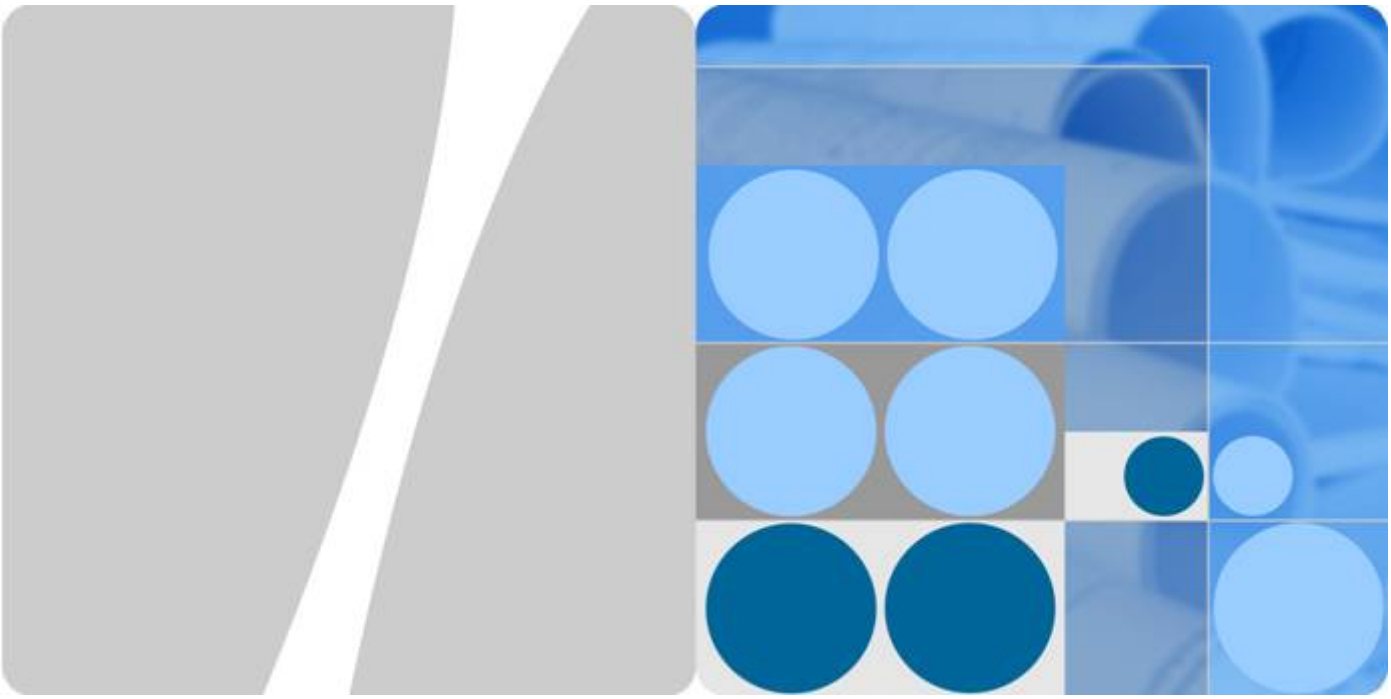


Huawei Access Points

V200R003C00

Configuration Guide

Issue 03

Date 2014-01-25

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

About This Document

Intended Audience

This document provides the concepts, configuration procedures, and configuration examples supported by the Access Point.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.
 NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.

Symbol	Description
NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

The command conventions that may be found in this document are defined as follows.

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

NOTE

The interface types, command outputs, and device models provided in this manual vary according to device configurations and may differ from the actual information.

Interface Numbering Conventions

Interface numbers used in this manual are examples. In device configuration, use the existing interface numbers on devices.

Security Conventions

- Password setting

  When configuring a password in plain text, the password is saved in the configuration file in plain text. The plain text has high security risks, so the cipher text is recommended. To ensure device security, change the password periodically.

  When you configure a password in cipher text that starts and ends with %@%@.....%@%@ or @%@%.....@%@% (the password can be decrypted by the device), the password is displayed in the same manner as the configured one in the configuration file. Do not use this setting.

- Encryption algorithm

  Currently, the device uses the following encryption algorithms: DES, 3DES, AES, RSA, SHA1, SHA-2, MD5 and SMS4. The encryption algorithm depends on the applicable scenario. Use the recommended encryption algorithm; otherwise, security defense requirements may be not met.

  - For the symmetrical encryption algorithm, use AES with the key of 128 bits or more.
  - For the asymmetrical encryption algorithm, use RSA with the key of 2048 bits or more.
  - For the hash algorithm, use SHA with the key of 256 bits or more.
  - For the HMAC algorithm, use HMAC-SHA2.

- Personal data

  Some personal data may be obtained or used during operation or fault location of your purchased products, services, features, so you have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.

Change History

Changes between document issues are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Changes in Issue 03 (2014-01-25)

This version has the following updates:

The following information is modified:

- Configuration Guide - Radio Resource Management
  - **5.2.1 Radio Calibration**
- Configuration Guide - QoS
  - **8.3.8 Configuring Traffic Policing**

The following information is deleted:

- Configuration Guide - Basic Configuration
  - Introduction to CLI

Changes in Issue 02 (2013-09-30)

This version has the following updates:

The following information is added:

- Radio Resource Management Configuration
  - **5.6 Configuring Background Neighbor Probing**

The following information is modified:

- WLAN Service Configuration
  - **4.6.3.7 Configuring a WLAN Service Set**
- Radio Resource Management Configuration
  - **5.7 Configuring Radio Calibration**
  - **5.11.1 Example for Configuring Radio Calibration for APs**

Changes in Issue 01 (2013-05-15)

Initial commercial release.

Contents

1 Configuration Guide - Basic Configuration

About This Chapter

This document describes methods to use command line interface and to log in to the device, file operations, and system startup configurations.

1.1 CLI Overview
Users perform configuration and routine maintenance on devices by running commands.

1.2 Logging In to the System for the First Time
This section describes how to log in to a new device to configure the device. You can log in through the console port.

1.3 Configuring a User Interface
When a user logs in to the device using the console port, Telnet, or SSH, the system manages the session between the user and the device on the corresponding user interface.

1.4 Configuring User Login
Users can log in to the device through a console port, Telnet, STelnet to perform local or remote device maintenance.

1.5 File Management
All files on the device are stored in storage devices and can be managed in multiple modes. The current device can function as a client to access files on other devices.

1.6 Configuring System Startup
When the device is powered on, system software starts and configuration files are loaded. To ensure smooth running of the device, manage system software and configuration files efficiently.

1.7 Configuring Fit/Fat Switching
You can switch an AP from a fat AP to a fit AP or a fit AP to a fat AP as required.

1.1 CLI Overview

Users perform configuration and routine maintenance on devices by running commands.

1.1.1 How to Use Command Lines

This section describes how to use command lines and some techniques to improve operating efficiency.

1.1.1.1 Entering Command Views

This section describes how to enter and exit from command views.

The device has many functions; therefore various configuration commands and query commands are provided to facilitate device management and maintenance. Huawei access point registers commands to different command views based on the functions of the commands, so users can easily use them. To use a function, enter the corresponding command view first and then run corresponding commands.

The device provides various command views. For the methods of entering the command views except the following views, see the *Huawei Wireless Access Points Command Reference*.

Common Command Views

Name	How To Enter	Function
User view	When a user logs in to the device, the user enters the user view and the following prompt is displayed on the screen: `<Huawei>`	In the user view, you can view the running status and statistics of the device.

System view	Run the **system-view** command and press **Enter** in the user view. The system view is displayed.
	`<Huawei> system-view`
	`Enter system view, return user view with Ctrl+Z.`
	`[Huawei]`
		In the system view, you can set the system parameters of the device, and enter other function views from this view.

Name	How To Enter	Function

Interface view	Run the **interface** command and specify an interface type and number to enter an interface view.
	`[Huawei] interface gigabitethernet X/Y/Z`
	`[Huawei-GigabitEthernetX/Y/Z]`
	NOTE
	● *X/Y/Z* indicates the number of an interface that needs to be specified. It is in the format of slot number/sub card number/interface sequence number.
	● The interface GigabitEthernet is only an example.
		You can configure interface parameters in the interface view. The interface parameters include physical attributes, link layer protocols, and IP addresses.

WLAN view	Run the **wlan** command and press **Enter** in the system view. The WLAN view is displayed.
	`[Huawei] wlan`
	`[Huawei-wlan-view]`
		In the WLAN view, you can configure most WLAN parameters.

NOTE

- The command line prompt Huawei is the default host name (sysname). The prompt indicates the current view. For example, <> indicates the user view and [] indicates all other views except user view.
- Some commands can be executed in multiple views, but they have different functions after being executed in different views. For example, you can run the **lldp enable** command in the system view to enable LLDP globally and in the interface view to enable LLDP on an interface.
- In the system view, you can run the **diagnose** command to enter the diagnosis view. Diagnostic commands are used for device fault diagnosis. If you run some commands in the diagnosis view, the device may run improperly or services may be interrupted. Contact Huawei technical support personnel and use these diagnostic commands with caution.

Quitting Command Views

You can run the **quit** command to return from the current view to an upper-level view.

For example, return from the interface view to the system view and run the **quit** command to return to the user view.

```
[Huawei-GigabitEthernet0/0/1]
quit
[Huawei]quit
<Huawei>
```

To return from the interface view directly to the user view, press **Ctrl+Z** or run the **return** command.

Press **Ctrl+Z** to return directly to the user view.
```
[Huawei-GigabitEthernet0/0/1]           #Press Ctrl+Z.
<Huawei>
```

Run the **return** command to return directly to the user view.
```
[Huawei-GigabitEthernet0/0/1] return
<Huawei>
```

1.1.1.2 Setting Command Levels

The system divides commands into four levels and sets the command level in the specified view. The device administrator can change the command level as required, so that a lower-level user can use some high-level commands. The device administrator can also change the command level to a larger value to improve device security.

Context

- The system grants users different access permissions based on their roles. User levels are classified into sixteen levels, which correspond to the command levels. Users can use only the commands at the same or lower level than their own levels. By default, there are four command levels 0 to 3 and sixteen user levels 0 to 15. **Table 1-1** describes the relationship between command levels and user levels.

Table 1-1 Relationship between command levels and user levels

User Level	Command Level	Name	Description
0	0	Visit level	Commands of this level include network diagnosis tool commands (such as ping and tracert), and commands for accessing external devices from the local device (such as Telnet).
1	0, 1	Monitoring level	Commands of this level are used for system maintenance, including display commands. **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are at level 3. For details about command levels, see the *Huawei Wireless Access Points Command Reference*.
2	0, 1, 2	Configuration level	Commands of this level are used for service configuration to provide direct network services, including routing commands and commands of each network layer.
3 to 15	0, 1, 2, 3	Management level	Commands of this level are used for basic system operations, including file system, FTP, TFTP download, user management, command level configuration, and debugging.

NOTICE

Changing the default command level without the guidance of technical personnel is not recommended. This may result in inconvenience for operation and maintenance and bring about security problems.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
command-privilege level level view view-name command-key
```

The command level is set in the specified view.

----End

1.1.1.3 Editing Command Lines

This sections describes operating techniques for editing command lines.

Editing Feature

You can edit commands in a CLI that supports multi-line edition. Each command can contain a maximum of 510 characters. The keywords in the commands are case insensitive. Whether a command parameter is case sensitive or not depends on what the parameter is.

Table 1-2 lists keys that are frequently used for command editing.

Table 1-2 Keys for command editing

Key	Function
Common key	Inserts a character at the current location of the cursor if the editing buffer is not full, and the cursor moves to the right. Otherwise, an alarm is generated.
Backspace	Deletes the character on the left of the cursor and the cursor moves to the left. When the cursor reaches the head of the command, an alarm is generated.
Left cursor key ← or Ctrl +B	Moves the cursor to the left by the space of a character. When the cursor reaches the head of the command, an alarm is generated.

Key	Function
Right cursor key → or Ctrl +F	Moves the cursor to the right by the space of a character. When the cursor reaches the end of the command, an alarm is generated.

Operating Techniques

Incomplete Keyword

You can enter incomplete keywords on the device. In the current view, you do not need to enter complete keywords if the entered characters can match a unique keyword. This function improves operating efficiency.

For example, to execute the **display current-configuration** command, you can enter **d cu**, **di cu**, or **dis cu**, but you cannot enter **d c** or **dis c** because they do not match unique keywords.

NOTE

The maximum length of a command (including the incomplete command) to be entered is 510 characters. If a command in incomplete form is configured, the system saves the command to the configuration file in its complete form, which may cause the command to have more than 510 characters. In this case, the command in incomplete form cannot be restored after the system restarts. Therefore, when you configure a command in incomplete form, pay attention to the length of the command.

Tab

Enter an incomplete keyword and press Tab to complete the keyword.

- When a unique keyword matches the input, the system replaces the incomplete input with the unique keyword and displays it in a new line with the cursor leaving a space behind. For example:

  1. Enter an incomplete keyword.

     ```
     [Huawei] info-
     ```

  2. Press **Tab**.

     The system replaces the entered keyword and displays it in a new line with the complete keyword followed by a space.

     ```
     [Huawei] info-center
     ```

- When the input has multiple matches, press Tab repeatedly to display the keywords beginning with the incomplete input in a circle until the desired keyword is displayed. In this case, the cursor closely follows the end of the keyword. For example:

  1. Enter an incomplete keyword.

     ```
     [Huawei] info-center log
     ```

  2. Press **Tab**.

     The system displays the prefixes of all the matched keywords. In this example, the prefix is **log**.

     ```
     [Huawei] info-center logbuffer
     ```

     Press **Tab** to switch from one matched keyword to another. In this case, the cursor closely follows the end of a word.

     ```
     [Huawei] info-center logfile
     [Huawei] info-center loghost
     ```

     Stop pressing **Tab** when the desired keyword is displayed.

- When an incorrect keyword is entered, press Tab and it is displayed in a new line without being changed. For example:

  1. Enter an incorrect keyword.

     ```
     [Huawei] info-center loglog
     ```

  2. Press **Tab**.

     ```
     [Huawei] info-center loglog
     ```

     The system displays information in a new line, but the keyword **loglog** remains unchanged and there is no space between the cursor and the keyword, indicating that this keyword does not exist.

1.1.1.4 Using Command Line Online Help

When using a command line, you can use the online help to obtain real-time help without memorizing a large number of complex commands.

When entering command lines, you can enter a question mark (?) at any time to obtain online help. You can choose to obtain full help or partial help.

Full Help

When entering a command, you can use the full help function to obtain keywords and parameters for the command. Use any of the following methods to obtain full help from a command line.

- Enter a question mark (?) in any command view to obtain all the commands and their simple descriptions. For example:

