information

Command	**identify-application proto-expect timeout** *time-seconds*
Parameter	time-seconds: Indicates the aging time, in seconds. The value range is from 0 to 65535.

Description	
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling DPI

Command	**identify-application dpi enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling DFI

Command	**identify-application dfi enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling QUIC Identification

Command	**identify-application quic enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	QUIC identification is enabled by default.

Enabling Length Sequence Identification

Command	**identify-application len-seq enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Enabling Application Collection

Command	**identify-application app-db enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Displaying Application Identification

Command	**show identify-application enable**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	N/A

Displaying Predictive Identification Function

Command	**show identify-application proto-expect enable**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display the prediction status and default aging time.

Displaying DFI Function

Command	**show identify-application dfi enable**
Parameter Description	N/A
Command Mode	Privileged EXEC mode
Usage Guide	Use this command to display the prediction status and default aging time.

Configuration Example

Enabling Application Identification

Configuration Steps	1. Enable application identification. 2. Disable DFI.
	Hostname# configure terminal Hostname(config)#no identify-application dfi enable
Verification	Display application identification and the DFI function.
	Hostname#show identify-application enable on Hostname#show identify-application dfi enable dfi unable!

Enabling Predictive Identification

Configuration Steps	1. Enable the predictive identification function. 2. Enable the application collection function.
	Hostname# configure terminal Hostname(config)#identify-application proto-expect enable Hostname(config)#identify-application app-db enable

Verification	Display the predictive identification function.
	Hostname#show identify-application proto-expect enable Proto-expect is enable Proto-expect app_db is enable Proto-expect timeout is not set[0s]

Common Errors

- Application identification is disabled, causing enabling failure of an application identification function.

1.4.5 Configuring the Feature of Assistance with AP Application Identification on the AC

Configuration Effect

After application identification of the AP with the assistance of the AC is configured, the AP can identify an application category based on a data flow and implement policy-based control including key application guarantee on this basis.

Notes

This feature takes effect only for APs in local forwarding mode. The application identification feature on the AC needs to be enabled simultaneously.

An application signature database must have been created on the AC. Otherwise, this feature does not take effect.

Configuration Step

In global configuration mode, use commands to enable application identification of the AP with the assistance of the AC and add or delete information about application groups that can be identified by the AP.

Verification

Run the **show identify-application ap-db** command to check whether the application identification feature is enabled and display information about application groups that can be identified.

Related Commands

Enabling Assistance with AP Application Identification on the AC

Command	**identify-application ap-enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	1. This feature is supported only for APs in local forwarding mode. 2. After enabling application identification of the AP with the assistance of the AC, use the **identify-application ap-db** command to add information about application groups that can be identified by the AP to make the feature of application identification take effect on the AC. 3. After this feature is disabled, application group information added through the **identify-application ap-db** command will not be deleted.

Configuring an Application Group That Can be Identified by the AP

Command	**identify-application ap-db** { *group-name* | **any** }
Parameter Description	*group-name*: Name of a custom application group.
Command Mode	Global configuration mode
Usage Guide	1. Use this command to configure a custom or system application group that needs to be identified. Applications in the configured application group will be identified by the AP. 2. If all applications need to be identified by the AP, run the **identify-application ap-db any** command. 3. The **no identify-application ap-db any** command is used to cancel the preceding configuration only. Information about custom or system application groups added through the **identify-application ap-db** command will not be deleted.

Configuration Example

Enabling the Feature of Assistance with AP Application Identification on the AC

Configuration Steps	1. Enable application identification of the AP with the assistance of the AC. 2. Configure information about an application group to be identified as required.

	`Hostname# configure terminal`
	`Hostname(config)# identify-application ap-enable`
	`Hostname(config)# identify-application ap-db Key_Group`

Verification	The following example displays information about application groups that can be identified by the AP.

	`Hostname# show identify-application ap-db`
	`ap-identify-application:on`
	`application list:`
	`  Key_Group`

Common Errors

After enabling this feature on the AC in centralized forwarding mode, the AP still does not support the application identification feature.

1.4.6 Configuring the L2 Application Identification Feature on the AC

Configuration Effect

The AC can identify applications for L2 packets after this feature is enabled.

Notes

This feature can be enabled after the feature of assistance with AP application identification on the AC is disabled.

Configuration Steps

Run the corresponding command in global mode to enable this feature.

Verification

Run the **show running-config** command to check whether the L2 application identification feature is enabled.

Related Commands

1. Enabling the L2 Application Identification Feature on the AC

Command	**identify-application ac-enable compatible**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	1. This feature conflicts with the feature of assistance with AP application identification on the AC, so it can only be enabled after the feature of assistance with AP application identification on the AC is disabled. 2. After this feature is enabled, the AC can identify L2 service applications. This feature is compatible with the identification features of 11.9(6)W4B1 and earlier versions. 3. The VAC scenario is not supported.

Configuration Example

1. Enabling the L2 Application Identification Feature on the AC

Configuration Steps The following example enables the L2 application identification feature on the AC.

```
Hostname#configure terminal
Hostname(config)#identify-application ac-enable compatible
```

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

```
Hostname# show running-config | inc identify-application ac-enable compatible
identify-application ac-enable compatible
```

Common Errors

Disable the feature of assistance with AP application identification on the AC before enabling the L2 application identification feature on the AC.

1.4.7 Configuring URL Identification

Configuration Effect

- Configure a custom URL object to identify HTTP or HTTPS data traffic based on URL matching information.
- Configure URL groups so that different ACLs can be applied to them.
- URL identification enables the device to identify URL information in data flows, and to apply different policies to different URLs.

Notes

- You can configure a maximum of 200 custom URL objects.

- You can add a maximum of 100 custom URL groups.
- If HTTP and HTTPS match characteristics of application identification and URL identification, and different policies are configured for application identification and URL identification, the blocking policy has the highest priority and takes effect first among all policies. For example, if rate limiting is configured in a WQoS profile and URL filtering is configured in an ACL for the same HTTP characteristics, URL filtering takes effect first and the packets are blocked, and rate limiting cannot be performed on the packets.
- Security channel has a higher priority than access control (policy control based on user role authentication). Free URL is a policy of security channel, while URL filtering based on user role is an access control policy. Therefore, if both free URL and URL filtering policies are configured, the free URL policy takes effect preferentially.
- A URL policy based on user role takes precedence over a global URL policy. If they are configured simultaneously, the URL policy based on user role takes effect preferentially.
- If a web page resource or sub-link no longer contains the URL of the parent page, it cannot be identified unless the URL of the subpage is also within the configured URL limit.
- If a browser uses the proxy function, URL identification becomes ineffective.
- In some scenarios, browsers use QUIC for data transmission, which causes URL filtering to take ineffective. The solution is to configure a QUIC application blocking policy, where UDP port 443 is used by default.
- Application identification includes the custom application identification protocol and application identification protocol of the signature database. In the system, custom protocol characteristics take precedence over protocol characteristics in the signature database. If an application protocol has both custom protocol characteristics and protocol characteristics of the signature database, the system matches custom protocol characteristics.
- IPv6 is not supported.
- Traffic identification on an AC's wired interface is not supported.

Configuration Step

Enabling URL Identification

Command	**identify-url enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the HTTP Port for URL Identification

Command	**identify-url http-port** *port-num*
Parameter Description	*port-num*: Indicates the port number. The value range is from 1 to 65535. Ports 80 and 8080 are supported by the system by default and cannot be configured or deleted.
Command Mode	Global configuration mode
Usage Guide	Run this command to add the HTTP port used by a website whose URL is not identified by default port 80 or 8080 to the port identification list so that the website URL can be identified.

Configuring the HTTPS Port for URL Identification

Command	**identify-url https-port** *port-num*
Parameter Description	*port-num*: Indicates the port number. The value range is from 1 to 65535. Ports 443 and 8080 are supported by the system by default and cannot be configured or deleted.
Command Mode	Global configuration mode
Usage Guide	If a website uses a non-default port (not port 443) as its HTTPS port to identify the website URL, you can run this command to add the HTTPS port number to the port identification list so that the interface can identify the website URL.

Creating a URL Group

Command	**identify-url url-group** *group-id* [**name** *group-name*]
Parameter Description	*group-id*: Indicates the ID of a URL group. The value range is from 1 to 511. *group-name*: Indicates the name of a URL group.
Command Mode	Global configuration mode
Usage Guide	1. This command is used to add a custom URL group or enter the URL group configuration mode if the URL group already exists. 2. A maximum of 100 custom URL groups can be added.

Creating a URL Object

Command	**identify-url url-name** *url-name* **regexp** *regexp*
Parameter Description	url-name: Indicates the name of a URL object. The value is a string of up to 63 characters. regexp: Indicates URL character matching information, which can contain a maximum of 99 characters. Only numerals, letters, and symbols are supported. The prefix http:// or https:// is not supported. Multi-level directories are not supported, that is, the directory symbol / is not supported.
Command Mode	Global configuration mode
Usage Guide	1. Fuzzy URL matching supports only domain name matching and does not support matching of lower-level directories. 2. URL character matching applies to both HTTP and HTTPS packets. 3. A maximum of 200 URL objects can be added.

Adding a URL Object to a URL Group

Command	**url** *url-name*
Parameter Description	url-name: Indicates the name of a URL object.
Command Mode	URL group configuration mode
Usage Guide	This command is used to add URL objects to a custom URL group.

Configuration Example

Configuring URL Identification

Configuration Steps

1. Enable URL identification.
2. Add HTTP port 60000 for URL identification.
3. Add HTTPS port 4430 for URL identification.
4. Create a URL object named **test** and configure the device to encapsulate the key character string baidu.com into protocol packets.
5. Create a URL group and set the group ID and group name to 5 and Web, respectively.
6. Add the created URL object **test** to the web group.

```
Hostname#config
Hostname(config)# identify-url enable
Hostname(config)# identify-url http-port 60000
Hostname(config)# identify-url https-port 4430
Hostname(config)# identify-url url-name test regexp *baidu.com*
Hostname(config)# identify-url url-group 5 name Web
Hostname(config-url-group)# url test
```

Verification

1. Run the **show identify-url enable** command to check whether URL identification is enabled.
2. Run the **show identify-url http-port** command to display HTTP ports for URL identification.
3. Run the **show identify-url https-port** command to display HTTPS ports for URL identification.
4. Run the **show identify-url url-name** command to display URL objects and packet matching information configured for each URL object.
5. Run the **show identify-url url-group** command to display URL groups and URL objects in each group.

Common Errors

More than 200 customized URL objects are added.

More than 100 custom URL groups are added.

1.4.8 Configuring the Language in Which Application Identification Information Is Displayed

Configuration Effect

The device displays identified application information based on the configured language.

Notes

Running this command triggers the signature database to be reloaded.

After the language is switched, the **identify-application custom name** and **identify-application custom-group** commands will be cleared. You need to reconfigure them.

After the language is switched, the **identify-application key** and **identify-application block** commands will be cleared. You need to reconfigure them.

Configuration Step

Run a command in global configuration mode to configure the language in which application identification information is displayed.

Verification

Run the **show running-config** command to display the configuration status of application language switching.

Run the **show identify-application class** command to display the language in which application identification information is displayed.

Related Commands

Configuring the Language in Which Application Identification Information Is Displayed

Command	**identify-application signature language** { **zh** | **en** }
Parameter Description	**zh**: Indicates that the application name and category are displayed in Chinese. **en**: Indicates that the application name and category are displayed in English.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Configuring Application Identification Information Displayed in English

Configuration Steps Configure application identification information displayed in English.

```
Hostname# configure terminal
Hostname(config)# identify-application signature language en
```

Verification Display the language in which application identification information is displayed.

```
Hostname#show identify-application class
HTTP 1-0-0-0
VOIP 2-0-0-0
```

Common Errors

N/A

1.5 Monitoring

Clearing

Command	Description
clear identify-url statistics	Clears URL identification packet statistics.