  ```
  <Huawei> ?
  User view commands:
    autosave       <Group> autosave command group
    backup         Backup  information
    cd             Change current directory
    clear          Clear
    clock          Specify the system clock
    cls            Clear screen
    compare        Compare configuration file
    copy           Copy from one file to another
  ...
  ```

- Enter some keywords of a command and a question mark (?) separated by a space. All keywords associated with this command, as well as simple descriptions, are displayed. For example:

  ```
  <Huawei> system-view
  [Huawei] user-interface vty 0 4
  [Huawei-ui-vty0-4] authentication-mode ?
    aaa       AAA authentication
    password  Authentication through the password of a user terminal interface
  [Huawei-ui-vty0-4] authentication-mode aaa ?
    <cr>  Please press ENTER to execute command
  [Huawei-ui-vty0-4] authentication-mode aaa
  ```

  - "aaa" and "password" are keywords. "AAA authentication" and "Authentication through the password of a user terminal interface" describe the keywords respectively.
  - <cr> indicates that there is no keyword or parameter in this position. You can press Enter to run this command.

- Enter some keywords of a command and a question mark (?) separated by a space. All parameters associated with this keyword, as well as simple descriptions, are listed. For example:

```
<Huawei> system-view
[Huawei] ftp timeout ?
  INTEGER<1-35791>  The value of FTP timeout (in minutes)
[Huawei] ftp timeout 35 ?
  <cr>  Please press ENTER to execute command
[Huawei] ftp timeout 35
```

"INTEGER<1-35791>" describes the value range of the parameter. "The value of FTP timeout (in minutes)" briefly describes the function of this parameter.

Partial Help

If you enter only the first or first several characters of a command keyword, partial help provides keywords that begin with this character or character string. Use any of the following methods to obtain partial help from a command line.

- Enter a character string followed directly by a question mark (?) to display all keywords that begin with this character string. For example:

```
<Huawei> d?
  debugging  <Group> debugging command group
  delete     Delete a file
  dir        List files on a filesystem
  display    Display information
<Huawei>d
```

- Enter a command and a string followed directly by a question mark (?) to display all the keywords that begin with this string. For example:

```
<Huawei> display b?
  binding           Display binding relation of profile
  bridge            Bridge MAC
  bridge-link       Bridge link
  bridge-profile    Display Bridge profile
  bridge-whitelist  Bridge Whitelist
```

- Enter the first several letters of a keyword in a command and press **Tab** to display a complete keyword. The first several letters, however, must uniquely identify the keyword. If they do not identify a specific keyword, press **Tab** continuously to display different keywords and you can select one as required.

NOTE

The command output obtained through the online help function is used for reference only.

1.1.1.5 Interpreting Command Line Error Messages

If a command is entered and passes syntax check, the system executes it. Otherwise, the system reports an error message.

Table 1-3 lists the common error messages.

Table 1-3 Common error messages of the command line

Error Message	Cause of the Error
Error: Unrecognized command found at '^' position.	No command is found.
	No keyword is found.

Error Message	Cause of the Error
Error: Wrong parameter found at '^' position.	The parameter type is incorrect.
	The parameter value exceeds the limit.
Error: Incomplete command found at '^' position.	The entered command is incomplete.
Error: Too many parameters found at '^' position.	Too many parameters are entered.
Error: Ambiguous command found at '^' position.	Indefinite command is entered.

1.1.1.6 Using the undo Command Line

If a command line begins with the keyword **undo**, it is an **undo** command line. The **undo** command lines restore default settings of parameters, disable functions, or delete configurations. Almost each configuration command line has a corresponding **undo** command.

Some examples of using the undo command are listed as follows:

- The **undo** command restores the default setting.

  The **sysname** command sets a device host name. For example:

  ```
  <Huawei> system-view
  [Huawei] sysname Server
  [Server] undo sysname
  [Huawei]
  ```

- The **undo** command disables a specified function.

  The **ftp server enable** command enables the FTP server function on the device. For example:

  ```
  <Huawei> system-view
  [Huawei] ftp server enable
  Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
  Info: Succeeded in starting the FTP server
  [Huawei] undo ftp server
  Info: Succeeded in closing the FTP server.
  ```

- The **undo** command deletes a specified configuration.

  The **header** command configures the header information displayed on terminals when users log in. For example:

  ```
  <Huawei> system-view
  [Huawei] header login information "Hello,Welcome to Huawei!"
  ```

  Log out of the terminal and re-log in. A message "Hello, Welcome to Huawei!" is displayed before authentication. Run the **undo header login** command.

  ```
  Hello,Welcome to Huawei!

  Login
  authentication


  Username:huawei
  Password:
  ```

```
------------------------------------------------------------------------------

  User last login
information:

------------------------------------------------------------------------------
  Access Type:
Telnet
  IP-Address :
192.168.40.1
  Time       : 2013-04-07 16:50:02
+08:00

------------------------------------------------------------------------------
<Huawei> system-view
[Huawei] undo header login
```

Log out of the terminal and re-log in. No message is displayed before authentication.

```
Login
authentication


Username:huawei
Password:

------------------------------------------------------------------------------

  User last login
information:

------------------------------------------------------------------------------
  Access Type:
Telnet
  IP-Address :
172.168.254.204
  Time       : 2005-08-19 17:45:30
+08:00

------------------------------------------------------------------------------
<Huawei>
```

NOTE

The command output provided here is used for reference only. The actual output information may differ from the preceding information.

1.1.1.7 Displaying History Commands

The device automatically stores history commands entered by a user. If you need to enter a command that has been executed, you can use this function to call up the history command.

By default, the system saves 10 history commands for each user. Run the **history-command max-size** *size-value* command to reset the number of history commands that are allowed to be saved in a specified user interface view. The maximum number is 256.

NOTE

If the value is too large, it may take a long time to obtain a required history command. Therefore, a large value is not recommended.

Table 1-4 shows operations of history commands.

Table 1-4 Accessing history commands

Action	Command or Key	Result
Display history commands.	**display history-command**	Display history commands entered by the current user.
Display the earlier history command.	Up arrow key ↑ or Ctrl+P	If there is an earlier history command, the earlier history command is displayed. Otherwise, an alarm is generated.
Display the later history command.	Down arrow key ↓ or Ctrl+N	If there is a later history command, the later history command is displayed. Otherwise, the command is cleared and an alarm is generated.

NOTE

You cannot access history commands using the Up arrow key ↑ in HyperTerminal Windows 9X. The Up arrow key ↑ has a different function in Windows 9X and need to be replaced by the shortcut key Ctrl+P.

When using history commands, note the following:

- The saved history commands are the same as that those entered by users. For example, if the user enters an incomplete command, the saved command also is incomplete.
- If the user runs the same command several times, only the latest command is saved. If the command is entered in different forms, they are considered as different commands.

  For example, if the **display current-configuration** command is run several times, only one history command is saved. If the **display current-configuration** command and the **dis curr** command are used, both of them are saved.

1.1.1.8 Using Command Line Shortcut Keys

You can use shortcut keys provided by the device to quickly enter commands.

There are two types of shortcut keys:

- User-defined shortcut keys: include Ctrl+G, Ctrl+L, Ctrl+O, and Ctrl+U. You can associate these shortcut keys with any commands. When a shortcut key is pressed, the system runs the corresponding command.
- System-defined shortcut keys: shortcut keys defined in the system that have fixed functions. Users cannot define these shortcut keys. **Table 1-5** lists the frequently used system-defined shortcut keys.

NOTE

The terminal in use may affect the functions of the shortcut keys. For example, if the shortcut keys defined by the terminal conflict with those defined in the system, the shortcut keys entered by the user are captured by the terminal program and the commands corresponding to the shortcut keys are not executed.

User-defined Shortcut Keys

When a user frequently uses a command or some commands, the user can use shortcut keys to define these commands. Only management-level users and configuration-level users have the rights to define shortcut keys. The configurations are as follows:

1. Run the **system-view** command to enter the system view.
2. Run the **hotkey** { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_U** } *command-text* command to configure a shortcut key corresponding to a command.

The system supports four user-defined shortcut keys and the default values are as follows:

- Ctrl+G: **display current-configuration**
- Ctrl+L: **undo idle-timeout**
- Ctrl+O: **undo debugging all**
- Ctrl+U: Null

NOTE

- When defining shortcut keys, use double quotation marks to define the command if this command contains several keywords separated by spaces. For example, **hotkey ctrl_l "display tcp status"**. Do not use double quotation marks to define a command if the command contains only one keyword.
- Run the **display hotkey** command to view the status of the defined, undefined, and system-defined shortcut keys.
- Run the **undo hotkey** command to restore default values of the configured shortcut keys.
- Shortcut keys are executed in the same way as commands. The system can record commands in their original formats in the command buffer and logs to help query and locate the fault.
- The user-defined shortcut keys are available to all users. If a user does not have the rights to use the command defined by a shortcut key, the system displays an error message when this shortcut key is executed.

System-defined Shortcut Keys

Table 1-5 System-defined shortcut keys

Key	Function
Ctrl+A	Moves the cursor to the beginning of the current line.
Ctrl+B	Moves the cursor back one character.
Ctrl+C	Stops performing current functions.
Ctrl+D	Deletes the character where the cursor is located at.
Ctrl+E	Moves the cursor to the end of the last line.
Ctrl+F	Moves the cursor forward one character.
Ctrl+H	Deletes the character on the left side of the cursor.
Ctrl+N	Displays the next command in the history command buffer.

Key	Function
Ctrl+P	Displays the previous command in the history command buffer.
Ctrl+W	Deletes a character string on the left side of the cursor.
Ctrl+X	Deletes all the characters on the left side of the cursor.
Ctrl+Y	Deletes all the characters on the right side of the cursor and the character where the cursor is located at.
Ctrl+Z	Returns to the user view.
Ctrl+]	Stops incoming connections or redirects the connections.
Esc+B	Moves the cursor back one word.
Esc+D	Deletes one word on the right side of the cursor.
Esc+F	Moves the cursor forward one word.

1.1.2 Displaying the Command Output

This section describes how to query the configuration information about command lines, control the method in which command outputs are displayed, and filter the command outputs.

1.1.2.1 Displaying Command Line Configurations

After the configurations are complete, you can run the **display** command to check the configuration and running information on the device.

For example, after all configurations of the FTP service are complete, you can run the **display ftp-server** command to check parameters of the FTP server. For details on the usage and functions of the **display** command, see Checking the Configuration in each feature of the *Configuration Guide*.

You can also check the current running configurations and configurations in the current view.

- Check the current running configurations:

  display current-configuration

  The configurations that have been executed but are not valid are not displayed.

- Check configurations in the current view:

  display this

  A configuration parameter that uses the default value or does not take effect is not displayed.

1.1.2.2 Controlling the Display Mode of Commands

When running commands, you can specify the display mode.

- When the display output is more than one page, you can use **Pg Up** and **Pg Dn** to display information on the previous page and the next page.
- When the information cannot be completely displayed on one screen, the system will pause and you can view the information. You can use the function keys listed in **Table 1-6** to control the display mode of command lines.

  NOTE

  The **screen-length** *screen-length* **temporary** command sets the lines to be displayed temporarily on the terminal screen. If *screen-length* is 0, the split screen function is disabled. Therefore, the system will not pause when the information cannot be completely displayed on one screen.

Table 1-6 Display mode of commands

Key	Function
Ctrl+C or Ctrl+Z	Stops displaying information and running commands. **NOTE** You can also press any key (the number key or letter key) except space and Enter.
Space	Continues to display the next screen of information.
Enter	Continues to display the next line of information.

1.1.2.3 Filtering Command Outputs

When running the **display** command to check the command output, you can use the regular expression (specifying the rule to display) to filter the output information and locate needed information quickly.

Regular Expressions

A regular expression is a mode matching tool. It consists of common characters (such as letters from a to z) and special characters (called meta-characters). The regular expression is a template according to which you can search for the required string.

A regular expression provides the following functions:

- Searches for and obtains a sub-string that matches a rule in the string.
- Substitutes a string based on a certain matching rule.

The regular expression consists of common characters and special characters.

- Common characters

  Common characters are used to match themselves in a string, including all upper-case and lower-case letters, digits, punctuations, and special symbols. For example, a matches the

letter "a" in "abc", 202 matches the digit "202" in "202.113.25.155", and @ matches the symbol "@" in "xxx@xxx.com".

- Special characters

  Special characters are used together with common characters to match the complex or special string combination. **Table 1-7** describes special characters and their syntax.

Table 1-7 Description of special characters

Special Characters	Function	Example
\	Defines an escape character, which is used to mark the next character (common or special) as the common character.	* matches "*".
^	Matches the starting position of the string.	^10 matches "10.10.10.1" instead of "20.10.10.1".
$	Matches the ending position of the string.	1$ matches "10.10.10.1" instead of "10.10.10.2".
*	Matches the preceding element zero or more times.	10* matches "1", "10", "100", "1000", and so on. (10)* matches "null", "10", "1010", "101010", and so on.
+	Matches the preceding element one or more times.	10+ matches "10", "100", "1000", and so on. (10)+ matches "10", "1010", "101010", and so on.
?	Matches the preceding element zero or one time. **NOTE** Huawei datacom devices do not support regular expressions with ?. When regular expressions with ? are entered on Huawei datacom devices, helpful information is provided.	10? matches "1" or "10". (10)? matches "null" or "10".
.	Matches any single character.	0.0 matches "0x0", "020", and so on. .oo. matches "book", "look", "tool", and so on.
()	Defines a subexpression, which can be null. Both the expression and the subexpression should be matched.	100(200)+ matches "100200", "100200200", and so on.

Special Characters	Function	Example
x|y	Matches x or y.	100|200 matches "100" or "200". 1(2|3)4 matches "124" or "134", instead of "1234", "14", "1224", and "1334".
[xyz]	Matches any single character in the regular expression.	[123] matches the character 2 in "255".
[^xyz]	Matches any character that is not in the regular expression.	[^123] matches any character except for "1", "2", and "3".
[a-z]	Matches any character within the specified range.	[0-9] matches any character ranging from 0 to 9.
[^a-z]	Matches any character beyond the specified range.	[^0-9] matches all non-numeric characters.
_	Matches a comma ",", left brace "{", right brace "}", left parenthesis "(", and right parenthesis ")". Matches the starting position of the input string. Matches the ending position of the input string. Matches a space.	_2008_ matches "2008", "space 2008 space", "space 2008", "2008 space", ",2008,", "{2008}", "(2008)", "{2008)", and "(2008}".

NOTE

Unless otherwise specified, all the characters in the preceding table must be printable characters.

- Degeneration of special characters

  Certain special characters, when placed at certain positions in a regular expression, degenerate to common characters.

  - The special characters following "\" match special characters themselves.
  - The special characters "*", "+", and "?" are placed at the starting position of the regular expression. For example, +45 matches "+45" and abc(*def) matches "abc*def".
  - The special character "^" is placed at any position except for the start of the regular expression. For example, abc^ matches "abc^".
  - The special character "$" is placed at any position except for the end of the regular expression. For example, 12$2 matches "12$2".
  - A right parenthesis ")" or right bracket "]" is not paired with a corresponding left parenthesis "(" or bracket "[". For example, abc) matches "abc)" and 0-9] matches "0-9]".

NOTE

Unless otherwise specified, degeneration rules also apply when the preceding regular expressions are subexpressions within parentheses.

- Combination of common and special characters

  In actual usage, regular expressions combine multiple common and special characters to match certain strings.

Specifying a Filtering Mode in a Command

NOTE

- The device uses a regular expression to implement the pipe character filtering function. A display command supports the pipe character only when there is excessive output information.
- When filtering conditions are set to query output information, the first line of the command output starts with the entire regular expression but not the string to be filtered.

Some commands can carry the keyword **| count** to display the number of matching entries. The keyword **| count** can be used together with other keyword.

Three filtering modes are provided for commands that support regular expressions.

- **| begin** *regular-expression*: displays all the lines beginning with the line that matches the regular expression.

  Filter the character strings to be entered until the specified case-sensitive character string is displayed. All the character strings following this specified character string are displayed on the screen.

- **| exclude** *regular-expression*: displays all the lines that do not match the regular expression.

  If the character strings to be entered do not contain the specified case-sensitive character string, they are displayed on the screen. Otherwise, they are filtered.

- **| include** *regular-expression*: displays all the lines that match the regular expression.

  If the character strings to be entered contain the specified case-sensitive character string, they are displayed on the screen. Otherwise, they are filtered.

NOTE

The value of *regular-expression* is a string of 1 to 255 characters. *regular-expression* cannot contain underlines (_).

The following examples describe how to specify a filter mode in a command.

Example 1: Run the **display interface brief** command to display all the lines that do not match the regular expression GigabitEthernet|NULL|Wlan-Radio. GigabitEthernet|NULL|Wlan-Radio matches GigabitEthernet, NULL or Wlan-Radio.