Displaying

Command	Description
show identify-application	Displays the application protocol tree information.
show identify-application block	Displays the applications or application classes that are added to the blocked application group.

show identify-application class	Displays the application class information.
show identify-application custom-group	Displays the application group information.
show identify-application custom- rule	Displays the user-defined application rules.
show identify-application download-group	Displays the applications or application classes that are added to Download_Group.
show identify-application enable	Displays application identification.
show identify-application group-state	Displays the grouping mode.
show identify-application high-group	Displays the applications or application classes that are added to High_Group.
show identify-application inhibitive	Displays the applications or application classes that are added to the rate-limited application group.
show identify-application key	Displays the applications or application classes that are added to the key application group.
show identify-application low-group	Displays the applications or application classes that are added to Low_Group.
show identify-application middle-group	Displays the applications or application classes that are added to Middle_Group.
show identify-application other	Displays the applications or application classes that are added to the Other application group.
show identify-application proto-expect enable	Displays the predictive protocol information.
show identify-application proto-detect enable	Displays the detective protocol information.
show identify-application version	Displays the version number of the signature database.
show identify-application ap-db	Displays information about application groups that can be identified by the AP and whether a feature is enabled or disabled.
show identify-url enable	Displays the application identification status.
show identify-url http-port	Displays the HTTP port information available for URL identification.
show identify-url https-port	Displays the HTTPS port information used for URL identification.
show identify-url statistics	Displays URL statistics.
show identify-url url-group [*group-id*]	Displays URL group information.
show identify-url url-name [*url-name*]	Displays custom URL information.

1 Configuring AEM

1.1 Overview

Application Experience Measurement (AEM) is used to measure the network performance between wireless users and application service nodes. Administrators can create an application group, add applications of interest to be measured to this group, and then configure this group as an application group of interest. AEM collects metrics between clients and servers that provide services for applications to measure the network performance of the applications of interest.

AEM can measure the following 32 metrics between wireless users and service nodes of applications in an application group of interest.

No.	Metric
1	Uplink traffic increment (byte)
2	Downlink traffic increment (byte)
3	Uplink packet number increment
4	Downlink packet number increment
5	Average server latency in TCP handshake (ms)
6	Average client latency in TCP handshake (ms)
7	Average air interface latency in TCP handshake (ms)
8	Client response latency (ms)
9	Server response latency or application latency (ms)
10	Number increment of TCP uplink retransmitted packets
11	Number increment of TCP downlink retransmitted packets
12	Number increment of TCP uplink out-of-order packets
13	Number increment of TCP downlink out-of-order packets
14	Average downlink air interface latency of application packets (ms)
15	Number increment of downlink application packets retransmitted over the air interface
16	Number increment of downlink application packets lost on the air interface
17	Number of active TCP flows of applications
18	Number of active UDP flows of applications
19	Number of new packet flows
20	Downlink packet sending times of the air interface
21	Average uplink TCP jitter (ms)
22	Average downlink TCP jitter (ms)
23	Average downlink jitter on the air interface (ms)
24	Number of TCP handshake failures
25	Number increment of uplink RTP packets
26	Number increment of downlink RTP packets
27	Number increment of lost uplink RTP packets

No.	Metric
28	Number increment of lost downlink RTP packets
29	Number increment of uplink RTP out-of-order packets
30	Number increment of downlink RTP out-of-order packets
31	Average uplink RTP jitter (ms)
32	Average downlink RTP jitter (ms)

The following sections describe the AEM function only.

Protocols and Standards

N/A

1.2 Applications

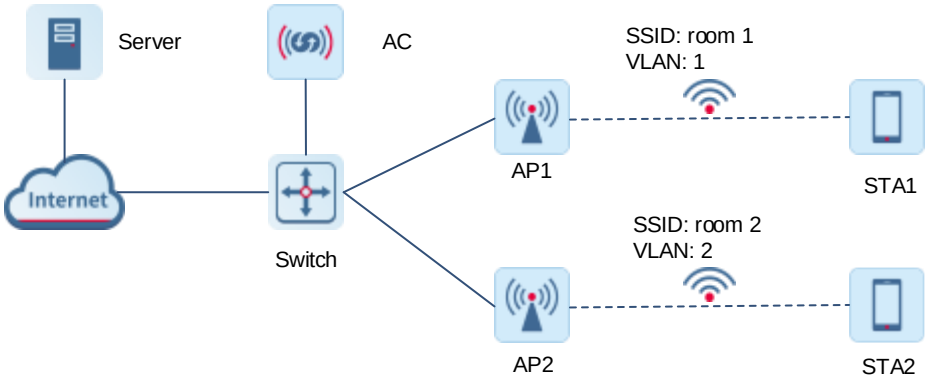
Application	Description
Measuring Application Experience of STAs in Fit AP Networking	Measures the network performance between STAs and the servers of the applications in an application group of interest in a fit AP scenario.

1.2.1 Measuring Application Experience of STAs in Fit AP Networking

Scenario

In a fit AP scenario, configure an application group of interest on the AC and deliver the application group of interest to APs. Then, measurement on applications of interest is automatically enabled on the APs. The APs collect metrics between STAs and the application server, including the packet transmission latency and the packet loss rate, and periodically report the information to the AC, as shown in the following figure.

Figure 1-1 AEM for STAs in Fit AP Networking



Remarks	Server: third-party application server on the remote end Switch: switch device AC: wireless access controller AP1 and AP2: wireless access points STA1 and STA2: client devices

Deployment

1. Enable application identification of the AC.
2. On the AC, enable application identification for APs.
3. Create an application group of interest.

1.3 Features

Basic Concepts

Application

An application (app) refers to the software program installed and run on a STA. Applications can be installed on smartphones, tablets, smart watches, or other devices to provide users with various network services, such as browsing web pages, sending emails, playing games, and holding video conferences.

Application of Interest

In various service scenarios, users have different requirements for applications. Therefore, network administrators need to have a comprehensive understanding of the user experience of specified applications. This helps them configure proper network management policies, thereby improving the user experience. Applications that administrators pay special attention to are known as applications of interest.

Application Group of Interest

To measure and manage the network experience of different applications, administrators can add the applications of interest to an application group and manage the application group to achieve unified management of the applications. Such an application group is called an application group of interest. The applications in an application group of interest are applications of interest.

RTP

Real-Time Transport Protocol (RTP) typically uses User Datagram Protocol (UDP) as the transport layer protocol. RTP is typically used to transmit real-time audio and video data over the Internet.

Overview

Features	Description
Measurement on Applications of Interest	Measures the packets of the applications in an application group of interest on STAs.

Features	Description
Collection Scale Limit	Adjusts the scale of measurement data collection on APs.

1.3.1 Measurement on Applications of Interest

On an AP, if an application identified by the application identification function belongs to an application group of interest, the AP collects statistics on packet flows of the application, and proactively reports them to the AC. Then, the AC measures the network performance of the application.

Working Principle

Measurement on applications of interest depends on application identification results. Upon receiving a packet, an AP performs application identification on the packet. If the application type is identified, the AP determines whether the application is a specified application of interest based on the application index. For applications of interest, the AP collects specific parameter information in packet flows based on the protocol characteristics of packets. The AP collects and summarizes information about applications of interest, and then proactively uploads the information to the AC.

1.3.2 Collection Scale Limit

Reporting information about applications of interest to the AC consumes a portion of network performance resources. Therefore, configure a proper policy for collecting information on applications of interest on the AC based on actual services. After the AC delivers the policy to APs, the APs report information about specified applications to the AC based on the policy.

Working Principle

When an AP summarizes the collected information about applications of interest, it limits the data specifications uploaded to the AC in three dimensions:

- Number of STAs for which application information is collected by each AP
- Number of applications of interest on each STA
- Number of data flows of each application of interest

1.4 Configuration

Configuration	Description and Command	
Configuring Measurement on Applications of Interest	⚠ (Mandatory)	
	app-experience app-group	Adds an application group of interest.
	⚠ (Optional) It is used to adjust the collection interval.	
	app-experience app-interval	Configures a collection interval for applications of interest.

Configuration	Description and Command	
Configuring an Application Information Collection Scale	(Optional) It is used to limit the number of STAs for which application information is collected by each AP to limit the data collection scale.	
	app-experience maximum-sta	Configures the maximum number of STAs for which application information is collected by each AP.
	(Optional) It is used to limit the number of applications of interest to be collected on each STA.	
	app-experience maximum-app	Configures the maximum number of applications of interest to be collected on each STA.
	(Optional) It is used to limit the number of packet flows to be collected for each application of interest.	
	app-experience maximum-flow	Configures the maximum number of packet flows to be collected for each application of interest.

1.4.1 Configuring Measurement on Applications of Interest

Configuration Effect

After an application group is configured as an application group of interest on the AC and is delivered to APs, measurement on applications of interest is automatically enabled on the APs. The APs periodically collect information on applications of interest and report the information to the AC.

Notes

- Before applying measurement on applications of interest, enable application identification of the AC and application identification for APs.
- Before applying measurement on applications of interest, ensure that application identification has been enabled for the system application group **any** on the APs.

Configuration Steps

Adding Application Group of Interest

- Mandatory.
- When an application group of interest is added, measurement on applications of interest is automatically enabled.

Command	**app-experience app-group** *custom-group-name*
Parameter Description	*custom-group-name*: Indicates the name of the application group. The value range is from 1 to 63 characters.

Defaults	No application group of interest is configured.
Command Mode	Global configuration mode
Usage Guide	1. Measurement on applications of interest depends on application identification results. Therefore, before applying measurement on applications of interest, enable application identification of the AC and application identification for APs. If application identification of the AC or application identification for APs is disabled, information on applications in the application group of interest cannot be collected. 2. Run the custom application group creation command of the application identification function to create an application group. Then, run this command to configure the created application group as an application group of interest. If an application group does not exist, the configuration fails. 3. Before applying measurement on applications of interest, ensure that application identification has been enabled for the system application group **any** on the APs. That is, verify that the **identify-application ap-db any** command has been executed. Application identification is enabled for the system application group **any** by default. If it is disabled, you need to manually enable it before applying measurement on applications of interest. After an application group is configured as an application group of interest, the applications in this application group become applications of interest.

Configuring an Application Information Reporting Interval for an Application Group of Interest

- Optional.

Command	**app-experience app-interval** *interval-time*
Parameter Description	*interval-time*: Indicates the interval for reporting collected information to the AC, in seconds. The value range is from 30 to 300.
Defaults	60s
Command Mode	Global configuration mode
Usage Guide	-

Verification

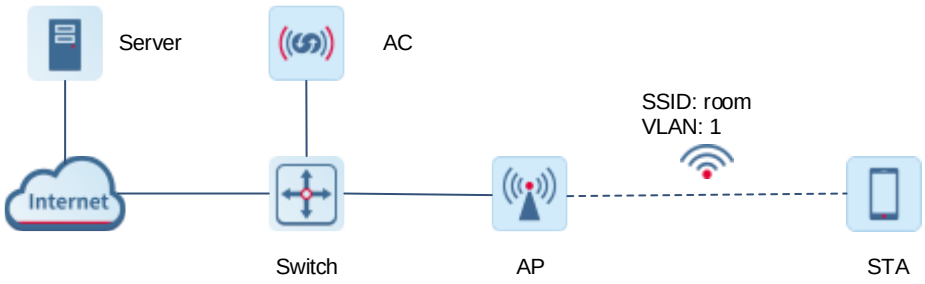
You are advised to perform the following two steps to verify the configuration and check whether the function takes effect.

- Run the **show running-config** command to display configuration.
- After a user uses an application of interest (such as opening the homepage of the application), run the **show app-experience table** command on the AC to display the collected application data.

For details about the **show** command output, see the command reference of the corresponding function.

Configuration Example

Adding Application Group of Interest

Scenario **Figure 1-2**	
Configuration Steps	1. Enable application identification of the AC. 2. Enable application identification for APs. 3. Create custom application group Download-Group and add application HTTP-DOWNLOAD to this application group. 4. Configure Download-Group as an application group of interest.

AC	`Hostname# configure terminal`
	`Hostname(config)# identify-application enable`
	`Hostname(config)# identify-application ap-enable`
	`Hostname(config)# identify-application custom-group Download-Group`
	`Hostname(config-custom-group)# app-add HTTP-DOWNLOAD`
	`Hostname(config-custom-group)# exit`
	`Hostname(config)# app-experience app-group Download-Group`

Verification	After STAs access applications in the application group of interest, run the **show app-experience table** command to display the collected data about the applications of interest.