```
<Huawei> display interface brief | exclude GigabitEthernet|NULL|Wlan-Radio
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(e): ETHOAM down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
Vlanif10                    down  down        --     --          0          0
Vlanif2001                  up    up          --     --          0          0
```

Example 2: Run the **display current-configuration** command to display all the lines that match the regular expression vlan.

```
<Huawei> display current-configuration | include vlan
vlan batch 10 2001
 port trunk allow-pass vlan 2001
```

NOTE

The preceding information is used for reference only.

1.1.3 Configuration Examples

This section provides several examples that illustrate the use of command lines.

1.1.3.1 Example for Using Tab

Networking Requirements

The user wants to enter commands in fast and convenient mode to facilitate completion of service configurations. The device supports the function that the user enters the first character or first several characters of the keyword and presses **Tab** to complete the keyword, which improves input efficiency.

Configuration Roadmap

The configuration roadmap is as follows:

1. If there is only one match for the incomplete keyword, enter the incomplete keyword and press **Tab**.
2. If there are several matches for the keyword, enter the incomplete keyword and press **Tab** repeatedly until the desired keyword is displayed.
3. Enter the incorrect keyword and press **Tab**. In this case, the incorrect keyword remains unchanged.

Use **Tab** if:

There Is Only One Match for an Incomplete Keyword

1. Enter an incomplete keyword.
   ```
   [Huawei] info-
   ```
2. Press **Tab**.

   The system replaces the entered keyword and displays it in a new line with the complete keyword followed by a space.
   ```
   [Huawei] info-center
   ```

There Are Several Matches for an Incomplete Keyword

The keyword **info-center** can be followed by the following keywords. (The command output provided here is used for reference only. The actual output information may differ from the following information.)

```
[Huawei] info-center ?
  channel             Set the name of information channel
  console             Setting of console configuration
  enable              Enable the infomation center
```

```
filter-id           Specify the configuration of the ID filtering table
logbuffer           Setting of log buffer configuration
logfile             <Group> logfile command group
loghost             Setting of logging host configuration
max-logfile-number  Setting of logfile numbers
monitor             Setting of monitor configuration
snmp                Setting of snmp configuration
source              Informational source setting
timestamp           Set the time stamp type of information
trapbuffer          Setting of trap buffer configuration
```

1. Enter an incomplete keyword.

   ```
   [Huawei] info-center log
   ```

2. Press **Tab**.

   The system displays the prefixes of all the matched keywords. In this example, the prefix is **log**.

   ```
   [Huawei] info-center logbuffer
   ```

   Press **Tab** to switch from one matched keyword to another. In this case, the cursor closely follows the end of a word.

   ```
   [Huawei] info-center logfile
   [Huawei] info-center loghost
   ```

   Stop pressing **Tab** when the desired keyword is displayed.

An Incorrect keyword Is Entered

1. Enter an incorrect keyword.

   ```
   [Huawei] info-center loglog
   ```

2. Press **Tab**.

   ```
   [Huawei] info-center loglog
   ```

   The system displays information in a new line, but the keyword **loglog** remains unchanged and there is no space between the cursor and the keyword, indicating that this keyword does not exist.

1.1.3.2 Example for Defining Shortcut Keys

This section provides an example for defining shortcut keys. In this example, the user defines the frequently used commands as shortcut keys to ease operations and improve efficiency.

Networking Requirements

The shortcut keys can be used on any device on the network. The user-defined shortcut keys are available to all users. If a user does not have the rights to use the command defined by a shortcut key, the system displays an error message when this shortcut key is executed.

Configuration Roadmap

The configuration roadmap is as follows:

1. Define the shortcut key **Ctrl+U** and associate it with the **display version** command.
2. Press **Ctrl+U** at the prompt of [Huawei] to run the **display version** command.

Procedure

Step 1 Define the shortcut key **Ctrl+U**, associate it with the **display version** command, and run the command.

```
<Huawei> system-view
[Huawei] hotkey ctrl_u "display version"
```

Step 2 Press **Ctrl+U** at the prompt of [Huawei] to run the **display version** command.

```
[Huawei] display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.130 (AP6010SN V200R003C00)
Copyright (C) 2011-2013 HUAWEI TECH CO., LTD
Huawei AP6010SN Router uptime is 0 week, 4 days, 0 hour, 35 minutes

MPU 0(Master) : uptime is 0 week, 4 days, 0 hour, 35 minutes
SDRAM Memory Size    : 128     M bytes
Flash Memory Size    : 32      M bytes
MPU version information :
1. PCB      Version  : H86D2TD1D200 VER.C
2. MAB      Version  : 0
3. Board    Type     : AP6010SN
4. BootROM  Version  : 54
```

----End

1.2 Logging In to the System for the First Time

This section describes how to log in to a new device to configure the device. You can log in through the console port.

1.2.1 Introduction

You can configure a device that is powered on for the first time by logging in through the console port.

The console port is a linear port on the device.

To configure a device, connect the user terminal serial port to the device console port.

1.2.2 Logging In Through a Console Port

After the device is powered on for the first time, you can log in to it from a PC through the console port to configure and manage the device.

Pre-configuration Tasks

Before logging in to the device through the console port, complete the following tasks:

- Preparing the console cable
- Installing the terminal emulation software on the PC

  NOTE

  You can use the built-in terminal emulation software (such as the HyperTerminal of Windows 2000/XP) on the PC. If no built-in terminal emulation software is available, use the third-party terminal emulation software. For details, see the software user guide or online help.

Configuration Procedure

Use the terminal emulation software to log in to the device through the console port, and complete basic configurations for the device.

Default Configuration

Table 1-8 Default configuration of the device console port

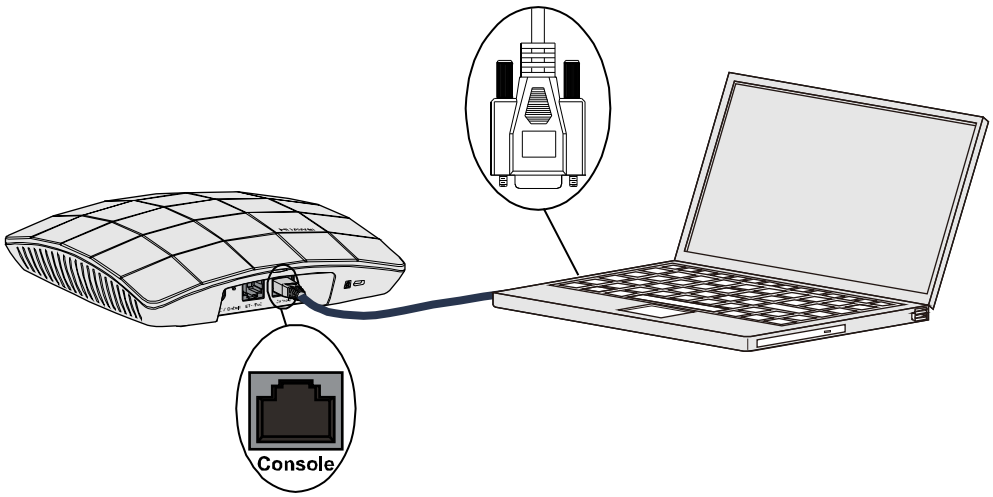
Parameter	Default Setting
Transmission rate	9600 bit/s
Flow control mode	None
Parity bit	None
Stop bit	1
Data bit	8

Procedure

Step 1 Use the terminal emulation software to log in to the device through the console port.

1. Insert the DB9 connector of the console cable delivered with the product to the 9-pin serial port on the PC, and insert the RJ45 connector to the console port of the device, as shown in **Figure 1-1**.

   Figure 1-1 Connecting to the device through the console port

2. Start the terminal simulation software on the PC. Establish a connection, and set the connected interface and communication parameters.

   NOTE

   A PC may have multiple connection interfaces; therefore, the interface connected through the console cable is selected in this example. Generally, COM1 is selected.

   If the serial port communication parameters of the device are modified, modify the communication parameters on the PC accordingly (ensure that the parameter values are the same) and re-establish the connection.

3. Press **Enter** until the following information is displayed. Enter the password and confirm password. (The following information is only for reference.)

```
Please configure the login password (maximum length 16)
Enter Password:
Confirm Password:
```

NOTE

- The password entered in interactive mode is not displayed on the screen.
- When you log in to the system again in password authentication mode, enter the password that is set during the initial login.

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

Step 2 Configure the device.

Set the time, date, name, and IP address for the device, and the user level and authentication mode for the Telnet user.

1. Set the time and date on the device.

Table 1-9 Actions for setting the time and date on the device

Action	Command	Description
Set the time zone.	**clock timezone** *time-zone-name* { **add** | **minus** } *offset*	● **add**: adds the specified time zone offset to the Coordinated Universal Time (UTC). That is, the sum of the default UTC time zone and *offset* is equal to the time zone specified by *time-zone-name*. ● **minus**: subtracts the specified time zone offset from the UTC. That is, the remainder obtained by subtracting *offset* from the default UTC time zone is equal to the time zone specified by *time-zone-name*.
Set the current time and date.	**clock datetime** *HH:MM:SS YYYY-MM-DD*	If the time zone is not set, the time set using this command is considered as the UTC time. Before setting the current time, you are advised to confirm the current zone and set the correct time zone offset.

Action	Command	Description
(Optional) Set the daylight saving time (DST).	**clock daylight-saving-time** *time-zone-name* **one-year** *start-time start-date end-time end-date offset* Or **clock daylight-saving-time** *time-zone-name* **repeating** *start-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *start-date1* } *end-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *end-date1* } *offset* [*start-year* [*end-year*]]	● By default, the DST is not configured. ● If you configure periodic DST, the combination of the DST start time and end time can be any of the following: date+date, day of the week+day of the week, date+day of the week, and day of the week+date. For the configuration method, see **clock daylight-saving-time**. **NOTE** When the DST is used, you can run the **clock timezone** *time-zone-name* { **add** | **minus** } *offset* command to set the time zone. The time zone in the output of the **display clock** command is, however, the name of the DST time zone. When the DST ends, the system displays the original time zone.

2. Set the device name and IP address.

   The IP address is used to log in to the device through Telnet.

Table 1-10 Actions for setting the device name and IP address

Action	Command	Description
Enter the system view.	**system-view**	-
Enable the Telnet service.	**system-view**	-
Set the device name.	**telnet server enable**	-
Enter the interface view.	**interface** *interface-type interface-number*	You can assign the IP address to the Layer 3 interface (such as the VLANIF interface).

Action	Command	Description
Assign the IP address to an interface.	**ip address** *ip-address* { *mask* | *mask-length* }	If a new IP address is assigned to an interface, the new IP address overrides the original one. **NOTE** Configure the IP address and routes according to the network plan to ensure that the routes between the terminal and device are reachable.

3. Configure the user level and authentication mode for the Telnet user.

Table 1-11 Actions for configuring the user level and authentication mode for the Telnet user

Action	Command	Description
Enter the system view.	**system-view**	-
Enter the VTY user interface view.	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
Set the Telnet user level.	**user privilege level** *level*	By default, users who log in through the VTY user interface can access commands at level 0.
Set the authentication mode for the Telnet user to AAA authentication.	**authentication-mode aaa**	By default, **password** authentication is used for console port login and **aaa** authentication is used for login on the VTY user interface. **NOTE** The system provides two authentication modes: AAA authentication and password authentication. AAA authentication requires both the user name and password, which is more secure than password authentication. This topic describes how to configure AAA authentication. For the configuration method of other authentication modes, see **Configuring the VTY User Interface**.
Enter the AAA view.	**aaa**	-

Action	Command	Description
Configure the user name and password for login through Telnet.	**local-user** *user-name* **password cipher** *password*	-
Set the login mode to Telnet.	**local-user** *user-name* **service-type telnet**	-

4. Save the configuration.

   After basic configuration is complete, you are advised to save the configuration. If the configuration information is lost, the connection and configuration for the first login must be performed again.

   Table 1-12 Actions for saving the configuration

Action	Command	Description
Return to the user view.	**return**	-
Save the configuration.	**save**	The current configuration has been saved in the configuration file. For detailed operations, see **1.6.2.1 Saving the Configuration File**.

Step 3 Check the configuration.

- Run the **display clock** command to check the current date and clock setting.
- Run the **display ip interface brief** [*interface-type* [*interface-number*]] command to check brief information about the IP address on the interface.
- Run the **display user-interface** [*ui-type ui-number1* | *ui-number*] [**summary**] command to check the physical attributes and configuration of the user interface.
- Run the **display local-user** command to check the local user list.

----End

1.2.3 Logging In to the Device Through Telnet

You can log in to the device through Telnet and configure the device.

Pre-configuration Tasks

Before logging in to the device through Telnet, complete the following tasks:

- Starting the device properly
- Preparing network cables used to connect device interfaces.

  NOTE

  Ensuring that the IP address 169.254.1.1 and subnet mask 255.255.0.0 have been configured on VLANIF 1 of the device before the delivery, and GE0/0/0 has been added to VLAN 1 by default.
- Configuring the PC's IP address and subnet mask. The IP address must be on the network segment 169.254.0.0/16 but cannot be 169.254.1.1. 169.254.1.100 is recommended. The subnet mask is 255.255.0.0.

NOTE

Before the device is delivered, the Telnet service has been configured on the device. The Telnet interface number is 23, and the default user name and password are respectively **admin** and **admin@huawei.com**.

Procedure

Step 1 Log in to the device from a PC through Telnet. A PC running Windows XP operating system is used as an example.

1. After the device is powered on, connect the PC's network interface to GE0/0/0 of the device using network cables.

   NOTE

   Ping 169.254.1.1 from the PC to check whether the device can be pinged successfully. If the ping operation fails, check whether the PC's IP address is correct or replace the network cable.
2. Choose **Start** > **All Programs** > **Accessories** > **Command Prompt** on the PC.
3. Run the **telnet 169.254.1.1** command to log in to the device through Telnet.
4. Enter the initial user name **admin** and password **admin@huawei.com**. When the following interface is displayed, login is successful. (The following information is only for reference.)

   ```
   Username:admin
   Password:
   <Huawei>
   ```

   NOTE

   It is recommended that you change the initial user name and password after login. For details, see **1.3 Configuring a User Interface**.

----End

1.2.4 Configuration Example

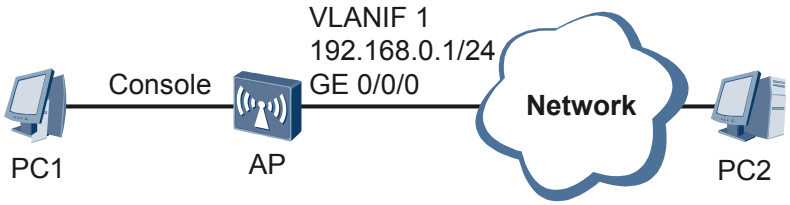
This section provides configuration examples for first login, including the examples for configuring the system time, system name, management IP address, and login using Telnet.

1.2.4.1 Example for Performing Basic Configurations After the First Device Login

Networking Requirements

After you log in to the device for the first time through the console port, perform basic device configurations, configure level 15 for users 0 to 4 who log in remotely through Telnet, and configure the AAA authentication mode for the users.

Figure 1-2 Networking diagram of performing basic configurations through the console port



Configuration Roadmap

1. Log in to the device through the console port.

   NOTE

   The HyperTerminal of Windows XP can be used as the terminal simulation software on the PC.

2. Perform basic device configurations.

Procedure

Step 1 Log in to the device from PC1 through the device's console port. For details, see **Logging In Through a Console Port**.

Step 2 Perform basic device configurations.

Set the system date, time, and time zone.