AC	`Hostname# show app-experience table`
	`sta ip time appidx upbytes dnbytes uppkts dnpkts tssd tscd tsad tur tdr tudp tddp tump tdmp dad dadp dalp tfc ufc tsfc dap turj tdrj dadj tsft`
	
	`rtp_uppkts rtp_dnpkts rtp_uplost rtp_dnlost rtp_upser rtp_dnser rtp_upjt rtp_dnjt`
	`92B2.5FE5.51A8 192.168.30.61 2024-08-06 10:08:01 1-26-2-0 8802 326586 163 220 0 0 0 0 3 0 0 0 0 0 0 0 2 0 2 0 0 269 0 0`
	`92B2.5FE5.51A8 192.168.30.61 2024-08-06 10:07:56 1-26-2-0 9504 1122395 176 751 0 0 0 0 15 0 0 0 0 0 0 0 4 0 4 0 0 12 0 0`

Common Errors

- Application identification of the AC or application identification for APs is disabled.
- A non-existing application group is configured as an application group of interest.
- Application identification is disabled for the system application group **any** on the APs. That is, the **no identify-application ap-db any** command has been executed.

1.4.2 Configuring an Application Information Collection Scale

Configuration Effect

An AP reports the collected information to the AC based on the configured collection limit, including the collection range and number.

Notes

N/A

Configuration Steps

Configuring the Maximum Number of STAs for Application Information Collection per AP

- Optional.

Command	**app-experience maximum-sta** *max-number*
Parameter Description	*max-number*: Indicates the maximum number of STAs for which application information is collected by each AP. The value range is from 1 to 100.
Defaults	The number of STAs for which application information is collected by each AP is not limited.
Command Mode	Global configuration mode
Usage Guide	Run this command to limit the number of STAs for which application information is collected by each AP, thereby limiting the collection scale.

Configuring the Maximum Number of Applications to Be Collected on Each STA

- Optional.

Command	**app-experience maximum-app** *max-number*
Parameter Description	*max-number*: Indicates the maximum number of applications to be collected on each STA. The value range is from 1 to 10.
Defaults	5
Command Mode	Global configuration mode
Usage Guide	-

Configuring the Maximum Number of Packet Flows to Be Collected for Each Application

- Optional.

Command	**app-experience maximum-flow** *max-number*
Parameter Description	*max-number*: Indicates the maximum number of packet flows to be collected for each application. The value range is from 1 to 5.
Defaults	Packet flow statistics are not collected based on applications.
Command Mode	Global configuration mode
Usage Guide	-

Verification

Run the **show running-config** command to display the application information collection limit.

Configuration Example

N/A

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show app-experience table [**sta** *sta-mac*] [**app-index** *app-index* | **app-name** *app-name*] [**limit** *limit*]	Displays the collected information on applications of interest.

Debugging

N/A

1 QoS-based Key Service Assurance

1.1 Overview

QoS-based key service assurance refers to policy services provided by Quality of Service (QoS) to guarantee the experience of key services. The policy services provided by QoS include modifying the Differentiated Services Code Point (DSCP) values of packets and configuring execution policies (such as rate limiting and blocking). QoS-based key service assurance includes key application assurance and key area assurance.

1.1.1 Key Application Assurance

For key application assurance, QoS policies are configured for applications based on application identification results. Application identification indicates that the access controller (AC) identifies the application (such as WeChat, QQ, Youku, and Fantasy Westward Journey) to which a packet belongs based on the packet features. On the AC, you can configure an application policy profile and define rules (such as configuring the DSCP value, packet discarding, and rate limiting for an application group) in the profile. An access point (AP) converts the DSCP value into an 802.11e priority and schedules and forwards packets based on the 802.11e priority, ensuring application-based QoS. Currently, a DSCP value can be configured only for downlink traffic.

If the priority configured for downlink traffic is higher than that of uplink traffic, the uplink traffic will be suppressed because the total channel bandwidth is fixed. If different priorities are set for traffic from different STAs, traffic with a higher priority can be accelerated theoretically. However, its bandwidth may not be improved because the air interface competition capabilities of STAs are determined by their drive and hardware.

This document only provides guidance on configuring key application assurance. For details about the guidance for application identification, see documents related to application identification.

1.1.2 Key Area Assurance

In finance and enterprise campus network scenarios, when an important activity is held in a conference room or an area, network experience in the area needs to be preferentially guaranteed. For example, preferentially guarantee network services at the conference site during an annual meeting. Essentially, key area assurance preferentially guarantees the traffic of VIP users or key applications within a small scope to ensure preferred forwarding of key traffic.

Protocols and Standards

- IEEE 802.11e-2005: Amendment 8: Medium Access Control (MAC) QualityofServiceEnhancements, IEEE Computer Society
- Wi-Fi: WMM Specification version 1.1

1.2 Applications

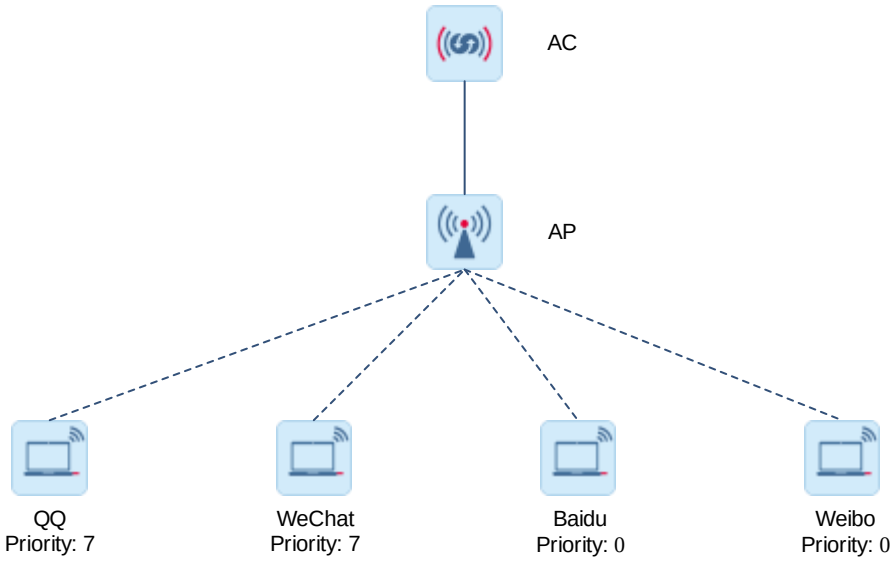
Application	Description
Configuring QoS Policies for Key Application Assurance in Fit AP Networking	Fit AP networking is adopted, including at least one AC and one AP.

1.2.1 Configuring QoS Policies for Key Application Assurance in Fit AP Networking

Scenario

On a wireless local area network (WLAN), an AC is deployed and application-based priority control is configured for the WLAN on the AC to guarantee traffic for key applications such as Tencent-related applications.

Figure 1-1



Remarks	AC: wireless access controller AP: wireless access point

Deployment

- Configure an application profile on the AC.
- Associate the WLAN with the application profile.

1.3 Features

Basic Concepts

DSCP

DSCP is a QoS classification standard of Differentiated service (Diff-Serv) released by IETF in December 1998. In the type of service (ToS) field in the IP header of each packet, the used 6 bits and unused 2 bits are used to distinguish the priority. DSCP uses 6 bits, and the DSCP value ranges from 0 to 63.

802.11e priority indicates the priority of wireless packets, which is divided into eight levels (0–7).

The following table describes the default mapping between DSCP values and 802.11e priorities.

802.11e Priority	DSCP Value: Binary (Decimal)
0	BE:000000(0)
1	CS2:010000(16), AF21:010010(18), AF22:010100(20), AF23:010110(22)
2	CS3:011000(24), AF31:011010(26), AF32:011100(28), AF33:011110(30
3	CS1:001000(08), AF11:001010(10), AF12:001100(12), AF13:001110(14)
4	CS4:100000(32), AF41:100010(34), AF42:100100(36), AF43:100110(38)
5	CS5:101000(40), EF:101110(46)
6	CS6:110000(48)
7	CS7:111000(56)

Overview

Feature	Description
QoS Policies for Key Application Assurance	Configures DSCP priorities, packet discarding, and rate limiting based on applications.
QoS Policies for Key Area Assurance	Configures DSCP priorities based on key areas.
Configuring Application Traffic Statistics Collection	Collects traffic statistics of different applications and uploads the statistics to the cloud.

1.3.1 QoS Policies for Key Application Assurance

Working Principle

Based on traffic characteristics, the application identification component on the AC can identify applications and control the uplink and downlink DSCP priorities of different applications in the following ways:

Different DSCP values can be set for different applications in the downlink direction. When a packet is sent to an AP, the Wi-Fi Multimedia (WMM) function on the AP converts the DSCP value of the packet to an 802.11e priority. Then, the AP schedules the packet based on the priority, ensuring priority control of different applications.

Different DSCP values can be set for different applications in the uplink direction. When an uplink application packet is sent to an AP through the air interface, the packet is marked with the corresponding DSCP value. The upstream wired network device converts the DSCP value of the packet into the corresponding priority for scheduling.

The DSCP priorities of uplink and downlink packets can be flexibly controlled in different application scenarios, improving network performance and QoS. In addition, Packet discarding can be configured for specified applications to block unauthorized application traffic. Different rate limits can be configured for different applications, such as configuring a traffic rate limit for download applications to avoid excessive bandwidth consumption.

1.3.2 QoS Policies for Key Area Assurance

Working Principle

For key area assurance, specific APs are added to key areas. Clients that access in the key areas are considered as key clients. When common clients access key applications, the DSCP priorities of packets are re-marked by QoS to ensure preferred traffic forwarding.

The APs in key areas re-mark the key traffic with higher DSCP priorities so that the key traffic in the key area is preferentially processed. Key traffic includes traffic of VIP users, traffic of key applications, and traffic of VIP users and key applications. For example, when common users access common applications in key areas, packets are not preferentially forwarded. When common users access key applications in key areas, packets are preferentially forwarded based on configured DSCP values.

1.3.3 Configuring Application Traffic Statistics Collection

Working Principle

The application identification module on the AC can identify an application based on the packet flow feature of the application. The AP stores packet size information based on flow space and sends the information to the AC. Run different commands to check statistics from different dimensions.

1.4 Configuration

Configuration	Description and Command	
Configuring QoS Policies for Key Application Assurance	⚠ (Mandatory) It is used to configure an application profile.	
	app-profile	Adds or modifies an application profile.
	app-rule	Configures a QoS policy for an application group.
	⚠ (Mandatory) It is used to configure an application profile for a WLAN.	
	app-profile	Associates a WLAN with the specified application profile.
Configuring QoS Policies for Key Area Assurance	⚠ (Mandatory) It is used to configure a key area profile.	
	dscp { **up-streams** | **down-streams** }	Configures the DSCP priorities of uplink or downlink traffic for a key area group.
	⚠ (Mandatory) It is used to associate an AP with a specified key area group profile.	
	area-group	Associates an AP with a specified key area group profile.
Configuring Application Traffic Statistics Collection	**app-traffic**	Configures application traffic statistics collection.
	app-traffic report enable	Configures the feature of reporting application traffic statistics to the cloud.

Configuration	Description and Command	
	app-traffic report interval	Configures the interval for reporting application traffic statistics to the cloud.

1.4.1 Configuring QoS Policies for Key Application Assurance

Configuration Effect

- Preferentially guarantee traffic of specific applications such as Tencent-related applications, including WeChat and QQ on WLAN 1. According to captured wireless packets, it is found that the 802.11e priority of WeChat, QQ, and Qzone is 7 and the 802.11e priority of other applications is 0.
- Preferentially guarantee wireless services of specific applications. In this case, the packets of the specified applications are forwarded preferentially. For example, if the DSCP value of uplink packets of Tencent-related applications is set to 56, when the uplink packets are sent to the AP through the air interface, the upstream wired network device captures the packets and finds that the packets are marked with DSCP 56, indicating that the forwarding priority of the packets is 56.
- Configure network access rules for different time ranges on the network. For example, block the access to stock software from 9:00 to 18:00 on Monday to Friday.
- Configure rate limiting for specific applications. For example, set the downlink rate limit to 10 Mbps for HTTP download applications.

Notes

- Application identification is implemented on the AC.
- Application identification QoS only supports the centralized forwarding mode. Before associating a WLAN with a profile, check the forwarding mode. If the forwarding mode is not centralized forwarding, set it to centralized forwarding.
- Before configuring key application assurance, enable application identification.

Configuration Steps

↘ Configuring an Application Profile

- Mandatory.
- Run the **app-profile** command in global configuration mode on the AC.