```
<Huawei> clock timezone BJ add 08:00:00
<Huawei> clock datetime 20:10:0 2012-07-26
```

Set the device name and management IP address. In this example, add GE0/0/0 to VLAN 1 and use VLANIF 1 as the device's management network port.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan 1
[AP-vlan1] quit
[AP] interface gigabitethernet 0/0/0
[AP-GigabitEthernet0/0/0] port link-type trunk
[AP-GigabitEthernet0/0/0] port trunk allow-pass vlan 1
[AP-GigabitEthernet0/0/0] port trunk pvid vlan 1
[AP-GigabitEthernet0/0/0] quit
[AP] interface vlanif 1
[AP-Vlanif1] ip address 192.168.0.1 255.255.255.0
[AP-Vlanif1] quit
```

Set the level and authentication mode for the Telnet users.

```
[AP] user-interface vty 0 4
[AP-ui-vty0-4] user privilege level 15
[AP-ui-vty0-4] authentication-mode aaa
[AP-ui-vty0-4] quit
[AP] aaa
[AP-aaa] local-user huawei password cipher admin@huawei
[AP-aaa] local-user huawei privilege level 15
[AP-aaa] local-user huawei service-type telnet
[AP-aaa] quit
```

Step 3 Verify the configuration.

After the configuration is complete, you can remotely log in to the device through Telnet from PC2.

NOTE

Ensure that there are reachable routes between the device and PC2 are reachable.

```
C:\Documents and Settings\Administrator> telnet 192.168.0.1
```

Press **Enter**, and enter the user name and password in the login window. If the authentication is successful, the command line prompt of the user view is displayed. (The following information is only for reference.)

```
Username:huawei
Password:
<AP>
```

----End

Configuration File

Configuration file of the device

```
#
 sysname AP
#
 clock timezone BJ add 08:00:00
#
aaa
 local-user huawei password cipher %$%$~^Mg.QBcGS^}H.Q*w~#*,JA8%$%$
 local-user huawei privilege level 15
 local-user huawei service-type telnet
#
interface Vlanif1
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/0/0
 port link-type trunk
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```

1.3 Configuring a User Interface

When a user logs in to the device using the console port, Telnet, or SSH, the system manages the session between the user and the device on the corresponding user interface.

1.3.1 User Interface Overview

The system supports the console and VTY user interfaces.

Each user interface maps a user interface view. In the user interface view that is a command-line interface (CLI), you can configure and manage all physical and logical interfaces that work in asynchronous and interactive modes to manage different user interfaces.

User Interfaces Supported by the Device

- Console (CON)

  The console port is a serial port provided by the main control board of a device.

  Each main control board provides one console port that conforms to the EIA/TIA-232 standard. The console port is a Data Connection Equipment (DCE) port. The serial port of a user terminal can directly connect to the console port of the device to access the device.

- VTY

  The Virtual Type Terminal (VTY) manages and monitors users who log in to the device using VTY user interfaces

  When a user's terminal connects to the device using Telnet or Secure Shell (SSH), a VTY is set up. A maximum of 15 users can log in to the device using VTY interfaces at the same time.

Relationship Between a User and a User Interface

A user interface is not devoted exclusively to a specific user. User interfaces are used to manage and monitor users that have logged in to the system using a certain method. Although a user interface can be used only by one user at a time, a user interface is not specific to a fixed user.

When a user logs in to the device, the system assigns an available user interface with the smallest number to the user. The login process depends on the configuration of the user interface. For example, when user A logs in to the device using the console port, the login process depends on the configuration in the console user interface view. If a user logs in to the device in different modes, the user interface assigned to the user is different. If a user logs in to the device at different time, the user interface assigned to the user may be different.

User Interface Number

When a user logs in to the device, the system assigns an available user interface with the smallest number to the user. User interfaces can be numbered in either of the following ways:

- Relative numbering

  The format of relative numbering is: user interface type + number.

  Relative numbering uniquely specifies a user interface of the same type. Relative numbering must comply with the following rules:

  - Number of the CON port: CON 0
  - Number of the VTY: The first VTY is 0, the second VTY is 1, and so on

- Absolute numbering

  Absolute numbering uniquely specifies a user interface or a group of user interfaces. You can run the **display user-interface** command to view user interfaces and their absolute numbers supported by the current device.

  There is only one console port on a main control board. 15 VTY user interfaces are provided. You can use the **user-interface maximum-vty** command in the system to set the maximum number of user interfaces. By default, the maximum number of user interfaces is 5.

  Table 1-13 describes the default absolute numbering of the console user interface and VTY user interface.

Table 1-13 Absolute and relative numbers of user interfaces

User Interface	Description	Absolute Number	Relative Number
Console user interface	Manages and controls users that log in to the device using the console interface.	0	0
VTY user interface	Manages and controls users that log in to the device using Telnet or SSH.	5 to 19	The first interface is VTY 0, the second is VTY 1, and so forth. By default, VTY 0 to VTY 4 are available. Absolute numbers 5 to 19 map relative numbers VTY 0 to VTY 14.

User Authentication Modes on a User Interface

After a user authentication mode is configured, the device authenticates users who want to log in.

Two authentication modes are available:

- Password authentication: A user is authenticated only by password.
- AAA authentication: A user is authenticated by user name and password. Telnet users usually use AAA authentication.

User Levels on User Interfaces

Users log in to the device are managed based on the user levels. The level of commands that a user can use depends on the level of the user.

- In the password authentication mode, the level of commands that the user can run depends on the level of the user interface.
- In the AAA authentication mode, the level of commands that the user can run depends on the level of the local user specified in AAA configuration.

1.3.2 Configuring the Console User Interface

Before logging in to the device using the console user interface to maintain the device locally, a user can configure the attributes of the user interface to ensure device security.

Pre-configuration Tasks

Before configuring a console user interface, complete the following tasks:

- Logging in to the device using a terminal

NOTE

To log in to the device through the console interface to maintain the device locally, configure the console user interface including the physical attributes, terminal attributes, user level, and user authentication mode. Users can set these parameters based on the site requirements or retain the default values.

Procedure

You can perform the configuration operations in any sequence.

1.3.2.1 Configuring the Physical Attributes of the Console User Interface

Context

The physical attributes of the console user interface include the transmission rate, flow control mode, parity bit, stop bit, and data bit of the console interface. To log in to the device using the console interface, ensure that the attributes of the HyperTerminal are consistent with the physical attributes of the device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface console interface-number
```

The console user interface view is displayed.

Step 3 Run:

```
speed speed-value
```

The transmission rate is set.

By default, the transmission rate is 9600 bit/s.

Step 4 Run:

```
parity { even | none | odd }
```

The parity bit is set.

By default, the parity bit is None.

Step 5 Run:

```
stopbits { 1.5 | 1 | 2 }
```

The stop bit is set.

By default, the stop bit is 1.

Step 6 Run:

```
databits { 5 | 6 | 7 | 8 }
```

The data bit is set.

By default, the data bit is 8.

----End

1.3.2.2 Configuring Terminal Attributes on the Console User Interface

Context

Users can configure terminal attributes including the timeout disconnection function, number of lines on the terminal screen, and size of the history command buffer on the console user interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface console interface-number
```

The console user interface view is displayed.

Step 3 Run:

```
idle-timeout minutes [ seconds ]
```

The timeout disconnection function is set.

If no operation is performed on the device before the end of the timeout period, the terminal disconnects from the device automatically.

By default, the timeout duration is 5 minutes.

Step 4 Run:

```
screen-length screen-length [ temporary ]
```

The number of lines displayed on the terminal screen is set.

The **temporary** parameter specifies the temporary number of lines displayed on the terminal screen.

The default number of lines displayed on the terminal screen is 24.

NOTE

The system automatically adjusts the number of terminal screen lines.

Step 5 Run:

```
history-command max-size size-value
```

The history command buffer is set.

By default, the history command buffer can store up to 10 commands.

----End

1.3.2.3 Configuring the User Level on the Console User Interface

Context

- Users can be configured with different user levels to control the device access permission, improving device security.
- There are 16 user levels numbered from 0 to 15, in ascending order of priorities.
- User levels map command levels. A user can only run commands at the same or lower level.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface console interface-number
```

The console user interface view is displayed.

Step 3 Run:

```
user privilege level level
```

The user level is set.

Table 1-14 describes the mapping between user levels and command levels.

Table 1-14 Mapping between user levels and command levels

User Level	Command Level	Permission	Description
0	0	Visit	Commands at this level are network diagnosis commands, such as ping and tracert commands, and commands used to access remote devices such as Telnet clients.
1	0 and 1	Monitoring	Commands at this level are system maintenance commands such as display commands. **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are at level 3. For details about command levels, see the *Huawei Wireless Access Points Command Reference*.
2	0, 1, and 2	Configuration	Commands at this level are used for service configuration. These commands include routing commands and commands at each network layer to provide network services to users.

User Level	Command Level	Permission	Description
3-15	0, 1, 2, and 3	Management	Commands at these levels are system basic operation commands that support services, including file system, FTP, TFTP, user management commands, command level configuration commands, and debugging commands.

NOTE

- By default, users that log in to the device using the console interface can run commands at level 15.
- If the command access level configured in the user interface view and user priority are inconsistent, user priority takes precedence.

----End

1.3.2.4 Configuring the User Authentication Mode on the Console User Interface

Context

The system provides AAA and password authentication modes to ensure device security.

Procedure

- Configuring AAA authentication
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     user-interface console *interface-number*

     The console user interface view is displayed.
  3. Run:
     authentication-mode aaa

     The user authentication mode is set to AAA.
  4. Run:
     quit

     Exit from the console user interface view.
  5. Run:
     aaa

     The AAA view is displayed.
  6. Run:
     local-user *user-name* **password cipher** *password*

The local user name and password are configured.

7. Run:
   local-user *user-name* **service-type terminal**

   The service type of the local user is set to terminal.
8. Run:
   quit

   The user quit the AAA view.

- Configuring password authentication
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     user-interface console *interface-number*

     The console user interface view is displayed.
  3. Run:
     authentication-mode password

     The user authentication mode is set to password.
  4. Run:
     set authentication password cipher

     The authentication password is configured. You can enter a password in cipher text.

----End

1.3.2.5 Checking the Configurations

Context

After configurations for the console user interface are complete, run the commands to check the configurations.

Procedure

- Run the **display users** [**all**] command to view user information for the user interface.
- Run the **display user-interface console** *ui-number* [**summary**] command to view the information about the user interface.
- Run the **display local-user** command to view the local user list.
- Run the **display access-user** command to view online users.

----End

1.3.3 Configuring the VTY User Interface

Before logging in to the device using Telnet or SSH to maintain the device locally or remotely, a user can configure a VTY user interface to ensure device security.

Pre-configuration Tasks

Before configuring a VTY user interface, complete the following tasks:

- Log in to the device using a terminal.

NOTE

Parameters have default values with the exception of the ACL number that restricts the call-in and call-out permissions on the VTY interface, authentication mode on the user interface, and user name and password. You can set parameters based on the site requirements.

Procedure

You can perform the configuration operations in any sequence.

1.3.3.1 Configuring the Maximum Number of Concurrent VTY User Interfaces

Context

Users can configure the maximum number of concurrent VTY user interfaces to control the number of users who log in to the device at the same time. The number of VTY user interfaces equals the total number of Telnet and SSH users.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface maximum-vty number
```

The maximum number of VTY user interfaces is set.

By default, the maximum number of VTY user interfaces is 5.

NOTICE

When the maximum number of VTY user interfaces is set to 0, no user (including the NMS user) can log in to the device using the VTY interface.

If you set the maximum number of the VTY user interfaces to a value smaller than the number of current online users, the system displays a configuration failure message.

After increasing the number of VTY user interfaces, you must configure the authentication mode for new VTY users.

----End

1.3.3.2 (Optional) Configuring Restrictions on ACL-based Logins on the VTY User Interface

Context

You can use the ACL to restrict login permissions on the VTY user interface. Before configuring restrictions on login permissions on the VTY user interface, run the **acl** command in the system view to create an ACL and enter the ACL view, and run the **rule** command to add rules for accessing the ACL.

NOTE

- The user interface supports basic ACLs (2000-2999) and advanced ACLs (3000-3999).
- ACL rule:
  - When **permit** is used in the ACL rule:
    - If the ACL is applied in the inbound direction, other devices that match the ACL rule can access the local device.
    - If the ACL is applied in the outbound direction, the local device can access other devices that match the ACL rule.
  - When **deny** is used in the ACL rule:
    - If the ACL is applied in the inbound direction, other devices that match the ACL rule cannot access the local device.
    - If the ACL is applied in the outbound direction, the local device cannot access other devices that match the ACL rule.
  - When the ACL rule is configured but packets from other devices do not match the rule:
    - If the ACL is applied in the inbound direction, other devices cannot access the local device.
    - If the ACL is applied in the outbound direction, the local device cannot access other devices.
  - When the ACL contains no rule:
    - If the ACL is applied in the inbound direction, any other devices can access the local device.
    - If the ACL is applied in the outbound direction, the local device can access any other devices.
- For details on how to configure the ACL, see "ACL Configuration" in the *Huawei Wireless Access Points Configuration Guide - Security*.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface vty first-ui-number [ last-ui-number ]
```

The VTY user interface view is displayed.

Step 3 Run:

```
acl acl-number { inbound | outbound }
```

ACL restrictions on VTY login permissions are configured.

- To restrict users at a specified address or address segment from logging in to the device, use the **inbound** parameter.

- To restrict users who have log in to a device from logging in to other devices, use the **outbound** parameter.

----End

1.3.3.3 Configuring Terminal Attributes on the VTY User Interface

Context

Users can configure terminal attributes on the VTY user interface. These attributes include the timeout disconnection function, number of lines on the terminal screen, and size of the history command buffer.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface vty first-ui-number [ last-ui-number ]
```

The VTY user interface view is displayed.

Step 3 Run:

```
shell
```

The VTY terminal service is enabled.

By default, all VTY terminal services are enabled.

Step 4 Run:

```
idle-timeout minutes [ seconds ]
```

The timeout disconnection function is set.

If no operation is performed on the device before the end of the timeout period, the terminal disconnects from the device automatically.

By default, the timeout duration is 5 minutes.

Step 5 Run:

```
screen-length screen-length [ temporary ]
```

The number of lines displayed on the terminal screen is set.

The **temporary** parameter specifies the temporary number of lines displayed on the terminal screen.

The default number of lines displayed on the terminal screen is 24.

Step 6 Run:

```
history-command max-size size-value
```

The history command buffer is set.

By default, the history command buffer can store up to 10 commands.

----End

1.3.3.4 Configuring the User Level on the VTY User Interface

Context

- Users can be configured with different user levels to control the device access permission, improving device security.
- There are 16 user levels numbered from 0 to 15, in ascending order of priorities.
- User levels map command levels. A user can only run commands at the same or lower level.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
user-interface vty first-ui-number [ last-ui-number ]
```

The VTY user interface view is displayed.

Step 3 Run:

```
user privilege level level
```

The user level is set.

Table 1-15 describes the mapping between user levels and command levels.

Table 1-15 Mapping between user levels and command levels

User Level	Command Level	Permission	Description
0	0	Visit	Commands at this level are network diagnosis commands, such as ping and tracert commands, and commands used to access remote devices such as Telnet clients.
1	0 and 1	Monitoring	Commands at this level are system maintenance commands such as display commands. **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are at level 3. For details about command levels, see the *Huawei Wireless Access Points Command Reference*.
2	0, 1, and 2	Configuration	Commands at this level are used for service configuration. These commands include routing commands and commands at each network layer to provide network services to users.

User Level	Command Level	Permission	Description
3-15	0, 1, 2, and 3	Management	Commands at these levels are system basic operation commands that support services, including file system, FTP, TFTP, user management commands, command level configuration commands, and debugging commands.

NOTE

- By default, users that log in to the device using the VTY interface can run commands at level 0.
- If the command access level configured in the user interface view and user priority are inconsistent, user priority takes precedence.

----End

1.3.3.5 Configuring the Authentication Mode for VTY Users

Context

The system provides AAA and password authentication modes to ensure device security.

Procedure

- Configuring AAA authentication
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     user-interface vty *first-ui-number* [*last-ui-number*]

     The VTY user interface view is displayed.
  3. Run:
     authentication-mode aaa

     The user authentication mode is set to AAA.
  4. Run:
     quit

     The user quits the VTY user interface view.
  5. Run:
     aaa

     The AAA view is displayed.
  6. Run:
     local-user *user-name* **password cipher** *password*

The local user name and password are configured.

7. Run:
   local-user *user-name* **service-type** { **telnet** | **ssh** }

   The service type of the local user is set to Telnet or SSH.
8. Run:
   quit

   Exit from the AAA view.

- Configuring password authentication
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     user-interface vty *first-ui-number* [*last-ui-number*]

     The VTY user interface view is displayed.
  3. Run:
     authentication-mode password

     The user authentication mode is set to password.
  4. Run:
     set authentication password cipher

     The authentication password is configured. You can enter a password in cipher text.

----End

1.3.3.6 Checking the Configurations

Context

After configurations for the VTY user interface are complete, run the commands to check the configurations.

Procedure

- Run the **display users** [**all**] command to view user information for the user interface.
- Run the **display user-interface maximum-vty** command to view the maximum number of VTY user interfaces.
- Run the **display user-interface vty** *ui-number1* [**summary**] command to view the information about the user interface.
- Run the **display local-user** command to view the local user list.
- Run the **display vty mode** command to view the VTY mode.

----End

1.3.4 Configuration Examples

This section describes configuration examples for user interfaces, including networking requirements, configuration notes, and configuration roadmap.

1.3.4.1 Example of Configuring the Console User Interface

Networking Requirements

Before logging in to the device using the console user interface to maintain the device locally, a user can configure the attributes of the console user interface to ensure device security.

In this example, the level of console users is 15. The password authentication mode and authentication password **Helloworld@6789** are configured for console users to log in to the device.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the user level on the console user interface.
2. Configure the authentication mode and password on the console user interface.

Procedure

Step 1 Configure the user level on the console user interface.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] user privilege level 15
```

Step 2 Configure the authentication mode and password on the console user interface.

```
[Huawei-ui-console0] authentication-mode password
[Huawei-ui-console0] set authentication password cipher
Enter Password(<6-16>):
Confirm Password:
[Huawei-ui-console0] quit
```

After the console user interface is configured, users can use the console interface to log in to the device in the password authentication mode to maintain the device locally. For details on how to log in to the device see **1.4.2.1 Logging In to the Device Through a Console Port**.

Step 3 Verify the configuration.

Run the **quit** command to disconnect the terminal from the device, connect the terminal to the device using a console cable, and verify that the new password is valid.

Run the **user-interface console 0** command to enter the console interface view, and run the **display this** command to check the configurations on the console interface.

```
[Huawei] user-interface console 0
[Huawei-ui-console0] display this
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %$%${>.zP!{s/X}>7M)7d7"/,.py}
xZ53^vDK'v5sN55>=zJ.p|,%$%$
#
return
```

----End

Configuration File

```
#
user-interface con 0
```

```
 authentication-mode password
 set authentication password cipher %$%${>.zP!{s/X}>7M)7d7"/,.py}
xZ53^vDK'v5sN55>=zJ.p|,%$%$
#
return
```

1.3.4.2 Example of Configuring a VTY User Interface

Networking Requirements

A user can use the VTY interface to log in to a remote device using Telnet. The device administrator can configure the attributes of the VTY user interface to ensure device security.

In this example, the level of VTY users is 2. The password authentication mode and authentication password **Helloworld@6789** are configured for VTY users to log in to the device. Only the user whose IP address is 10.1.1.1 can log in to the device.

If a user logs in to the device and does not perform an operation within 30 minutes, the user's terminal disconnects from the device.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the maximum number of concurrent VTY user interfaces to 8.
2. Configure restrictions on call-in and call-out permissions on the VTY user interface to allow users at a specified address or address segment to log in to the device.
3. Configure terminal attributes on the VTY user interface.
4. Configure the user level on the VTY user interface.
5. Configure the authentication mode and password of the VTY user interface.

Procedure

Step 1 Configure the maximum number of concurrent VTY user interfaces.

```
<Huawei> system-view
[Huawei] user-interface maximum-vty 8
```

Step 2 Configure restrictions on call-in and call-out permissions on the VTY user interface.

```
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule deny source 10.1.1.1 0
[Huawei-acl-basic-2000] rule permit source any
[Huawei-acl-basic-2000] quit
[Huawei] user-interface vty 0 7
[Huawei-ui-vty0-7] acl 2000 inbound
```

Step 3 Configure terminal attributes on the VTY user interface.

```
[Huawei-ui-vty0-7] shell
[Huawei-ui-vty0-7] idle-timeout 30
[Huawei-ui-vty0-7] screen-length 30
[Huawei-ui-vty0-7] history-command max-size 20
```

Step 4 Configure the user level on the VTY user interface.

```
[Huawei-ui-vty0-7] user privilege level 2
```

Step 5 Configure the authentication mode and password of the VTY user interface.

```
[Huawei-ui-vty0-7] authentication-mode password
```

```
[Huawei-ui-vty0-7] set authentication password cipher
Enter Password(<6-16>):
Confirm Password:
[Huawei-ui-vty0-7] quit
```

After the VTY user interface is configured, users can log in to the device in the password authentication mode using Telnet to maintain the device locally or remotely. For details on how to log in to the device see **1.4.2.2 Logging In to the Device Through Telnet**.

Step 6 Verify the configuration.

Connect the terminal to the device using Telnet, and verify that the new password is valid.

Use 10.1.1.1 to log in to the device using Telnet. The login fails.

Run the **user-interface vty 0 7** command to enter the VTY interface view, and run the **display this** command to check the configurations on the VTY interface.

```
[Huawei] user-interface vty 0 7
[Huawei-ui-vty0-7] display this
#
user-interface maximum-vty 8
user-interface vty 0 7
 acl 2000 inbound
 authentication-mode password
 user privilege level 2
 set authentication password cipher %%$%$RdF~Z+6N|0d^a3%v5`W~3.%ymjpAD#$u
[T'e#e32hd8G~4+&%$%$
 history-command max-size 20
 idle-timeout 30 0
 screen-length 30
#
return
```

----End

Configuration File