Command	**app-profile** *profile-name*
Parameter Description	*profile-name*: Name of an application profile.
Defaults	No application profile is configured by default.
Command Mode	Global configuration mode
Usage Guide	N/A

↘ Configuring Uplink and Downlink DSCP Policies for an Application Group

Command	**app-rule** *group-name* **dscp** [**up-streams** | **down-streams**] *value* [**time-range** *time-rang-name*]

Parameter Description	*group-name*: Name of an application group. **up-streams**: DSCP value of uplink packets of a specific application group. **down-streams**: DSCP value of uplink packets of a specific application group. *value*: DSCP value, ranging from 0 to 63. *time-rang-name*: Effective time of the DSCP policy. You can associate the DSCP policy with a configured time policy name. For details about the time policy, see *Configuring Time Range*.
Defaults	No application profile is configured by default.
Command Mode	app-profile mode
Usage Guide	N/A

Configuring a Block Policy for an Application Group

Command	**app-rule** *group-name* **deny** [**time-range** *time-rang-name*]
Parameter Description	*group-name*: Name of an application group. *time-rang-name*: Effective time of the block policy. You can associate the block policy with a configured time policy name. For details about the time policy, see *Configuring Time Range*.
Defaults	No block policy is configured.
Command Mode	app-profile mode
Usage Guide	N/A

Configuring a Rate Limit Policy for an Application Group

Command	**app-rule** *group-name* **per-user-limit** { **down-streams** | **up-streams** } **average-data-rate** *average-data-rate* **burst-data-rate** *burst-data-rate* [**time-range** *time-rang-name*]
Parameter Description	*group-name*: Name of an application group. **down-streams**: Downlink traffic rate limit for an application group. **up-streams**: Uplink traffic rate limit for an application group. *average-data-rate*: Average rate limit, in 8 kbps. The value ranges from 8 to 261,120. *burst-data-rate*: Burst limit, in 8 kbps. The value ranges from 8 to 261,120. *time-rang-name*: Effective time of the block policy. You can associate the block policy with a configured time policy name. For details about the time policy, see *Configuring Time Range*.
Defaults	No rate limit policy is configured.
Command Mode	app-profile mode
Usage Guide	The rate limit policy for an application group takes effect for the application group of each user on a WLAN.

Associating a WLAN with an Application Profile

- Mandatory.
- Run the **app-profile** command in WLAN configuration mode on the AC.

Command	**app-profile** *profile-name*
Parameter Description	*name*: Name of an application profile.

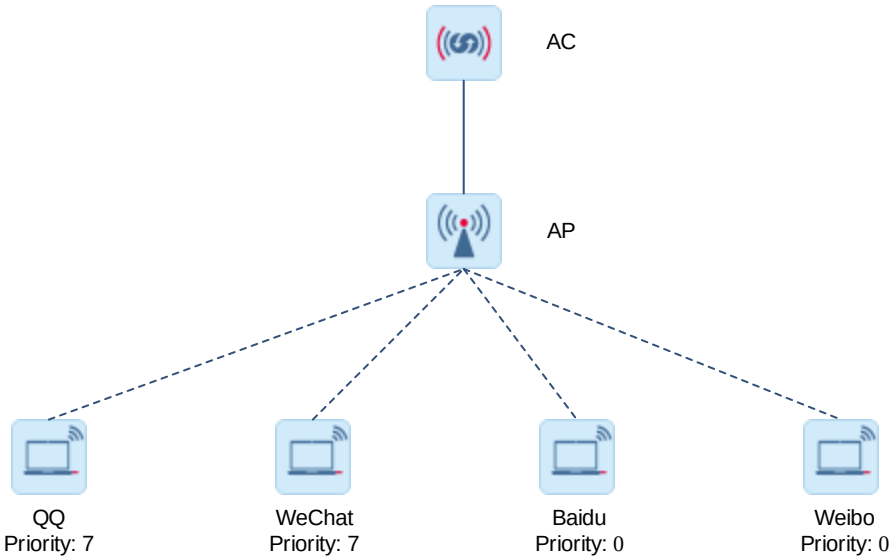
Defaults	A WLAN is not associated with an application profile by default.
Command Mode	WLAN configuration mode
Usage Guide	N/A

Verification

Run the **show running-config** command to display the profile information and WLAN association information.

Configuration Example

Configuring Application-based Traffic Priority Control

Scenario **Figure 1-2**	
Configuration Steps	Create a custom application group Tencent and add WeChat, QQ, and QZone to this group.

AC	`Hostname(config)# identify-application custom-group Tencent`
	`Hostname(config-custom-group)# app-add QZone`
	`Hostname(config-custom-group)# app-add WeChat`
	`Hostname(config-custom-group)# app-add QQ`

	Add an application profile.
	`Hostname(config)# app-profile P-Tencent` `Hostname(config-app-profile)#`
	According to the DSCP table in the Basic Concepts section, DSCP 56 maps wireless priority 7. Therefore, set the DSCP value of application group Tencent to 56.
	`Hostname(config-app-profile)# app-rule Tencent dscp down-streams 56`
	Set the uplink DSCP value of app group tencent to 56.
	`Hostname(config-app-profile)#app-rule Tencent dscp up-streams 56`
	Block access to stock software for a network.
	`Hostname(config-app-profile)# app-rule Stock-Group deny`
	Block access to stock software from 9:00 to 18:00 on Monday to Friday.
	`Hostname(config)#time-range app_rule_tl` `Hostname(config-time-range)# periodic Weekdays 9:00 to 18:00`

	Hostname(config)#app-profile P-Office Hostname(config-app-profile)#app-rule Stock-Group deny time-range app_rule_tl
	Set the downlink traffic rate limit for applications used for HTTP download to 10 Mbps.
	Hostname(config-app-profile)# app-rule Download-Group down-streams average-data-rate 10000 burst-data-rate 12000
	Associate the WLAN with the application profile.
	Hostname(config)# wlan-config 1 Hostname(config-wlan)# app-profile P-Tencent
Verification	Run the **show running-config** command to display the configurations.
AC	Hostname# show running-config | begin app-profile app-profile P-Tencent app-rule Tencent dscp 56

Common Errors

- N/A

1.4.2 Configuring QoS Policies for Key Area Assurance

Configuration Effect

Uplink and downlink packets of VIP users and key applications in key areas are preferentially forwarded.

Notes

You can specify the DSCP priorities for uplink and downlink packets based on VIP users, key applications, and key area groups separately. The combination rules are as follows:

- VIP user: If a wireless application profile is associated in user role configuration mode, client users of this role that access the applications in the profile are subject to the policy of the application group (for example, modifying the DSCP value of uplink packets to 46).
- Key application: If a wireless application profile is associated in WLAN configuration mode, client users on the WLAN that access the applications in the profile are subject to the policy of the application group (for example, modifying the DSCP value of uplink packets to 48).

  If two wireless application profiles are separately associated in user role configuration mode and WLAN configuration mode and both the role and WLAN attributes of a client user match the two profiles, the profile associated in user role configuration mode prevails. (In this example, the policy rule of modifying the DSCP value of uplink packets to 46 prevails.)
- Key area: In AP configuration mode, specify the DSCP priority of uplink or downlink packets (for example, modifying the DSCP value of uplink packets to 56). If policy rules are also configured for VIP users and key applications, the policy rule with the largest DSCP value prevails. (That is, if a VIP user connects to the AP in a key area and accesses the applications in the application profile, the DSCP value of the uplink packets of the user is modified to 56.)

Configuration Steps

Configuring a Key Area Group

- Mandatory.

- Run the **area-group** command in global configuration mode on the AC. If no key area group exists, run this command to create a group and enter the area group configuration mode. If a key area group exists, run this command to enter the area group configuration mode.

Command	**area-group** *group-name*
Parameter Description	*group-name*: Indicates the name of a key area group. The value is a string of 1 to 63 characters.
Defaults	No key area group is configured.
Command Mode	Global configuration mode
Usage Guide	A maximum of 128 key area groups can be added. You can run the **no area-group** *group-name* command to delete an existing area group.

Configuring Policy Rules for the DSCP Value of Uplink or Downlink Traffic in a Key Area Group

Command	**dscp** { **up-streams** | **down-streams** } *dscp-value*
Parameter Description	**up-streams**: Configures the DSCP value for a key area group in the uplink direction. **down-streams**: Configures the DSCP value for a key area group in the downlink direction. *dscp-value*: Indicates the DSCP value. The value range is from 0 to 63. A larger value indicates a higher priority.
Defaults	No policy rule is configured.
Command Mode	Area group configuration mode
Usage Guide	If DSCP value policies are configured for a key area group and a VIP user or key application simultaneously, the configuration with the largest DSCP value prevails.

Associating an AP with a Key Area Group

- Mandatory.
- Run the **area-group** command in AP configuration mode on the AC.

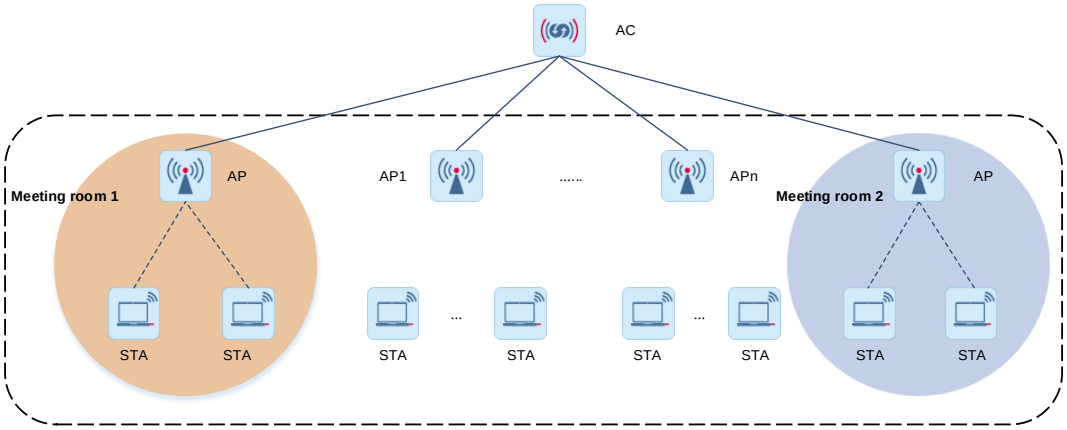
Command	**area-group** *group-name*
Parameter Description	*group-name*: Indicates the name of a key area group. The value is a string of 1 to 63 characters.
Defaults	An AP is not associated with a key area group.
Command Mode	AP configuration mode
Usage Guide	1. An AP can be associated with only one key area group and a key area group can be associated with up to 50 APs. 2. A key area group cannot be associated in all-AP configuration mode.

Verification

- Run the **show running-config** command to display key area and AP association information.

Configuration Example

QoS Policies based on the Key Area Group

Scenario **Figure 1-3**	
Configuration Steps	Add key area group **Meeting room 1**, set the DSCP values of both uplink and downlink traffic to 56, and associate the area group with AP1.
AC	Hostname(config)# area-group Meeting room 1 Hostname(config-area-group)# dscp up-streams 56 Hostname(config-area-group)# dscp down-streams 56 Hostname(config-area-group)# exit Hostname(config)# ap-config AP1 Hostname(config-ap)# area-group Meeting room 1
	Add key area group **Meeting room 2**, set the DSCP values of both uplink and downlink traffic to 46, and associate the area group with AP2.
	Hostname(config)# area-group Meeting room 2 Hostname(config-area-group)# dscp up-streams 46 Hostname(config-area-group)# dscp down-streams 46 Hostname(config-area-group)# exit Hostname(config)# ap-config AP2 Hostname(config-ap)# area-group Meeting room 2
Verification	Run the **show running-config** command to display the configuration.

Common Errors

N/A

1.4.3 Configuring Application Traffic Statistics Collection

Configuration Effect

- Enable or disable application traffic statistics collection to control whether the AC periodically collects application traffic statistics.
- Enable or disable the feature of reporting statistics to the cloud to control whether application traffic statistics are uploaded to the cloud.
- Configure the interval for reporting statistics to the cloud to control the frequency of synchronizing application traffic statistics from a device to the cloud.

Notes

Before configuring application traffic statistics collection, enable the application identification feature first.

Configuration Steps

Configuring Application Traffic Statistics Collection

- Mandatory.
- Use the **app-traffic enable-statistics** command to configure this feature in global configuration mode on the AC.

Command	**app-traffic** { **enable-statistics** | **disable-statistics** | **reset-statistics** }
Parameter Description	**enable-statistics**: Enables application traffic statistics collection. **disable-statistics**: Disables application traffic statistics collection. **reset-statistics**: Clear application traffic statistics.
Defaults	The feature is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Feature of Reporting Application Traffic Statistics to the Cloud

- (Optional) This feature is used to decide whether application traffic statistics are uploaded to and displayed on the cloud
- Use the **app-traffic report enable** command to configure this feature in global configuration mode on the AC.

Command	**app-traffic report enable**
Parameter Description	N/A
Defaults	The feature is disabled.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring the Interval for Reporting Application Traffic Statistics to the Cloud

Use the **app-traffic report interval** *value* command to configure this feature in global configuration mode on the AC.

Command	**app-traffic report interval** *value*
Parameter Description	*value*: Interval for reporting application traffic statistics to the cloud, in seconds. The value ranges from 30 to 3,600.
Defaults	300s
Command Mode	Global configuration mode
Usage Guide	N/A

Verification

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

Configuration Example

Configuring the Feature of Collecting Application Traffic Statistics and Reporting the Statistics to the Cloud

Configuration Steps	1. Enable the feature of collecting application traffic statistics. 2. Enable the feature of reporting application traffic statistics to the cloud. 3. Set the interval for reporting statistics to 60 seconds.

AC	`Hostname# config`
	`Hostname(config)# app-traffic enable-statistics`
	`Hostname(config)# app-traffic report enable`
	`Hostname(config)# app-traffic report interval 60`

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

AC	`Hostname# show running | include app-traffic`
	`app-traffic enable-statistics`
	`app-traffic report enable`
	`app-traffic report interval 60`

Common Errors

N/A

1.5 Monitoring

Clearing

N/A

Displaying

Command	Description
show app-profile	Displays details of an application profile.
show area-group [*group-name*]	Displays details about a key area group.
show app-traffic top-apps *N* **scope** { **app** | **group** }	Displays the traffic of the top *N* apps/application groups on the AC.
show app-traffic per-station *mac-address* **top** *N* **scope** { **app | group** }	Displays the traffic of the top *N* applications/application groups of a MAC address on the AC.
show app-traffic per-app *app-name* **top** *N* **scope** { **app** | **group** }	Displays the top *N* STAs of an application/application group on the AC.

Debugging

N/A

1 Configuring DNS-CACHE

1.1 Overview

DNS-CACHE can cache the results of domain name resolutions. When a client requests for access to a domain name for the first time, the domain name is resolved and the resolution result is cached. When the client requests to access the same domain name next time, the device directly returns the cached result, instead of obtaining the IP address from an external domain name server (DNS).

Protocols and Standards

RFC1034: Domain Names - Concepts and Facilities

1.2 Applications

Application	Description
Deploying Egress Gateway of Cybercafé	Deploys DNS-CACHE in the egress gateway of a cybercafé.

1.2.1 Deploying Egress Gateway of Cybercafé

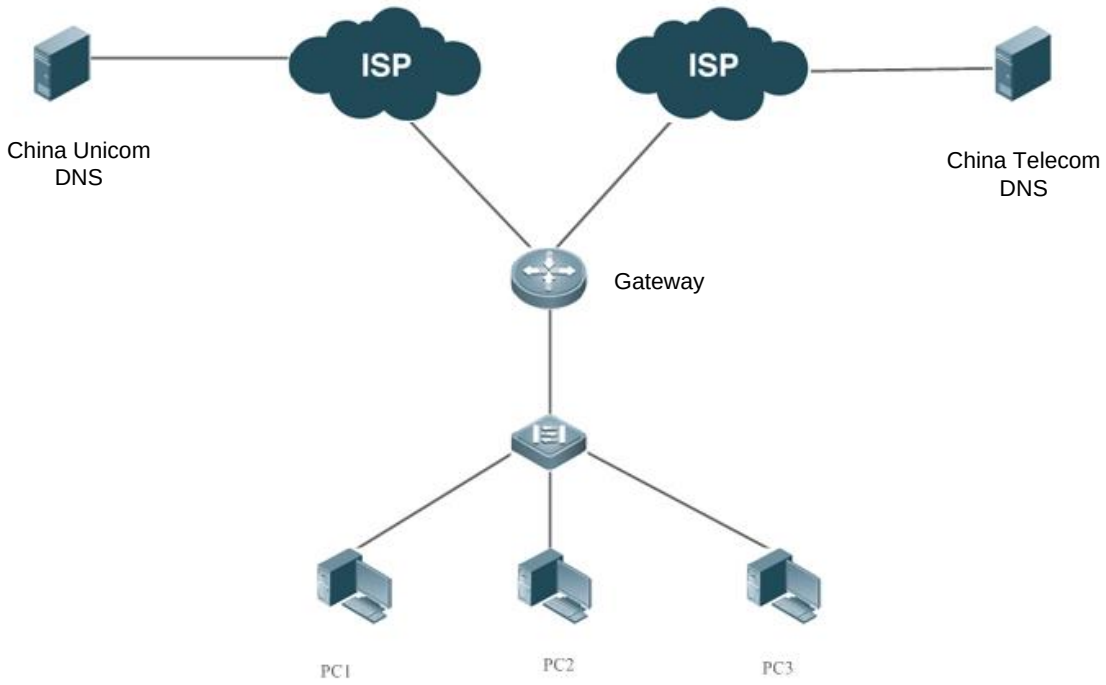
Scenario

Scenario restrictions related to DNS-CACHE are as follows:

1. The DNS is deployed in the internal network.
2. The virtual private network (VPN) supports Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP) clients only.

Figure 1-1 shows the typical application scenario of cybercafé clients.

Figure 1-1 Typical Application Scenario of Cybercafé clients



Remarks	In the cybercafé scenario, the DNS is generally located in an external network. A large number of network applications connect to the Internet via the egress gateway to browse Web pages, play online games, and so on.

Deployment

- Basic NAT: Implement basic network address translation (NAT) to ensure that clients access the Internet normally.
- Application identification: Indentify the application with traffic forwarding.
- Flow control: Implement functions such as traffic guarantee of key applications in combination with APP-IDENTIFY.
- Flow control: Control the application traffic in the network.
- DNS-CACHE: Cache the results of domain name resolutions to avoid network performance from being affected by an unstable external DNS server, thereby improving user experience.

1.3 Features

Basic Concepts

Domain Name

A domain name is an easy-to-remember server address that facilitates communication. During network access, one or more domain names are resolved into a corresponding IP address.

Static Cache

Static cache is a user-defined rule that specifies a resolution correspondence between a domain name and a fixed IP address.

Overview

Feature	Description
DNS-CACHE	Caches the results of domain name resolutions.

1.3.1 DNS-CACHE

DNS-CACHE can cache the results of domain name resolutions. When a client requests for access to a domain name for the first time, the domain name is resolved and the resolution result is cached. When the client requests access to the same domain name next time, the device directly returns the cached result, instead of obtaining the IP address from an external DNS.

Working Principle

Cache matching is performed on a DNS request packet. If the DNS request packet hits the cache, a DNS response packet is constructed and returned, and the DNS request packet is discarded. The matching criteria include the domain name, DNS IP address, and egress gateway. If the DNS request packet misses the cache, the DNS request is forwarded and the DNS response packet is cached.

Related Configuration

Enabling DNS-CACHE

DNS-CACHE is enabled by default.

Run the **dns-cache enable** command in global configuration mode to enable DNS-CACHE.

Run the **no dns-cache enable** command in global configuration mode to disable DNS-CACHE.

Configuring Cache Time

The cache time of a DNS node is 300 seconds by default.

Run the **dns-cache old time** *time* command to adjust the cache time in the range 1–600 seconds.

Run the **no dns-cache old-time** command in global configuration mode to delete related configurations. After the deletion, the cache time is restored to the default value.

Configuring Static Cache Policy

The dynamic cache is matched by default.

Run the **dns-cache static domain** *domain* **ip"***ip1 ip2 …***"** command to configure the static cache policy. You can configure a maximum of eight IP addresses in one policy.

Run the **no dns-cache static domain** *domain* command in configuration mode to delete related configurations.

1.4 Configuration

Configuration	Description and Command	
Enabling/Disabling DNS-CACHE	(Mandatory) It is used to enable traffic monitoring and audit.	
	dns-cache enable	Enables DNS-CACHE.
Configuring Cache Time	(Optional) It is used to configure the cache time of a node.	
	dns-cache old-time *time*	Configures the cache time in seconds. The value ranges from 1 to 600 seconds.
Configuring User-defined Static Cache	(Optional) It is used to configure the user-defined static cache.	
	dns-cache static domain *domain* **ip"***ip1 ip2 …***"**	Configures the user-defined static cache. You can configure a maximum of 100 static cache policies, and one domain name corresponds to a maximum of eight IP addresses.

1.4.1 Enabling/Disabling DNS-CACHE

Configuration Effect

- Enable DNS-CACHE to cache results of domain name resolutions. In this way, the gateway can directly return response packets for requests with the same domain name, instead of applying for the IP address from an external server.

Notes

- If DNS-CACHE is disabled, the DNS cache function is invalid.
- The DNS cache time is limited. The DNS cache time is 300 seconds by default and can be set to 600 seconds at maximum.
- If DNS-CACHE is disabled, cached data is deleted.

Configuration Steps

- Run the **dns-cache enable** command in global configuration mode to enable DNS cache audit.

Verification

- Run the ***show dns-cache enable*** command to check whether DNS-CACHE is enabled.

Related Commands

Enabling Traffic Monitoring and Audit

Command	**dns-cache enable**
Parameter Description	N/A
Command Mode	Global configuration mode
Usage Guide	Run this command to enable DNS-CACHE

Configuration Example

Enabling Traffic Monitoring and Audit

Configuration Steps	Configure this function on the egress gateway.
	`Hostname# configure terminal` `Hostname(config)#dns-cache enable`
Verification	● Check whether DNS-CACHE is enabled.

	`Hostname#show dns-cache enable`
	`dns-cache is on`
	`Hostname#`

1.4.2 Configuring Cache Time

Configuration Effect

- Configure the cache time for storing the cached results. The cache time is 300 seconds by default and ranges from 1–600 seconds.

Notes

- Optional
- If DNS-CACHE is disabled, the DNS cache function is invalid and cached data is deleted.
- The cache time is 300 seconds by default and ranges from 1–600 seconds.
- After the configuration is deleted, the cache time is restored to the default value.

Configuration Steps

- Run the **dns-cache old-time** *time* command in global configuration mode to configure the DNS cache time.

Verification

- Check the cache time of each node.

Related Commands

Configuring Cache Time

Command	**dns-cache old-time** *time*
Parameter Description	*time*: Indicates the cache time. The range is 1–600 seconds.
Command Mode	Global configuration mode
Usage Guide	Run this command to change the cache time of each node.

Configuration Example

Setting the Cache Time to 600 Seconds

Configuration Steps	Set the cache time to 600 seconds on the egress gateway.

	`Hostname# configure terminal`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`Hostname(config)# dns-cache old-time 600`

Verification	● Check the configuration information.
	`Hostname(config)#show run | in dns-cache` `dns-cache old-time 600`

1.4.3 Configuring User-defined Static Cache

Configuration Effect

- Configure the user-defined static cache, so that a domain name is directly resolved into a fixed IP address without involving the DNS server.

Notes

- If DNS-CACHE is disabled, the DNS cache function is invalid.
- You can configure a maximum of 100 policies.
- One domain name corresponds to a maximum of eight IP addresses.

Configuration Steps

- Run a command in global configuration mode to configure static cache.

Verification

- Check whether the designated domain name is directly resolved into the fixed IP address without involving the DNS server.

Related Commands

Configuring the Pre-generation Time of Reports

Command	**dns-cache static domain domain** { **interface** *interface-type interface-number* **| ip "***ip1 ip2 …***"** }
Parameter Description	*domain*: Indicates the domain name, which contains no more than 64 bytes. **interface** *interface-type interface-number*: Indicates the interface type and number. The specified

	domain name will be resolved into the IP address of this interface. *ip*: Indicates the IP address obtained by resolving the domain name.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuration Example

Mapping Domain Name www.baidu.com to IP Address 1.2.3.4 5.6.7.8 9.1.3.5

Configuration Steps	Map the domain name www.baidu.com to the IP address 1.2.3.4 5.6.7.8 9.1.3.5 on the egress gateway.
	Hostname#config Enter configuration commands, one per line. End with CNTL/Z. Hostname(config)#dns-cache static domain www.baidu.com ip "1.2.3.4 5.6.7.8 9.1.3.5"
Verification	● Check the static cache.
	Hostname(config)#show run | in dns-cache dns-cache static domain www.baidu.com ip 1.2.3.4 5.6.7.8 9.1.3.5 Hostname(config)#

1.5 Monitoring

Displaying

Description	Command
Displays the operation status of DNS-CACHE.	**show dns-cache state**

Debugging

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

Description	Command
Debugs data configured in the CLI.	**debug dns-cache cli**

1 Configuring RNFP

1.1 Overview

Ruijie Network Foundation Protection (RNFP) is a collection of means for defending devices against attacks.