```
#
acl number 2000
 rule 5 deny source 10.1.1.1 0
 rule 10 permit
#
user-interface maximum-vty 8
user-interface vty 0 7
 acl 2000 inbound
 authentication-mode password
 user privilege level 2
 set authentication password cipher %%$%$RdF~Z+6N|0d^a3%v5`W~3.%ymjpAD#$u
[T'e#e32hd8G~4+&%$%$
 history-command max-size 20
 idle-timeout 30 0
 screen-length 30
#
return
```

1.4 Configuring User Login

Users can log in to the device through a console port, Telnet, STelnet to perform local or remote device maintenance.

1.4.1 User Login Overview

When the device works as the server, a user can log in to the device through a console port, Telnet, or STelnet. When the device works as the client, the user can log in to other devices from the client through Telnet or STelnet.

To manage and maintain devices locally or remotely, a user needs to configure the user interface, user management information, and terminal services before login.

- User interface: provides the login entry.
- User management information: ensures login security.
- Terminal services: support login protocols such as Telnet and Secure Shell Telnet (STelnet).

A user can log in to the device in one of the modes describes in **Table 1-16** to configure and manage the device.

Table 1-16 User login modes

Login Mode	Advantage	Disadvantage	Usage Scenario	Description
Logging In Through the Console Port	A dedicated Console cable is used to connect terminals and the device to ensure effective control on the device.	Devices cannot be remotely logged in and maintained.	• The device is configured for the first time. • A user cannot remotely log in to the device. • The device cannot be started. The user can access the uBoot menu through the console port for diagnosis or system upgrade.	By default, you can log in to the device through the console port to configure parameters for console port login. The Telnet service is enabled on the device before delivery. You can use the default IP address to log in to the device through Telnet and configure parameters for console port login. **NOTE** For details on first login using the default IP address in telnet mode or through the console port, see **1.2 Logging In to the System for the First Time**.

Login Mode	Advantage	Disadvantage	Usage Scenario	Description
Logging In Through Telnet	Devices can be managed and maintained locally or remotely. Each device does not need to be connected to a terminal, which facilitates user operations.	The TCP protocol is used to transmit data in plain text, which brings security threats.	A user connects a terminal to the network, logs in to the device through Telnet, and performs local or remote configuration. This cannot apply to the network required for high security.	By default, the Telnet service is enabled on the device. You can use the default IP address to log in to the device through Telnet and configure Telnet login parameters. You can also log in to the device through the console port to configure Telnet login parameters. **NOTE** For details on first login using the default IP address in telnet mode or through the console port, see **1.2 Logging In to the System for the First Time**.
Logging In Through STelnet	The STelnet protocol implements secure remote logins on insecure networks, which ensures data integrity and reliability and guarantees secure data transmission.	Configurations are complicated.	If the network has a high security requirement, a user can log in to the device through STelnet. STelnet based on the Secure Shell (SSH) protocol provides information security and authentication, which protects devices against attacks such as IP address spoofing.	By default, you cannot log in to the device directly through STelnet. To log in to the device through STelnet, log in to the device through the console port or remotely through Telnet and configure STelnet login parameters. **NOTE** For details on first login using the default IP address in telnet mode or through the console port, see **1.2 Logging In to the System for the First Time**.

Console Port

A main control board provides one console port that conforms to the EIA/TIA-232 standard. The console port is a Data Connection Equipment (DCE) port. The serial port on a user terminal is directly connected to the console port on the device for login.

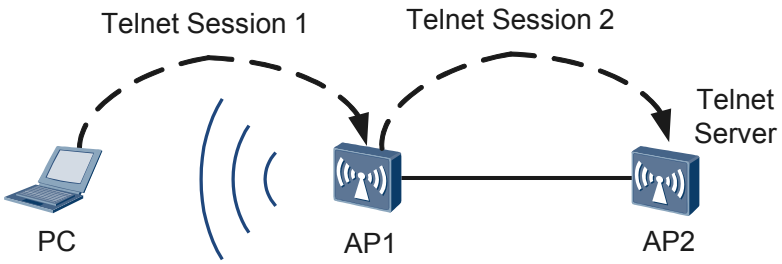
Telnet

In the TCP/IP protocol suite, the Telnet protocol is applied to the application layer. The Telnet protocol provides remote login and virtual terminal functions through networks. The server/

client mode is used. The Telnet client sends a request to the Telnet server, which then provides the Telnet service. The device supports the Telnet client and server functions.

As shown in **Figure 1-3**, AP1 works as the Telnet server and provides the Telnet client service, and AP2 provides the Telnet server functions for AP1.

Figure 1-3 Diagram of the client/server mode adopted by Telnet



STelnet

Telnet uses the TCP protocol to transmit plain text, which does not have a secure authentication mode and is vulnerable to Denial of Service (DoS), IP address spoofing, and route spoofing attacks.

Through STelnet based on SSH, the client and server establish a secure connection through negotiation, and the client can then log in to the server. SSH provides secure remote access on an insecure network by supporting the following functions:

- Revest-Shamir-Adleman Algorithm (RSA) authentication: A key pair consisting of the public and private keys needs to be created on the client, and the public key is sent to the server to which the client will log in. The server compares the client public key carried in the packet with the locally configured client public key. If the two public keys are inconsistent, the server disconnects from the client. If they are consistent, the client continues using the private key in the local key pair to perform digest algorithm, and sends the result (digital signature) to the server. The server uses the preconfigured client public key to authenticate the digital signature.
- Data Encryption Standard (DES), 3DES, and AES128: AES is Advanced Encryption Standard. User names, passwords, and transmitted data can be encrypted.

  NOTE

  The AES128 algorithm is recommended to improve data transmission security.

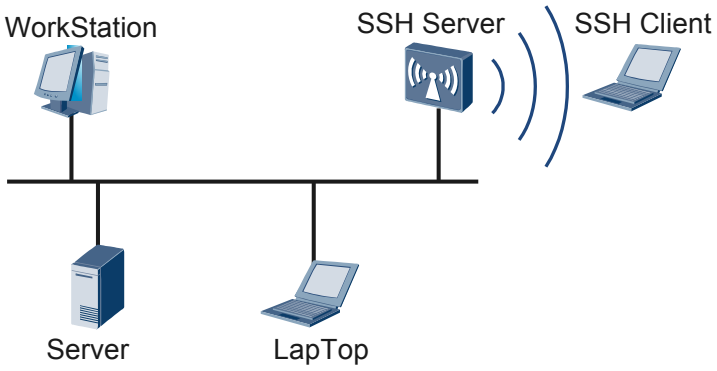
The device supports the SSH server functions and can connect to multiple SSH clients. The device also supports the SSH client functions and allows users to establish SSH connections to the SSH server and remotely log in to the server. When working as the SSH server, the device supports SSH2.0 and SSH1.0. When working as the SSH client, the device only supports SSH2.0.

SSH supports local connections and WAN connections.

- Local connection

  As shown in **Figure 1-4**, an SSH channel can be established between the SSH client and server for local connections.

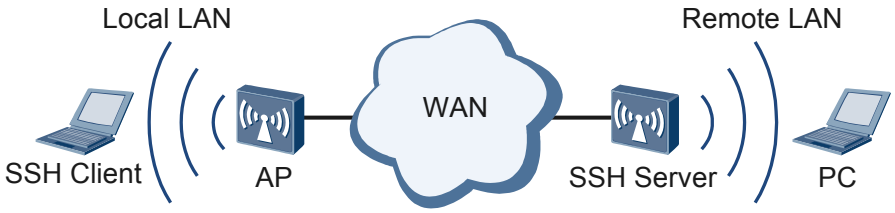
Figure 1-4 Establishing an SSH channel on a LAN



- WAN connection

  As shown in **Figure 1-5**, an SSH channel can be established between the SSH client and server for WAN connections.

Figure 1-5 Establishing an SSH channel on a WAN



1.4.2 Logging In to the Device

A user can log in to the device through a console port, Telnet, or STelnet. After login, the user can perform common operations to manage and maintain the device.

1.4.2.1 Logging In to the Device Through a Console Port

Pre-configuration Tasks

Before logging in to the device through a console port, complete the following tasks:

- Preparing the console cable
- Installing the terminal emulation software on the PC

  NOTE

  You can use the built-in terminal emulation software (such as the HyperTerminal of Windows 2000/XP) on the PC. If no built-in terminal emulation software is available, use the third-party terminal emulation software. For details, see the software user guide or online help.

Default Configuration

Table 1-17 Default configuration of the device console port

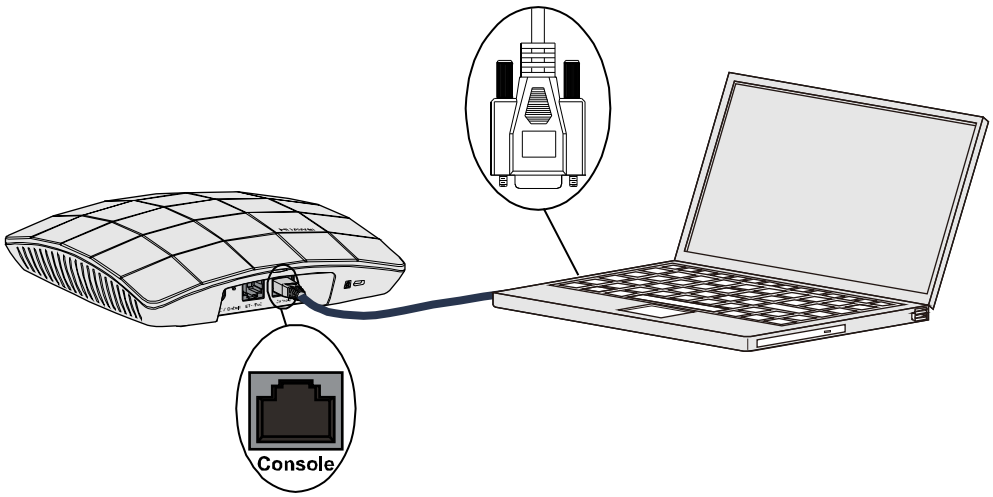
Parameter	Default Setting
Transmission rate	9600 bit/s
Flow control mode	None
Parity bit	None
Stop bit	1
Data bit	8

Procedure

Step 1 Use the terminal simulation software to log in to the device through a console port.

1. Insert the DB9 connector of the console cable delivered with the product to the 9-pin serial port on the PC, and insert the RJ45 connector to the console port of the device, as shown in **Figure 1-6**.

   Figure 1-6 Connecting to the device through the console port

2. Start the terminal simulation software on the PC. Establish a connection, and set the connected port and communication parameters.

   NOTE

   A PC may have multiple connection ports; therefore, the port connected through the console cable is selected in this example. Generally, COM1 is selected.

   If the serial port communication parameters of the device are modified, modify the communication parameters on the PC accordingly (ensure that the parameter values are the same) and re-establish the connection.

3. Press **Enter** until the system prompts you to enter the password. (The system will prompt you to enter the user name and password in AAA authentication. The following information is only for reference.)

```
Login authentication


Password:
```

You can run commands to configure the device. Enter a question mark (?) whenever you need help.

----End

Checking the Configuration

- Run the **display users** [**all**] command to check the user log information on the user interface.
- Run the **display user-interface console 0** command to check the user interface information.
- Run the **display local-user** command to check the local user attributes.
- Run the **display access-user** command to check the online user information.

1.4.2.2 Logging In to the Device Through Telnet

Pre-configuration Tasks

Before logging in to the device through Telnet, complete the following task:

- Configuring routes between a terminal and the device

Configuration Process

NOTE

The Telnet protocol poses a security risk, and therefore the STelnet V2 mode is recommended.

Table 1-18 describes the tasks in the configuration process for login through Telnet.

Table 1-18 Tasks in the configuration process for login through Telnet

No.	Task	Description	Remarks
1	**Configuring the Telnet server functions and parameters**	Enable Telnet server functions and configure the server parameters.	Tasks 1, 2, and 3 can be performed in any sequence.
2	**Configuring the Telnet user login interface**	Configure the user level, authentication mode, call-in and call-out permission, and other basic attributes for the VTY user interface.	
3	**Configuring a local Telnet user (AAA authentication mode)**	Configure the user name and password when the AAA authentication mode is used.	

No.	Task	Description	Remarks
4	**Logging in to the device through Telnet from a terminal**	Use the Telnet client software to log in to the device from a terminal.	-

Default Configuration

Table 1-19 Default settings of the parameters for logging in to the device through Telnet

Parameter	Default Setting
Telnet service	Enabled
Telnet server port number	23
VTY user interface authentication mode	No authentication mode
Protocol supported by the VTY user interface	Telnet protocol
User level	The default command access level for the VTY user interface is 0

NOTE

When multiple users operate the device concurrently, configurations may conflict, which causes system errors. To prevent this problem, it is recommended that you run the **config lock** command in the system view to lock system configurations before performing device operations. After the device operation is complete, you can run the **undo config lock** command to unlock the system configurations.

Procedure

- **Configuring the Telnet server functions and parameters**

  Before connecting to the device through Telnet from a user terminal, make sure that the Telnet service is enabled on the device.

  Table 1-20 Configuring the Telnet server functions and parameters

Operation	Command	Description
Enter the system view.	**system-view**	-
Enable the Telnet service.	**telnet server enable**	By default, the Telnet service is enabled.

Operation	Command	Description
(Optional) Configuring the listening port of the Telnet server	**telnet server port** *port-number*	The default listening port number is 23. After the listening port number of the Telnet server is changed, attackers do not know the new listening port number. This effectively prevents attackers from accessing the listening port.
(Optional) Specify physical interfaces on the Telnet server to which clients can connect.	**telnet server permit interface** { *interface-type interface-number* }	By default, clients can connect to all the physical interfaces and BSS interfaces on the Telnet server.

- **Configuring the Telnet user login interface**

  Configure the user level, call-in and call-out permission, and other basic attributes for the VTY user interface.

  Table 1-21 Configuring the Telnet user login interface

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the VTY user interface view.	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
Configure the user level for the user interface.	**user privilege level** *level*	The default user level for the VTY user interface is 0. To run the commands of a higher level, configure a higher user level. If the user level configured for the user interface conflicts with the user's operation permission, the user permission takes precedence.

Operation	Command	Description
Configure the user authentication mode.	**authentication-mode** { **password** | **aaa** }	The password and AAA authentication modes are supported. Configure either authentication mode as required. For details on the password authentication mode, see **Configuring a user authentication mode for the VTY user interface**. The AAA authentication mode is recommended.
Configure the VTY user interface to support the Telnet protocol.	**protocol inbound** { **all** | **telnet** }	By default, the VTY user interface supports the Telnet protocol.
(Optional) Configure restrictions on ACL-based logins on the user interface.	For details, see **(Optional) Configuring Restrictions on ACL-based Logins on the VTY User Interface**.	By default, login permissions are not restricted. Configure this action to prevent a user with a certain address or address segment from logging in to the device or prevent a user who has logged in to the device from logging in to another device.
(Optional) Configure other attributes of the user interface.	For details, see **Configuring the Maximum Number of VTY User Interfaces** and **Configuring Terminal Attributes for the VTY User Interface**.	Use the default settings for other attributes of the VTY user interface. You can configure attributes based on the usage requirements.

- **Configuring a local Telnet user (AAA authentication mode)**

  Configure the administrator's user name and password to ensure that only the administrator can log in to the device.

  Table 1-22 Configuring a local Telnet user (AAA authentication mode)

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the AAA view.	**aaa**	-

Operation	Command	Description
Configure the local user name and password.	**local-user** *user-name* **password cipher** *password*	-
Configure the service type for the local user.	**local-user** *user-name* **service-type telnet**	-
Configure the level for the local user.	**local-user** *user-name* **privilege level** *level*	After login, a user can only run the commands at levels equal to or lower than the user level, which ensures the device security. If the user level configured for the user interface conflicts with the user's operation permission, the user permission takes precedence.

- **Logging in to the device through Telnet from a terminal**

  You can use Windows command line prompts or third-party software to log in to the device through Telnet from a terminal. Windows command line prompts are used as an example.

  Perform the following operations on the terminal:

  1. Access the command line window.
  2. Run the **telnet** *ip-address port* command to log in to the device through Telnet.

     ```
     C:\Documents and Settings\Administrator> telnet 10.137.217.177 1025
     ```

  3. Press **Enter** and enter the password and the user name configured for the AAA authentication mode in the login window. If authentication is successful, the command-line prompt of the user view is displayed and you have successfully logged in to the device. (The following information is only for reference.)

     ```
     Login authentication

     Username:admin1234
     Password:
     <Telnet Server>
     ```

----End

Checking the Configuration

- Run the **display users** [**all**] command to check the connections on the user interface.
- Run the **display tcp status** command to check all TCP connections.
- Run the **display telnet server status** command to check the current connections of the Telnet server.

1.4.2.3 Logging In to the Device Through STelnet

Pre-configuration Tasks

Before logging in to the device through STelnet, complete the following tasks:

- Configuring routes between a terminal and the device
- Installing the SSH client software on the terminal

Configuration Process

NOTE

The STelnet V1 protocol poses a security risk, and therefore the STelnet V2 mode is recommended.

Table 1-23 describes the tasks in the configuration process for login through STelnet.

Table 1-23 Tasks in the configuration process for login through STelnet

No.	Task	Description	Remarks
1	**Configuring the STelnet server functions and parameters**	Generate the local server key pair, enable the STelnet server function, and set the server parameters including the listening port, key pair updating interval, and SSH authentication timeout interval and retries.	Tasks 1, 2, and 3 can be performed in any sequence.
2	**Configuring the SSH user login interface**	Configure the user level, authentication mode, whether to support the SSH protocol, and other basic attributes for the VTY user interface.	
3	**Configuring an SSH user**	Configure the SSH user name, password, authentication mode, and service type.	
4	**Logging in to the device through STelnet**	Use the SSH client software to log in to the device from a terminal.	-

Default Configuration

Table 1-24 Default settings of the parameters for logging in to the device through STelnet

Parameter	Default Setting
STelnet service	Disabled
SSH server port number	22
Interval for updating the SSH server key pair	0 hours, indicating that the key pair is never updated
Timeout interval for SSH authentication	60 seconds
Maximum number of SSH authentication retries	3
SSH server's compatibility with earlier versions	Enabled
VTY user interface authentication mode	No authentication mode
Protocol supported by the VTY user interface	Telnet protocol
SSH user authentication mode	No authentication mode supported
SSH user service type	No service type supported
Whether the SSH server assigns a public key to a user	No public key assigned
User level	The default command access level for the VTY user interface is 0

NOTE

When multiple users operate the device concurrently, configurations may conflict, which causes system errors. To prevent this problem, it is recommended that you run the **config lock** command in the system view to lock system configurations before performing device operations. After the device operation is complete, you can run the **undo config lock** command to unlock the system configurations.

Procedure

- **Configuring the STelnet server functions and parameters**

Table 1-25 Configuring the STelnet server functions and parameters

Operation	Command	Description
Enter the system view.	**system-view**	-

Operation	Command	Description
Generate the local RSA key pair.	**rsa local-key-pair create**	Run the **display rsa local-key-pair public** command to view the public key in the local RSA key pair. Configure the public key on the SSH server.
Enable the STelnet service.	**stelnet server enable**	By default, the STelnet service is disabled. After you disable the STelnet service on the SSH server, all clients that have logged in through STelnet are disconnected.
(Optional) Set the listening port of the SSH server.	**ssh server port** *port-number*	The default listening port number is 22. If a new listening port number is set, the SSH server terminates all established STelnet connections, and uses the new port number to listen on new requests for Stelnet connections. This prevents attackers from accessing the standard SSH service port and ensures security.
(Optional) Set the interval for updating a key pair.	**ssh server rekey-interval** *hours*	The default interval for updating the SSH server key pair is 0, indicating that the key pair is never updated. The server key pair is automatically updated at the configured interval, which ensures security.
(Optional) Set the SSH authentication timeout interval.	**ssh server timeout** *seconds*	The default timeout interval for SSH authentication is 60 seconds. If you have not logged in successfully within the timeout interval for SSH authentication, the current connection is terminated to ensure security.
(Optional) Set the number of SSH authentication retries.	**ssh server authentication-retries** *times*	The default number of SSH authentication retries is 3. The number of SSH authentication retries is set to prevent access from unauthorized users.

Operation	Command	Description
(Optional) Enable the compatibility with SSH protocols of earlier versions.	**ssh server compatible-ssh1x enable**	By default, an SSH server running SSH2.0 is compatible with SSH1.X.
(Optional) Specify physical interfaces on the SSH server to which clients can connect.	**ssh server permit interface** { *interface-type interface-number* }	By default, clients can connect to all the physical interfaces and BSS interfaces on the SSH server.

- **Configuring the SSH user login interface**

  Configure the VTY user interface for login to support the SSH protocol before logging in to the device through SSH.

  Table 1-26 Configuring the SSH user login interface

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the VTY user interface view.	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
Configure the AAA authentication mode for the VTY user interface.	**authentication-mode aaa**	By default, **password** authentication is used for console port login and **aaa** authentication is used for login on the VTY user interface. To configure the VTY user interface to support SSH, configure the AAA authentication mode for the VTY user interface. If the AAA authentication mode is not set, the **protocol inbound ssh** command does not take effect.

Operation	Command	Description
Configure the VTY user interface to support the SSH protocol.	**protocol inbound** { **all** | **ssh** }	By default, the VTY user interface supports the Telnet protocol. If the VTY user interface does not support the SSH protocol, you cannot log in to the device through STelnet.
(Optional) Configure other attributes of the VTY user interface.	For details, see **Configuring VTY User Interfaces**.	Other user interface attributes include the maximum number of user interfaces, terminal attributes, and user level. These attributes have default values, and you do not need to set them. You can configure attributes based on the usage requirements.

- **Configuring SSH user information**

  Configure SSH user information including the authentication mode. Authentication modes including RSA, password, password-rsa, and all are supported.

  - The password-rsa authentication mode consists of the password and RSA authentication modes.
  - The all authentication mode indicates that SSH users only need to authenticated by password, or RSA.

  NOTE

  - If the SSH user uses the password authentication mode, only the SSH server needs to generate the RSA key. If the SSH user uses the RSA authentication mode, both the SSH server and client need to generate the RSA key and save and configure the public key of the peer end locally.

Table 1-27 Configuring SSH user information

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the AAA view.	**aaa**	-
Create SSH users.	**local-user** *user-name* **password cipher** *password*	-
Configure the SSH user level.	**local-user** *user-name* **privilege level** *level*	-
Configure the service type for SSH user.	**local-user** *user-name* **service-type ssh**	-
Return to the system view.	**quit**	-

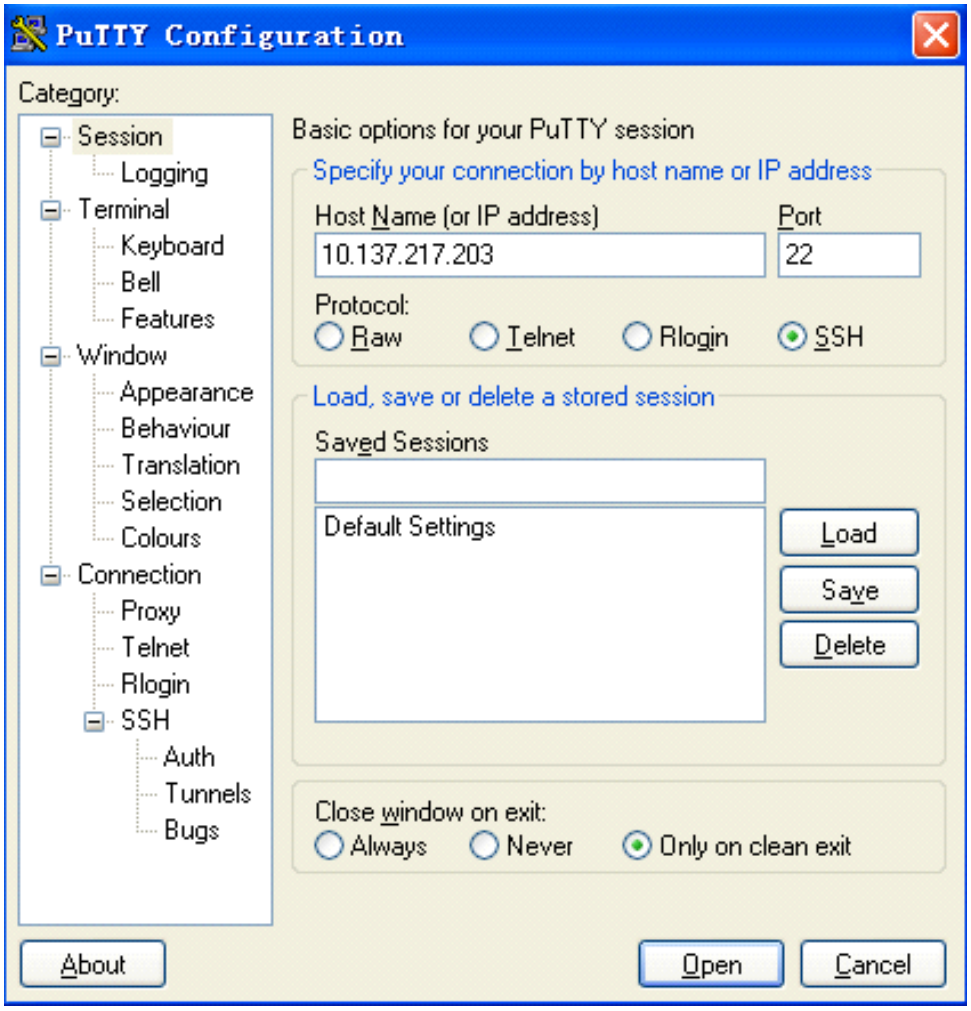
Operation		Command	Description
Configure the authentication mode for SSH users.		**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **all** }	-
If any one of the following authentication modes is configured for SSH users: ● rsa ● password-rsa	Enter the RSA public key view.	**rsa peer-public-key** *key-name*	-
	Enter the public key editing view.	**public-key-code begin**	-
	Edit the public key.	*hex-data*	● The public key must be a hexadecimal character string in the public key format generated by the SSH client software. For details, see SSH client software help. ● Copy and paste the RSA public key to the device that functions as the SSH server.
	Quit the public key editing view.	**public-key-code end**	-
	Return to the system view.	**peer-public-key end**	-
	Assign an RSA public key to an SSH user.	**ssh user** *user-name* **assign rsa-key** *key-name*	-

- **Logging in to the device through STelnet**

  Use the SSH client software to log in to the device through STelnet from a terminal. The third-party software PuTTY is used as an example here.

Use the PuTTY software to log in to the device, enter the device IP address, and select the SSH protocol type.

Figure 1-7 PuTTY Configuration page - password authentication mode



Click **Open**. Enter the user name and password at the prompt, and press **Enter**. You have logged in to the SSH server. (The following information is only for reference.)

```
login as: client001
Sent username "client001"

client001@10.137.217.203's password:

<SSH Server>
```

----End

Checking the Configuration

- Run the **display ssh user-information** [*username*] command to check information about an SSH user on the SSH server. If no SSH user is specified, this command displays information about all SSH users on the SSH server.

- Run the **display ssh server status** command to check the global SSH server configuration.
- Run the **display ssh server session** command to check the sessions connected to the SSH client on the SSH server.

1.4.2.4 Common Operations After Login

After logging in to the device, you can operate and manage the device.

- **Displaying online users**
- **Sending messages to other user interfaces**
- **Automatically searching for the undo command in the upper-level view**
- **Locking a user interface**
- **Displaying online users**

  After login, you can check the information about online users.

  - Run the **display users** [**all**] command to check the online user information.
- **Sending messages to other user interfaces**

  You can send messages from the current user interface to other user interfaces.

  1. Run the **send** { **all** | *ui-type ui-number* | *ui-number1* } command to configure the function of sending messages between user interfaces.
  2. Enter the message to send as prompted. Press **Ctrl+Z** or **Enter** to finish entering the message. Press **Ctrl+C** to terminate the operation.
  3. At the system prompt, enter **Y** to send the message or enter **N** to cancel message sending.
- **Automatically searching for the undo command in the upper-level view**

  When you run the undo command not registered with the current view, the system returns to the upper-level view to search for this undo command. If the undo command can be found, it takes effect. If the undo command cannot be found, the system continues to search for it in the next upper-level view until the system view.

  1. Run the **system-view** command to display the system view.
  2. Run the **matched upper-view** command to enable the undo command to run in the upper-level view.

     By default, the undo command does not automatically match the upper-level view.

     NOTE

     The **matched upper-view** command is only valid for current login users who run this command.

     You are not advised to configure the undo command to automatically match the upper-level view, unless necessary.
- **Locking a user interface**

  When you leave the operation terminal temporarily, you can lock the user interface to prevent unauthorized users from logging in to the terminal.

  1. Run the **lock** command to lock the user interface.
  2. Enter the lock password and confirm password.

     ```
     <Huawei> lock
     Enter Password(<6-16>):
     ```

```
Confirm Password:
Info: The terminal is locked.
```

After you run the **lock** command, the system prompts you to enter the lock password and confirm password. If the two passwords are the same, the current interface is locked successfully.

To unlock the user interface, you must press **Enter** and enter the correct login password as prompted.

1.4.3 Configuring the Device as the Client to Log In to Another Device

A user can log in to another device on the network through Telnet or STelnet from the current device to manage and maintain the remote device.

1.4.3.1 Configuring the Device as the Telnet Client to Log In to Another Device

Pre-configuration Tasks

Before configure the device as the Telnet client to log in to another device, complete the following tasks:

- Logging in to the device from a terminal
- Configuring a route between the device and Telnet server
- Enabling the Telnet service on the Telnet server
- Obtaining the Telnet user name, password, and port number configured on the Telnet server

Configuration Process

NOTE

The Telnet protocol poses a security risk, and therefore the STelnet V2 protocol is recommended.

Table 1-28 describes the tasks in the process of configuring the device as the Telnet client to log in to another device.

Table 1-28 Tasks in the process of configuring the device as the Telnet client to log in to another device

No.	Task	Description	Remarks
1	**(Optional) Configure the Telnet client source address**	Configure the Telnet client source address. The source address can be set to a source IP address or source interface information, ensuring communication security.	-
2	**Log in to another device through Telnet.**	Use the Telnet command to log in to the device from a terminal.	

Procedure

Step 1 (Optional) Configure the source address of the Telnet client.

Table 1-29 Configure the source address of the Telnet client.

Action	Command	Description
Enter the system view.	**system-view**	-
Configure the Telnet client source address.	**telnet client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	The Telnet client source address on the server must be the same as the address configured running this command.
Return to user view.	**quit**	-

Step 2 Log in to another device through Telnet.

Table 1-30 Actions for logging in to another device through Telnet

Action	Command	Description
Use the IPv4 address to log in to the server through Telnet.	**telnet** [**-a** *source-ip-address*] *host-ip* [*port-number*]	-

----End

Checking the Configuration

- Run the **display tcp status** command to check all TCP connections.

1.4.3.2 Configuring the Device as the STelnet Client to Log In to Another Device

Pre-configuration Tasks

Before configure the device as the STelnet client to log in to another device, complete the following tasks:

- Logging in to the device from a terminal
- Configuring a route between the device and STelnet server
- Enabling the STelnet service on the STelnet server
- Obtaining the SSH user information and port number configured on the STelnet server

Configuration Process

Table 1-31 describes the tasks in the process of configuring the device as the STelnet client to log in to another device.

Table 1-31 Tasks in the process of configuring the device as the STelnet client to log in to another device

No.	Task	Description	Remarks
1	**Generating a local key pair**	Generate a local key pair and configure the public key on the SSH server. Perform this task only when the device logs in to the SSH server in RSA authentication mode.	Tasks 1 and 2 can be performed in any sequence.
2	**Configuring the mode for connecting the device to the SSH server for the first time**	You can enable the first authentication function of the SSH client or configure the SSH client to assign a public key to the SSH server.	
3	**Logging in to another device through STelnet.**	Use the STelnet client software to log in to the device from a terminal.	-

Default Configuration

Table 1-32 Default values for configuring the device as the STelnet client to log in to another device

Parameter	Default Setting
First authentication on the SSH client	Disabled
Whether the SSH client assigns the RSA public key to the SSH server	No

Procedure

- **Generating a local key pair**

  NOTE

  Perform this step only when the device logs in to the SSH server in RSA authentication mode, not the password authentication mode.

  Table 1-33 Actions for generating a local key pair

Action	Command	Description
Enter the system view.	**system-view**	-

Action	Command	Description
Generate the local RSA key pair.	**rsa local-key-pair create**	Run the **display rsa local-key-pair public** command to view the public key in the local RSA key pair. Configure the public key on the SSH server.

- **Configuring the mode for connecting the device to the SSH server for the first time**

  If the public key of the SSH server has not been saved on the client, the system cannot check SSH server validity when the device that works as the client connects to the SSH server for the first time. The connection fails. Perform one of the following operations:

  - Enabling the first authentication mode on the SSH client: The system does not check the public key of the SSH server, which ensures that the first connection is successful. The system then assigns and saves the public key for subsequent authentication. For details, see **Table 1-34**. This configuration method is simple.
  - Configuring the SSH client to assign a public key to the SSH server. The public key generated on the server is saved on the client, which ensures that the SSH server validity check is successful for the first connection. For details, see **Table 1-35**. This configuration method is complex but has high security.

  Select either of the preceding configuration method as required.

Table 1-34 Actions for enabling first authentication for the SSH client

Action	Command	Description
Enter the system view.	**system-view**	-
Enable first authentication for the SSH client.	**ssh client first-time enable**	By default, first authentication is disabled on the SSH client.

Table 1-35 Actions for configuring the SSH client to assign the RSA public key to the SSH server

Action	Command	Description
Enter the system view.	**system-view**	-
Enter the RSA public key view.	**rsa peer-public-key** *key-name*	-
Enter the public key editing view.	**public-key-code begin**	-

Action	Command	Description
Edit the public key.	*hex-data*	● The public key must be a hexadecimal character string in the public key encoding format, and generated by the SSH server. ● After entering the public key editing view, you must enter the RSA public key that is generated on the server to the client.
Quit the public key editing view.	**public-key-code end**	● If no key public code hex-data is entered, the public key cannot be generated after you run this command. ● If the specified key *key-name* has been deleted, the system displays a message indicating that the key does not exist and returns to the system view directly when you run this command.
Return to the system view.	**peer-public-key end**	-
Bind the RSA public key to the SSH server.	**ssh client** *servername* **assign rsa-key** *keyname*	If the SSH server public key saved in the SSH client does not take effect, run the **undo ssh client** *servername* **assign rsa-key** command to cancel the binding between the SSH server and RSA public key, and run this command to assign a new RSA public key to the SSH server.

- **Logging in to another device through STelnet**

Table 1-36 Actions for logging in to another device through STelnet

Action	Command	Description
Enter the system view.	**system-view**	-

Action	Command	Description
Use the IPv4 address to log in to the SSH server through STelnet.	**stelnet** [**-a** *source-address*] *host-ip* [*port-number*] [[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]	The STelnet client can log in successfully with no port specified only when the server is listening on port 22. If the server is listening on another port, the port number must be specified upon login. When logging in to the SSH server, the STelnet client can carry the source IP address and select a key exchange algorithm, an encryption algorithm, and an HMAC algorithm, and configure the keepalive function.

----End

Checking the Configuration

Run the **display ssh server** { **status** | **session** } command to check the mapping between all SSH servers and RSA public keys on the SSH client.

1.4.4 Configuration Examples

This section describes the examples for logging in to the device through a console port, Telnet, and for configuring the device to log in to another device.

1.4.4.1 Example for Logging In to the Device Through a Console Port

Networking Requirements

When you cannot remotely log in to the device, you can perform local login through a console port. If you log in to the device through a console port, only password authentication is required. To improve security, use AAA on the console user interface.

Figure 1-8 Networking diagram of user login through a console port

Configuration Roadmap

The configuration roadmap is as follows:

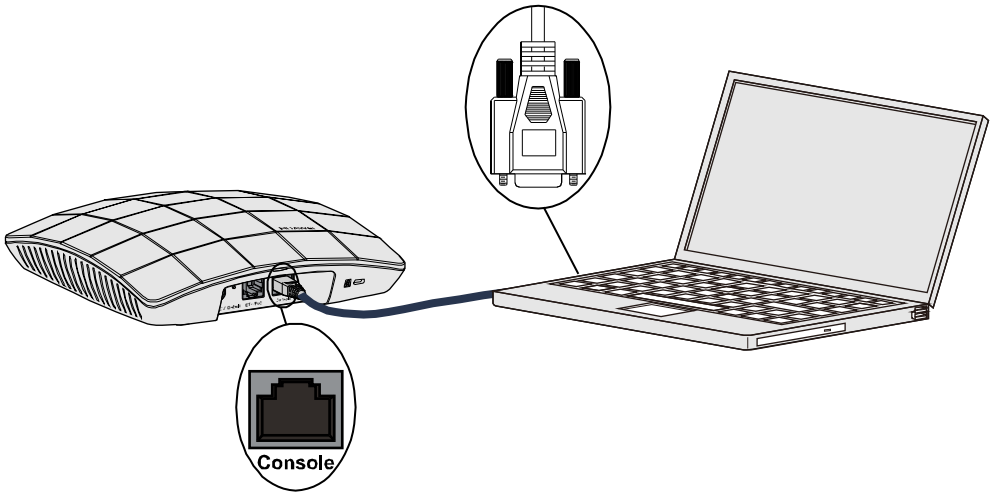
1. Use the terminal simulation software to log in to the device through a console port.
2. Configure the authentication mode of the console user interface.

Procedure

Step 1 Use the terminal simulation software to log in to the device through a console port.

1. Insert the DB9 connector of the console cable delivered with the product to the 9-pin serial port on the PC, and insert the RJ45 connector to the console port of the device, as shown in **Figure 1-9**.

   Figure 1-9 Connecting to the device through the console port

2. Start the terminal simulation software on the PC. Establish a connection, and set the connected port and communication parameters.

   NOTE

   A PC may have multiple connection ports; therefore, the port connected through the console cable is selected in this example. Generally, COM1 is selected.

   If the serial port communication parameters of the device are modified, modify the communication parameters on the PC accordingly (ensure that the parameter values are the same) and re-establish the connection.

3. Press **Enter** until the system prompts you to enter the password. (The system will prompt you to enter the user name and password in AAA authentication. The following information is only for reference.)

   ```
   Login authentication