When encountering network attacks or high loads, RNFP is capable of protecting key resources on the control and management plane of routers, to prevent device breakdown and improve device availability.

1.2 Applications

Application	Description
There Are a Large Amount of Traffic that Attacks Devices on the Network	A large amount of abnormal traffic on the network will cause very high CPU utilization of devices, slow or suspended response of the Command Line Interface (CLI), loss of link or network control protocol packets, and finally link or network jitter. The processing bandwidth is occupied by illegitimate packets, which results in the failure to process important protocol packets.

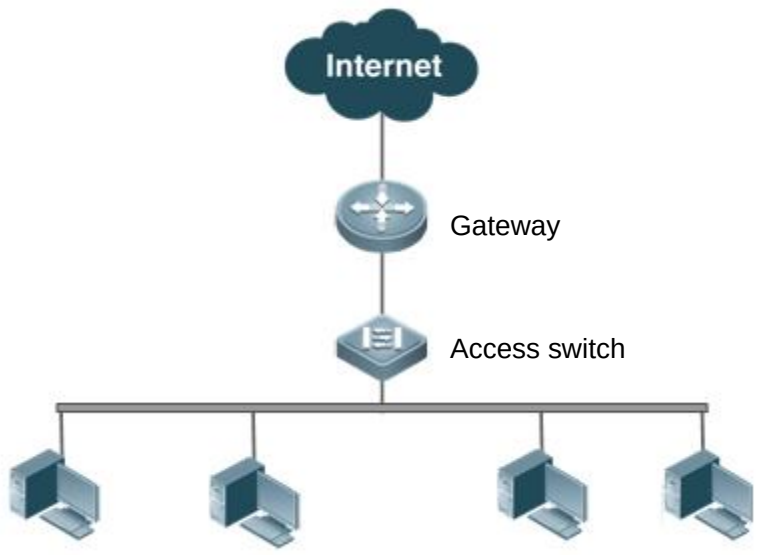
1.2.1 There Are a Large Amount of Traffic that Attacks Devices on the Network

Scenario

In the network-attacked environment, RNFP reduces the CPU utilization in case of attacks and safeguards key protocol packets so that administrators can access the devices normally.

- Restricts attack traffic.
- Safeguards non-attack traffic.

Figure 1-1



Deployment

- Configure the local anti-attack rate-limit policy on the device.
- Add the IP address of the administrator to the whitelist to safeguard the traffic for the administrator to manage devices.

1.3 Features

Basic Concepts

Classify

RNFP identifies and classifies data traffic transmitted to the control plane. It classifies traffic into the protocol traffic, manage traffic, and data traffic, which facilitates submodules to limit the rate and filter traffic in a differentiated manner.

Sub-interface

All traffic transmitted to the control plane is classified by Classify into three types, which are separately processed by the three sub-interfaces below:

- Protocol sub-interface: Processes all protocol control traffic transmitted to the local device, including link-layer protocol packets and routing protocol packets.
- Manage sub-interface: Processes all management protocol traffic transmitted to the local device, such as FTP, Telnet, SNMP, and ARP protocol packets.
- Data sub-interface: Processes all data traffic that cannot be processed by the fast forwarding plane.

SCPP

Segregate Control Plane Protection (SCPP), according to user-defined policies, match traffic of the three sub-interfaces to different ACLs according to user-defined policies, to implement finer-granularity rate limit and protection.

Glean-CAR

Glean-CAR limits the rate of the traffic that is matched by the fast forwarding plane to the REF Glean adjacency (the traffic is matched to the direct route but the host route that matches the destination IP address is not found, and therefore the traffic needs to be transmitted to the control plane for destination IP address resolution).

ARP-CAR

The fast forwarding plane cannot process ARP packets and need to transmit them to the control plane for processing. ARP-CAR can limit the rate of ARP packets for each neighbor.

Port-Filter

Port-Filter checks whether ports are enabled on local applications for TCP and UDP packets transmitted to the local device, and filters out the traffic transmitted to the local device, for which the network service is not enabled on the local device, before the traffic reaches the control plane.

MPP

Management Plane Protection (MPP) allows administrators to specify one or multiple interfaces as the inband management interfaces (supporting receiving of management packets and forwarding of normal services). After MPP is enabled, only a specified inband management interface is allowed to receive management packets of a specified protocol. Service packets, protocol packets, and ARP packets are not affected.

ACPP

Aggregate Control Plane Protection (ACPP) uses the default or user-defined rate to limit the rate of the traffic on the protocol sub-interface, manage sub-interface, and data sub-interface based on classification results of Classify, to ensure that the traffic does not exceed the processing capacity of the control plane, thereby protecting the control plane.

Local Anti-attack Whitelist

When accessing an attacked device, users will feel stuck or fail to access the device. The local anti-attack whitelist can be configured to free whitelisted users from all anti-attack policies, their device access packets are not discarded due to rate limit, thereby preventing stuck access or access failures.

User Management Device Restriction

User management device restriction forbids intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in Secure Shell (SSH) mode, and manage the device over the Simple Network Management Protocol (SNMP), with no need to associate Access Control Lists (ACLs).

ARP Attack Detection

In a Layer-2 environment, the Address Resolution Protocol (ARP) attacks in the intranet may affect the normal Internet access of intranet users. ARP attack detection aims at detecting possible ARP attacks on the network and listing suspicious hosts of ARP attacks for administrators to locate and rectify faults.

- Sub-interfaces involved in the device anti-attack are different from traditional sub-interfaces of devices. A device anti-attack interface indicates an internal channel for transmitting a certain type of traffic to the control plane. Such interfaces can be used to conveniently conduct anti-attack configuration and processing on traffic.
- Anti-attack sub-functions of devices (SCPP, Glean-CAR, ARP-CAR, Port-Filter, MPP, and ACPP) are independent of each other in the configuration. Users can combine or configure anti-attack sub-functions according to requirements and policies. Note that some sub-interfaces have restrictions on the application sub-interfaces.

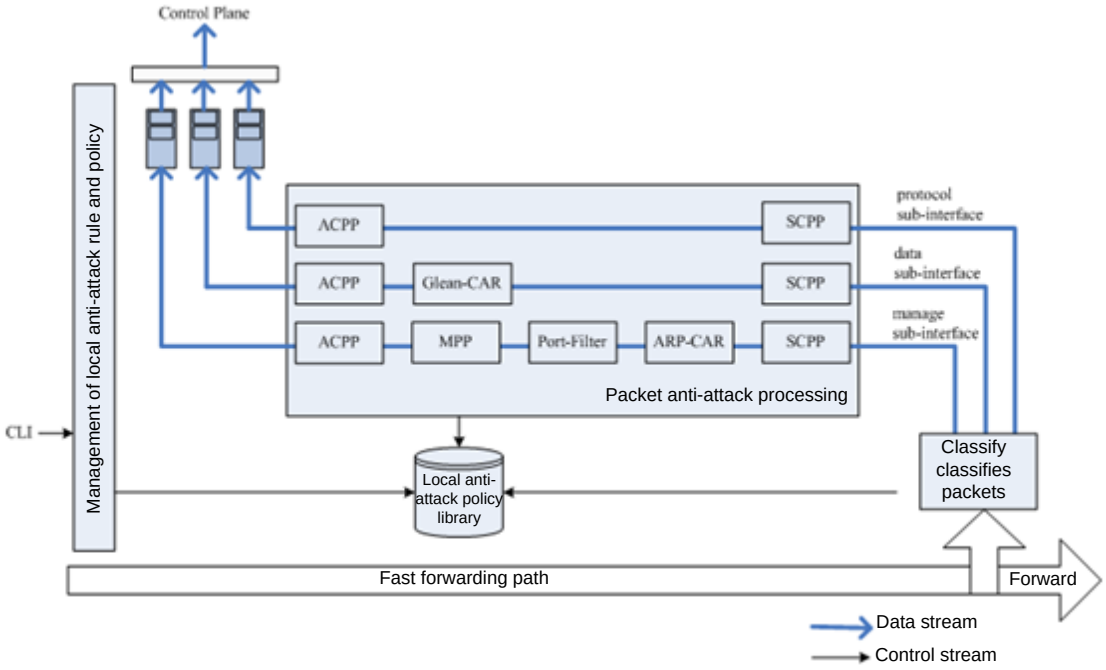
Overview

Feature	Description
Local Anti-attack	Distributes packets transmitted to the control plane to different sub-interfaces for rate limit based on the packet type.
Attack Detection	Detects attack behaviors on the network.
Local Anti-attack Whitelist	Ensures management traffic by not limiting the rate of traffic from whitelisted users.
User Management Device Restriction	Forbids intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.

1.3.1 Local Anti-attack

Classify and filter data packets to be processed by the control plane, and limit their rates, so as to protect key resources of the control plane.

Working Principle



As shown in the figure above, packet classification and rate limit are implemented by multiple submodules. Packets to be processed by the control plane are classified and then rate limit is conducted on them according to policies configured for different sub-interfaces.

protocol sub-interface

The protocol sub-interface conducts rate limit and filtering on all protocol control traffic transmitted to the local device. It covers two submodules: SCPP and ACPP. Packets are processed by in SCPP > ACPP order.

data sub-interface

The data sub-interface conducts rate limit and filtering on all traffic that cannot be processed by the fast forwarding plane. It covers three submodules: SCPP, Glean-CAR, and ACPP. Packets are processed by in SCPP > Glean-CAR > ACPP order.

manage sub-interface

The manage sub-interface conducts rate limit and filtering on all management protocol traffic transmitted to the local device. It covers five submodules: SCPP ARP-CAR, Port-Filter, MPP, and ACPP. Packets are processed by in SCPP > ARP-CAR > Port-Filter > MPP >ACPP order.

ACPP directly forwards the packets allowed by SCPP, ARP packets, and Glean packets without rate limit.

Related Configuration

Configuring Local Anti-attack

By default, all rate limit functions are disabled.

Run the **control-plane** [**protocol** | **manage** | **data**] command to access different sub-interfaces and configure different function policies for the sub-interfaces.

Run the **ef-rnfp enable** command to globally enable packet classification and rate limit.

Run the **scpp list** *acl_no* { [**bw-rate** *rate* **bw-burst-rate** *brust-rate*] [**conn-create-rate** *create-rate* **conn-create-burst-rate** *create-burst-rate*] [**conn-total** *num*] } [**log**] command to configure SCPP to limit the rate of ACL-matched packets and adjust the rate limit values of SCPP.

Run the **acpp bw-rate** *rate* **bw-burst-rate** *burst-rate* [**log**] command to configure the ACPP rate limit.

Run the **glean-car** *packet_rate_per_group* [**log**] command to configure Glean-CAR and limit the rate of packets that matches the Glean-CAR.

Run the **port-filter** [**log**] command to configure port-filter to reject packets received by locally disabled ports.

Run the **management-interface** *interface* **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** } [**log**] command to configure the management interface and configure the management interface to receive packets of the specified management protocols. Non-configured interfaces cannot receive packets of these protocols.

Run the **arp-car** *packet_rate_per_group* [**log**] command to configure ARP-CAR to limit the rate of ARP packets.

1.3.2 Attack Detection

Detect and record attack behaviors on the network.

Working Principle

When the total packets discarded by submodules of sub-interfaces reach a threshold, the device considers that traffic attack occurs on the network. It collects statistics on the type of attack packets, IP addresses, packet count, and packet size.

When the device receives abnormal ARP packets from a host, it records the host as the suspicious host of ARP attacks. The device considers that ARP spoofing occurs and adds the hosts to the ARP spoofing suspect list in the event of the following cases: A host conducts ARP scanning on the entire network (by default, more than 200 ARP requests are transmitted within 10s); the MAC address of a host maps to multiple IP addresses; the MAC address attempted to be updated based on an ARP request is different from the existing MAC address.

Related Configuration

↘ Configuring Traffic Attack Detection

By default, attack detection is disabled. When the **ef-rnfp enable** command is executed to globally enable packet classification and rate limit, traffic attack detection is enabled by default.

Run the **attack threshold** *drop-num* command to set the attack judgment threshold. The default value is 500.

Run the **show attack** { **current** | **history** } command to display attack information.

↘ Configuring ARP Attack Detection

By default, attack detection is disabled.

Run the **anti-arp-spoof** command to enable ARP attack detection.

Run the **anti-arp-spoof** [**scan** *arp-num*] command to set the ARP scanning threshold. The default value is 20.

Run the **show arp-suspect** command to display the ARP spoofing suspect list.

1.3.3 Local Anti-attack Whitelist

Add the IP address of the administrator to the whitelist so that the administrator can normally manage devices even if the network is attacked.

Working Principle

The local anti-attack module does not limit the rate of traffic from whitelisted IP addresses but allows the traffic to directly pass.

Related Configuration

Configuring the Local Anti-attack Whitelist

By default, there is no IP address in the whitelist.

Run the **security web permit** *low-ip-address* [*high-ip-address*] command to configure the whitelist range. A maximum of 32 IP addresses or IP address segments are supported.

1.3.4 User Management Device Restriction

For common Ping, Web, Telnet, SSH, and SNMP attack behaviors on the network, user management device restriction forbids intranet/extranet users to ping the device or access the Web page of the device, with no need to use ACLs, delivering great flexibility and convenience.

Working Principle

User management device restriction intercepts ping packets, Web packets for device access, Telnet packets or SSH login packets, and SNMP packets, in an effort to forbid the ping, Web access, Telnet and SSH login, and SNMP management behaviors.

Related Configuration

Configuring User Management Device Restriction

By default, the function is disabled.

Run the **security deny** command to configure the user management device restriction function.

1.4 Configuration

Configuration	Description and Command	
Configuring Local Anti-attack	⚠ (Optional) It is used to configure rate limit rules.	
	control-plane	Enters the control-plane configuration mode.
	scpp	Configures SCPP.
	glean-car	Configures Glean rate limit.
	arp-car	Configures ARP rate limit.

	port-filter	Configures port filtering.
	mpp	Configures MPP.
	acpp	Configures ACPP.
	ef-rnfp	Enables local anti-attack.
	rnfp-ping-reply { **enable** | **threshold** }	Configures rnfp-ping response acceleration.
Configuring Attack Detection	(Optional) It is used to configure attack detection rules.	
	attack threshold	Configures the attack confirmation threshold.
	anti-arp-spoof	Configures ARP attack detection.
Configuring the Local Anti-attack Whitelist	(Optional) It is used to configure local anti-attack whitelisted users.	
	security web permit	Configures whitelisted IP addresses.
Configuring User Management Device Restriction	(Optional) It is used to forbid intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.	
	security deny	Forbids intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.

1.4.1 Configuring Local Anti-attack

Configuration Effect

- Reduce the CPU utilization of the device even if the network is attacked.
- Improve the CLI response speed even if the network is attacked.
- Safeguard important packets such as link or network control protocol packets when the network is attacked.

Notes

- If the Telnet operation and Web access slow down after the function is configured, you can add the IP address used in the Telnet operation and Web access to the local anti-attack whitelist to ensure the traffic of the IP address.

Configuration Steps

↘ Entering the control-plane Configuration Mode

- Mandatory.
- Enter different sub-interfaces.

↘ Configuring Rate Limit

- Mandatory.
- Configure different functions to implement rate limit.

Verification

- Check the CPU utilization.
- Check the CLI response speed.
- Check whether important protocol packets are safeguarded.

Related Commands

Entering the control-plane Configuration Mode

Command	**control-plane** [**protocol** | **manage** | **data**]
Parameter Description	**protocol**: Enters the protocol sub-interface. **manage**: Enters the manage sub-interface. **data**: Enters the data sub-interface. Non-sub-interface functions are configured if no parameter is set.
Command Mode	Global configuration mode
Usage Guide	N/A

Configuring SCPP

Command	**scpp list** *acl_no* { [**bw-rate** *rate* **bw-burst-rate** *burst-rate*] [**conn-create-rate** *create-rate* **conn-create-burst-rate** *create-burst-rate*] [**conn-total** *num*] } [**log**]
Parameter Description	**list** *acl_no*: Indicates ACL rules, which are used to search out the traffic to be processed by SCPP. **bw-rate** *rate*: Indicates the rate limit. The unit is pps. **bw-burst-rate** *burst-rate*: Indicates the burst rate limit. The unit is pps. **conn-create-rate** *create-rate*: Indicates the rate limit for connection creation per second. **conn-create-burst-rate** *create-burst-rate*: Indicates the rate limit for burst connection creation per second. **conn-total** *num*: Indicates the limit on the total number of connections. **log**: Indicates whether to output logs.
Command Mode	control-plane mode
Usage Guide	The three sub-interfaces can conduct SCPP processing on traffic on the sub-interfaces. By default, SCPP is disabled. It is enabled only after users explicitly configure SCPP rules.

Configuring Glean Rate Limit

Command	**glean-car** *packet_rate_per_group*
Parameter Description	*packet_rate_per_group*: Configures the rate limit value for the traffic that is initiated by users (sources), who are in the same group according to the hash algorithm, and is matched to the Glean adjacency. The unit is pps.
Command Mode	control-plane mode
Usage Guide	The Glean-CAR function can be configured only on the data sub-interface. Currently, the hash algorithm extracts lower *N* bits from the source address (the value of *N* varies with products).

	Note that Glean-CAR can limit the rate of the traffic that is initiated by users, who are in the same group according to the hash algorithm, and is matched to the Glean adjacency. For example, User A (with IP address of 192.168.52.57) and User B (with IP address of 192.168.60.57) (share the same hash result) send traffic to directly connected Destination Host C (with IP address of 172.16.0.5). Before 172.16.0.5 is successfully resolved by ARP, if Glean-CAR 5 is configured, a maximum of five packets out of the traffic initiated by User A and User B can be transmitted to the control plane every second, requesting the control plane to conduct ARP resolution on the destination IP address. By default, Glean-CAR is disabled. It is enabled only after users explicitly configure Glean-CAR rules.

Configuring ARP Rate Limit

Command	**arp-car** *packet_rate_per_group*
Parameter Description	*packet_rate_per_group*: Configures the rate limit value for ARP traffic that is initiated by users, who are in the same group according to the hash algorithm. The unit is pps.
Command Mode	control-plane mode
Usage Guide	The ARP-CAR function can be configured only on the manage sub-interface. Currently, the hash algorithm extracts lower *N* bits from the source address (the value of *N* varies with products). Note that ARP-CAR can limit the rate of the ARP traffic initiated by users who are in the same group according to the hash algorithm. For example, User A (with IP address of 192.168.52.57) and User B (with IP address of 192.168.60.57) (share the same hash result) send the ARP request for 192.168.52.1 to the device. If ARP-CAR 5 is configured, a maximum of five packets out of the traffic initiated by User A and User B can be transmitted to the control plane every second, requesting the control plane to give ARP response. By default, ARP-CAR is disabled. It is enabled only after users explicitly configure ARP-CAR rules.

Configuring Port Filtering

Command	**port-filter**
Parameter Description	**N/A**
Command Mode	control-plane mode
Usage Guide	Configure Port-Filter to filter out received transport-layer packets, for which services are not enabled. The Port-Filter function can be configured only on the manage sub-interface. By default, Port-Filter is disabled. It is enabled only after users explicitly configure Port-Filter.

Configuring MPP

Command	**management-interface** *interface* **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** }
Parameter Description	*interface*: Specifies an inband management interface. **allow** { **ftp** | **http** | **ssh** | **snmp** | **telnet** | **tftp** }: Configures the allowed management protocol.
Command Mode	control-plane mode
Usage Guide	Configure MPP to specify an inband management interface and management protocol packets allowed by the interface.

	The MPP sub-function can be configured only on the manage sub-interface. A maximum of 16 inband management interfaces can be configured, and each interface can receive packets of multiple or all management protocols. After MPP is enabled, non-inband management interfaces are not allowed to receive management packets, and inband management interfaces are allowed to receive packets of only specified management protocols. By default, MPP is disabled. It is enabled only after users explicitly configure MPP rules.

Configuring ACPP

Command	**acpp bw-rate** *rate* **bw-burst-rate** *burst-rate*
Parameter Description	*rate*: Indicates rate limit. The unit is pps. *burst-rate*: Indicates burst rate limit. The unit is pps.
Command Mode	control-plane mode
Usage Guide	Configure ACPP for classified traffic that is transmitted to the control plane. The three sub-interfaces can conduct ACPP processing on the traffic on the sub-interfaces. By default, ACPP is disabled. It is enabled only after users explicitly configure ACPP rules.

Enabling Local Anti-attack

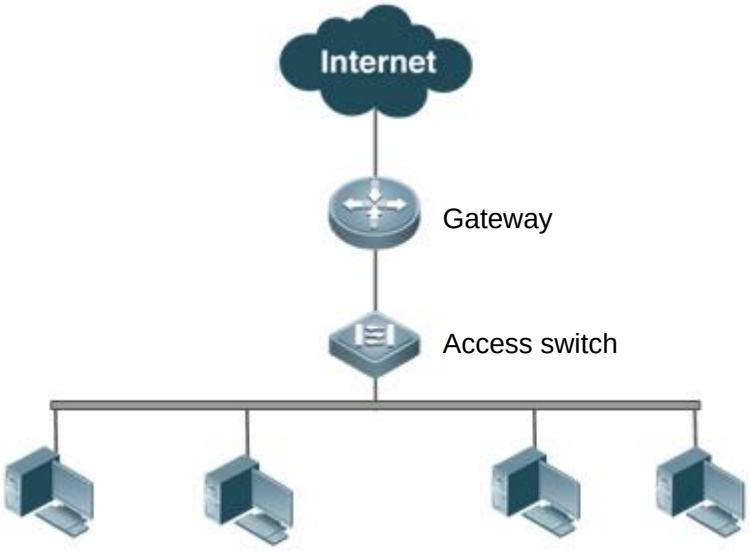
Command	**ef-rnfp** { **enable** | **disable** }
Parameter Description	**enable**: Enables local anti-attack. **disable**: Disables local anti-attack.
Command Mode	control-plane mode
Usage Guide	When no local anti-attack policy is configured, if local anti-attack is enabled, the default policy (ACPP on each sub-interface, port-filter on the manage sub-interface, and Glean-CAR on the data sub-interface) is enabled. The default anti-attack rules and policy are set based on different products and platforms. After local anti-attack is disabled, rate limit functions are all unavailable.

Configuring Ping Response Acceleration

Command	**rnfp-ping-reply** { **enable** | **threshold** }
Parameter Description	**enable**: Accelerates the response to external ping requests. **threshold**: Indicates the threshold for the number of ping packets responded per second. The value ranges from 0 to 65,535, in packets per second (pps).
Command Mode	Global configuration mode
Usage Guide	When ping response acceleration is enabled, the forwarding plane directly responds to external ping requests. This reduces response latency. When ping response acceleration is disabled, ping requests will be responded through the standard protocol stack. The ping response acceleration function is disabled by default.

Configuration Example

Configuring Local Anti-attack on the Gateway

Scenario Figure 1-2	
Configuration Steps	● Configure the local anti-attack rate-limit policy on the gateway. ● Configure ACPP on the protocol sub-interface, and set the rate limit to 500 pps for the traffic on the protocol sub-interface and allowable burst peak to 600 pps. ● Configure ACPP on the data sub-interface, and set the rate limit to 500 pps for the traffic on the data sub-interface and allowable burst peak to 600 pps. ● Configure Glean-CAR to allow 10 packets from each source to be matched to the Glean adjacency every second. ● Configure ACPP on the manage sub-interface, and set the rate limit to 500 pps for the traffic on the manage sub-interface and allowable burst peak to 600 pps. ● Configure ARP-CAR to allow 10 ARP packets from each source to pass every second. ● Configure Port-Filter. ● Configure MPP rules, in which Port Gi0/0 is specified as the inband management interface, and the interface is allowed to receive packets of only the Telnet and SNMP protocols. ● Enable local anti-attack globally.

A	`Hostname # configure terminal`
	`Hostname(config)# control-plane protocol`
	`Hostname(config-cp)# acpp bw-rate 500 bw-burst-rate 600`
	`Hostname(config)# control-plane data`
	`Hostname(config-cp)# acpp bw-rate 500 bw-burst-rate 600`
	`Hostname(config-cp)# glean-car 10`
	`Hostname(config)# control-plane manage`
	`Hostname(config-cp)# acpp bw-rate 500 bw-burst-rate 600`

	Hostname(config-cp)# arp-car 10 Hostname(config-cp)# port-filter Hostname(config-cp)# management-interface gi0/0 allow telnet snmp Hostname(config)# control-plane Hostname(config-cp)# ef-rnfp enable
Verification	Run the **show ef-rnfp alll** command to display the configuration.

A	Hostname# show ef-rnfp all
	Aggregate control plane protection information:
	  Data subinterface: enable
	  RULE:
	  bandwidth rate limit: 500(pps), burst: 600(pps)
	  log: off
	  STATISTIC:
	  dropped 0 packets
	  Manage subinterface: enable
	  RULE:
	  bandwidth rate limit: 500(pps), burst: 600(pps)
	  log: off
	  STATISTIC:
	  dropped 0 packets
	  Protocol subinterface: enable
	  RULE:
	  bandwidth rate limit: 500(pps), burst: 600(pps)
	  log: off
	  STATISTIC:
	  dropped 0 packets
	Segregate control plane protection information:
	  Data subinterface: disable
	  Manage subinterface: disable
	  Protocol subinterface: disable
	ARP CAR information:
	  Manage subinterface: enable
	  RULE:

```
      allow packet rate per source:  10(pps)
      log:  off
    STATISTIC:
      dropped 0 packets
Glean CAR information:
  Data subinterface:  enable
    RULE:
      allow packet rate per source:  10(pps)
      log:  off
    STATISTIC:
      dropped 0 packets
Port Filter information:
  Manage subinterface:  enable
    RULE:
      TCP open port:
        23, 80, 1723, 2650, 4430, 8081,
      UDP open port:
        67, 68, 161, 514, 3784, 3785, 6000,
        log:  off
    STATISTIC:
      dropped 0 tcp packets
      dropped 0 udp packets
Management plane protection information:
  Manage subinterface:  enable
    RULE:  management interface:  GigabitEthernet 0/0, id:  1fa52
      allow:   snmp telnet
      log:  off
    STATISTIC:
      dropped 0 disallow management protocol packets
  dropped 0 management protocol packet from non management interface
```

Common Errors

- If only an interface is configured as the inband management interface, other interfaces may not be managed normally.

1.4.2 Configuring Attack Detection

Configuration Effect

- The device can detect and record attacks occurring on the network.

Notes

- The local anti-attack must be enabled.

Configuration Steps

Entering the Global control-plane Mode

- Mandatory.

Configuring the Traffic Attack Detection Threshold

- Mandatory.
- Configure the traffic attack detection threshold.

Configuring ARP Attack Detection

- Mandatory.
- Configure the ARP attack detection policy.

Verification

- The device can detect traffic attacks on the network.
- The device can detect ARP attacks on the network.

Related Commands

Configuring the Attack Confirmation Threshold

Command	**attack threshold** *drop-num*
Parameter Description	*drop-num*: Indicates the rate threshold of packets discarded by the local anti-attack module for determining whether network attacks exist. The unit is pps.
Command Mode	control-plane mode
Usage Guide	N/A

Configuring ARP Attack detection

Command	**anti-arp-spoof** [**scan** *arp-num*]
Parameter Description	*arp-num*: Indicates the quantity threshold of ARP packets received from an IP address per second within 10 seconds for determining whether the IP address is used to conduct ARP scanning. ARP attack detection is enabled if no parameter is set.
Command Mode	control-plane mode
Usage Guide	Enable ARP anti-attack. If this command is run, the device is capable of identifying ARP spoofing. It considers that ARP spoofing occurs and adds the hosts to the ARP spoofing suspect list in the event of

	the following cases: A host conducts ARP scanning on the entire network (more than 200 ARP requests are transmitted within 10s); the MAC address of a host maps to multiple IP addresses; the MAC address attempted to be updated based on an ARP request is different from the existing MAC address.

Configuration Example

↘ Configuring Attack Detection

Configuration Steps	● Enable the local anti-attack function globally. ● Set the traffic attack threshold. ● Configure ARP attack detection.
	Hostname# configure terminal Hostname(config)# control-plane Hostname(config-cp)# ef-rnfp enable Hostname(config-cp)# attack threshold 500 Hostname(config-cp)# anti-arp-spoof scan 10 Hostname(config-cp)# anti-arp-spoof
Verification	● Display traffic attack information. ● Display ARP attack information.
	Hostname# show ip pim sparse-mode mroute Hostname# show attack-info current System currently not in attack! Hostname# show attack-info history System attack record at 1970-1-2 15:53:18, System in attack 8s ALL: 6958 packets, 584680 bytes PROTOCOL packets bytes ARP 1733 103980 UDP 5225 480700 TOP5 IP attack: IP packets bytes interface 172.18.3.84 2797 257324 Gi0/5 172.18.3.52 2428 223376 Gi0/5 172.18.3.80 1635 98100 Gi0/5 192.168.205.196 92 5520 Gi0/5 3.3.3.6 6 360 Gi0/5 Hostname#show arp-suspect IP address MAC address

	192. 168. 1. 1 00d0. f800. 0002

1.4.3 Configuring the Local Anti-attack Whitelist

Configuration Effect

- When the device is attacked, whitelisted users can manage the device in Telnet or Web mode.

Notes

- Only add the IP address of the administrator to the whitelist.

Configuration Steps

↘ **Entering Global control-plane Mode**

- Mandatory.

↘ **Configuring Whitelisted Users**

- Optional.

Verification

Simulate network attacks to initiate device attacks, enable the local anti-attack, and configure whitelisted users.

- Non-whitelisted users feel stuck when telnetting to or accessing the Web page of the device, or fail to access the Web page of the device.
- Whitelisted users can telnet to and access the Web page of the device smoothly.

Related Commands

↘ **Configuring Anti-attack Whitelisted Users**

Command	**security web permit** *low-ip-address* [*high-ip-address*]
Parameter Description	*low-ip-address*: Indicates the allowable IP address or the start IP address of the allowable IP address range. *group-or-source-address*: Indicates the end IP address of the allowable IP address range.
Command Mode	control-plane mode
Usage Guide	If a user configures security deny to deny Web access but needs to allow some specified IP addresses to access the Web page of the device, the user can run this command to add allowable IP addresses to the web permit IP whitelist. This command specifies the IP addresses that are allowed to access the Web page of the device (regardless of the local anti-attack rate limit and deny command).

Configuration Example

↘ **Configuring the Local Anti-attack Whitelist (Whitelisted IP Address Range: 192.168.1.2—192.168.1.10)**

Configuration Steps	● Configure whitelisted users.

	Hostname# configure terminal Hostname(config)# control-plane Hostname(config-cp)# security web permit 192.168.1.2 192.168.1.10
Verification	Simulate network attacks and configure local anti-attack whitelisted users. ● Users not included in the local anti-attack whitelist cannot smoothly telnet to the device or access the Web page of the device. ● Users included in the local anti-attack whitelist can smoothly telnet to the device and access the Web page of the device.
	N/A

Common Errors

- All intranet users are added to the whitelist. As a result, the CPU utilization will be abnormal in the case of attacks from intranet users.

1.4.4 Configuring User Management Device Restriction

Configuration Effect

- After the ping operation is forbidden, non-whitelisted users cannot ping the device.
- After the Web access is forbidden, non-whitelisted users cannot access the Web page of the device.
- After Telnet and SSH login are forbidden, non-whitelisted users cannot telnet to the device or log in to the device in SSH mode.
- After SNMP management is forbidden, non-whitelisted users cannot manage the device over SNMP.

Notes

- This function can be used with the local anti-attack whitelist.

Configuration Steps

↘ **Entering Global control-plane Mode**

- Mandatory.

↘ **Forbidding Intranet/Extranet Users to Ping the Device**

- Optional.

↘ **Forbidding Intranet/Extranet Users to Access the Web Page of the Device**

- Optional.

↘ **Forbidding Intranet/Extranet Users to Telnet to the Device or Log In to the Device in SSH Mode**

- Optional.

↘ **Forbidding Intranet/Extranet Users to Manage the Device over SNMP**

- Optional.

Verification

Enable the function of forbidding intranet/extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.

- Non-whitelisted users fail to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and mange the device over SNMP.
- Whitelisted users can ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and mange the device SNMP.

Related Commands

Configuring User Management Device Restriction

Command	**security deny** { **lan** { **tcp** | **udp** } **port** *port-number* | **lan-ping** | **lan-snmp** | **lan-ssh** | **lan-telnet** | **lan-web** | **vpn-telnet-ssh-web** | **wan** { **tcp** | **udp** } **port** *port-number* | **wan-ping** | **wan-snmp** | **wan-ssh** | **wan-telnet** | **wan-web** }
Parameter Description	**lan**: Forbids users to access specified TCP or UDP ports of the device from a LAN port. **tcp**: Indicates TCP ports. **udp**: Indicates UDP ports. **port** *port-number*: Indicates the TCP or UDP port number. **lan-ping**: Forbids users to ping the device from a LAN port. **lan-snmp**: Forbids users to manage the device over SNMP from a LAN port. **lan-ssh**: Forbids users to login to the device in SSH mode from a LAN port. **lan-telnet**: Forbids users to telnet to the device from a LAN port. **lan-web**: Forbids users to access the Web page of the device from a LAN port. **vpn-telnet-ssh-web**: Forbids VPN users to telnet to the device, login to the device in SSH mode or access the Web page of the device. **wan**: Forbids users to access specified TCP or UDP ports of the device from a WAN port. **wan-ping**: Forbids users to ping the device from a WAN port. **wan-snmp**: Forbids users to manage the device over SNMP from a WAN port. **wan-ssh**: Forbids users to login to the device in SSH mode from a WAN port. **wan-telnet**: Forbids users to telnet to the device from a WAN port. **wan-web**: Forbids users to access the Web page of the device from a WAN port.
Command Mode	control-plane mode
Usage Guide	If the functions are enabled but no whitelist is configured, you need to edit configurations through the console or Telnet.

Configuration Example

Configuring the Local Anti-attack Whitelist (Whitelisted IP Address Range: 192.168.1.2—192.168.1.10)

Configuration Steps	● Configure whitelisted users. ● Configure the functions of forbidding Intranet/Extranet users to ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and manage the device over SNMP.
	Hostname# configure terminal Hostname(config)# control-plane Hostname(config-cp)# security web permit 192.168.1.2 192.168.1.10 Hostname(config-cp)# security deny wan-ping Hostname(config-cp)# security deny wan-web Hostname(config-cp)# security deny lan-ping Hostname(config-cp)# security deny lan-web Hostname(config-cp)# security deny lan-snmp Hostname(config-cp)# security deny wan-snmp Hostname(config-cp)# security deny lan-ssh Hostname(config-cp)# security deny lan-telnet Hostname(config-cp)# security deny wan-ssh Hostname(config-cp)# security deny wan-telnet Hostname(config-cp)#
Verification	● Non-whitelisted users cannot ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and or mange the device over SNMP. ● Whitelisted users can ping the device, access the Web page of the device, telnet to the device or log in to the device in SSH mode, and mange the device over SNMP.

Common Errors

- After the ping operation and Web access are forbidden, but no user is added to the whitelist, users cannot log in to the Web page of the device.

1.5 Monitoring

Clearing

Description	Command
Clears historical attack information.	**clear attack-info history**

Displaying

Description	Command

Displays device anti-attack configurations and statistics.	**show ef-rnfp** {**acpp** { **data** | **manage** | **protocol** } | **scpp** { **data** | **manage** | **protocol** } | **glean-car** | **arp-car** | **port-filter** | **mpp** | **all** | **web-permit-ip** | **anti-arp-spoof** }
Displays current attack traffic.	**show attack-info current**
Displays historical attack traffic.	**show attack-info history**
Displays the ARP spoofing suspect list.	**show arp-suspect**

Debugging

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

Description	Command
Debugs local anti-attack.	**debug** { **acpp** | **scpp** | **glean-car** | **arp-car** | **port-filter** | **mpp** | **all** }
Records debugging data into the buffer.	**show ef-rnfp debug-buf clear**
Outputs debugging data.	**show ef-rnfp debug-buf echo**