   Password:
   ```

   You can run commands to configure the device. Enter a question mark (?) whenever you need help.

Step 2 Configure the authentication mode of the console user interface.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] authentication-mode aaa
[Huawei-ui-console0] user privilege level 15
[Huawei-ui-console0] quit
[Huawei] aaa
[Huawei-aaa] local-user admin1234 password cipher Helloworld@6789
[Huawei-aaa] local-user admin1234 privilege level 3
[Huawei-aaa] local-user admin1234 service-type terminal
```

After the preceding operations, you can re-log in to the device on the console user interface only by entering the user name **admin1234** and password **Helloworld@6789**.

----End

Configuration Files

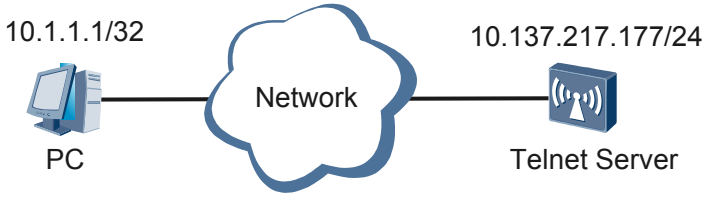
```
#
aaa
 local-user admin1234 password cipher %$%$~^Mg.QBcGS^}H.Q*w~#*,JA8%$%$
 local-user admin1234 privilege level 3
 local-user admin1234 service-type terminal
#
user-interface con 0
 authentication-mode aaa
#
return
```

1.4.4.2 Example for Logging In to the Device Through Telnet

Networking Requirements

As shown in **Figure 1-10**, the PC and the server (Huawei device) are reachable to each other. To implement easy remote configuration and management of the device, configure AAA authentication for Telnet users on the server and configure a security policy that allows only the administrator to log in to the device.

Figure 1-10 Networking diagram of logging in to the device through Telnet



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Telnet login mode to implement remote network device maintenance.
2. Configure the administrator's user name and password and the AAA authentication mode to ensure that only the administrator can log in to the device.

3. Configure a security policy to ensure that the administrator's PC can be used to log in to the device.

Procedure

Step 1 Set the server listening port number and enable the server function.

```
<Huawei> system-view
[Huawei] sysname Telnet Server
[Telnet Server] telnet server enable
[Telnet Server] telnet server port 1025
```

Step 2 Set the VTY user interface parameters.

Set the maximum number of VTY user interfaces.

```
[Telnet Server] user-interface maximum-vty 8
```

Set the IP address of the device to which the user is allowed to log in.

```
[Telnet Server] acl 2001
[Telnet Server-acl-basic-2001] rule permit source 10.1.1.1 0
[Telnet Server-acl-basic-2001] quit
[Telnet Server] user-interface vty 0 7
[Telnet Server-ui-vty0-7] acl 2001 inbound
```

Configure the terminal attributes of the VTY user interface.

```
[Telnet Server-ui-vty0-7] shell
[Telnet Server-ui-vty0-7] idle-timeout 20
[Telnet Server-ui-vty0-7] screen-length 30
[Telnet Server-ui-vty0-7] history-command max-size 20
```

Configure the user authentication mode of the VTY user interface.

```
[Telnet Server-ui-vty0-7] authentication-mode aaa
[Telnet Server-ui-vty0-7] quit
```

Step 3 Configure the login user information.

Configure the login authentication mode.

```
[Telnet Server] aaa
[Telnet Server-aaa] local-user admin1234 password cipher Helloworld@6789
[Telnet Server-aaa] local-user admin1234 service-type telnet
[Telnet Server-aaa] local-user admin1234 privilege level 3
[Telnet Server-aaa] quit
```

Step 4 Configure the client login.

Enter commands at the command line prompt to log in to the device through Telnet.

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177 1025
```

Press **Enter**, and enter the user name and password in the login window. If the authentication is successful, the command line prompt of the user view is displayed. The user view configuration environment is displayed.

```
Login authentication

Username:admin1234
Password:
<Telnet Server>
```

----End

Configuration Files

Telnet server configuration file

```
#
 sysname Telnet Server
#
telnet server port 1025
#
acl number 2001
 rule 5 permit source 10.1.1.1 0
#
aaa
 local-user admin1234 password cipher %$%$~^Mg.QBcGS^}H.Q*w~#*,JA8%$%$
 local-user admin1234 privilege level 3
 local-user admin1234 service-type telnet
#
user-interface maximum-vty 8
user-interface vty 0 7
 acl 2001 inbound
 authentication-mode aaa
 history-command max-size 20
 idle-timeout 20 0
 screen-length 30
#
return
```

1.4.4.3 Example for Logging In to the Device Through STelnet

Networking Requirements

As shown in **Figure 1-11**, users require secure remote login, but Telnet cannot provide a secure authentication method. In this scenario, STelnet can be configured to ensure security of remote login. 10.137.217.203 is the IP address of the management interface on the SSH server. Two login users client001 and client002 need to be configured on the SSH server. PC1 uses the account of client001 to log in to the SSH server through password authentication; PC2 uses the account of client002 to log in to the SSH server through RSA authentication.

Figure 1-11 Networking diagram of logging in to the device through STelnet

Configuration Roadmap

The configuration roadmap is as follows:

1. Install the SSH server software on PC1. Install the key pair generation software, public key conversion software, and SSH server login software on PC2.
2. Generate a local key pair on the SSH server to implement secure data exchange between the server and client.

3. Configure different authentication modes for the SSH users **client001** and **client002** on the SSH server.
4. Enable the STelnet service on the SSH server.
5. Configure the STelnet server type for the SSH users **client001** and **client002** on the SSH server.
6. Log in to the SSH server as the **client001** and **client002** users through STelnet.

Procedure

Step 1 Generate a local key pair on the server.

```
<Huawei> system-view
[Huawei] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 2048]:1024
Generating keys...
........++++++++
..++++++++
............+++++++++
......+++++++++
```

Step 2 Create an SSH user on the server.

NOTE

There are four authentication modes for an SSH user: password, RSA, password-RSA, and all.

- If the authentication mode is password or password-RSA, configure a local user on the server with the same user name.
- If the authentication mode is RSA, password-RSA, or all, save the RSA public key generated on the SSH client to the server.

Configure the VTY user interface.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound all
[SSH Server-ui-vty0-4] user privilege level 5
[SSH Server-ui-vty0-4] quit
```

- Create an SSH user named **client001**.

  # Create an SSH user named **client001** and configure the password authentication mode for the user.Set the password of the **client001** user to **huawei@123**.

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client001 password cipher huawei@123
  [SSH Server-aaa] local-user client001 privilege level 3
  [SSH Server-aaa] local-user client001 service-type ssh
  [SSH Server-aaa] quit
  [SSH Server] ssh user client001 authentication-type password
  ```

- Create an SSH user named **client002**.

  # Create an SSH user named **client002** and configure the RSA authentication mode for the user.

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client002 password cipher Huawei@2012
  [SSH Server-aaa] local-user client002 privilege level 3
  [SSH Server-aaa] local-user client002 service-type ssh
  ```

```
[SSH Server-aaa] quit
[SSH Server] ssh user client002 authentication-type rsa
```

Generate a local key pair of the client on PC2.

NOTE

The software varies in acutal situation. The following software is for reference only.

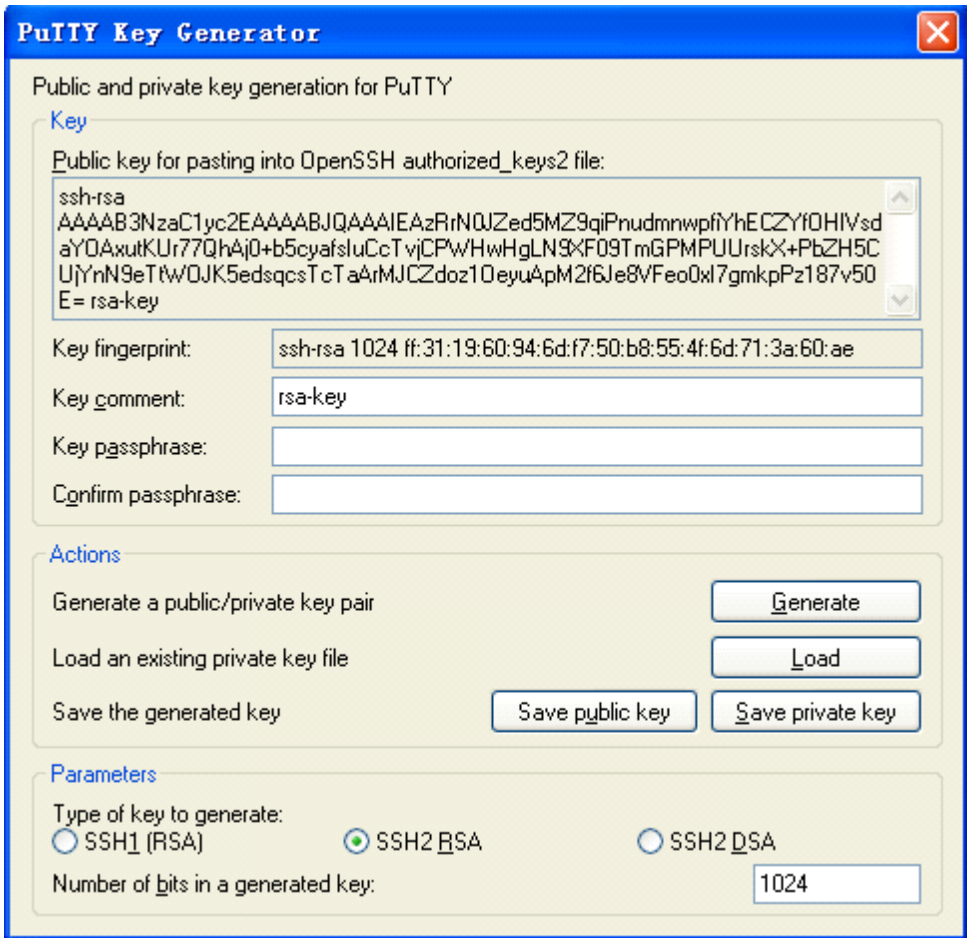
1. Run **puttygen.exe** on the client. It is used to generate the public and private key files.

   Select **SSH2 RSA** and click **Generate**. By moving the cursor in the blank area, you can find that the key is being generated.

   Figure 1-12 PuTTY Key Generate page (1)

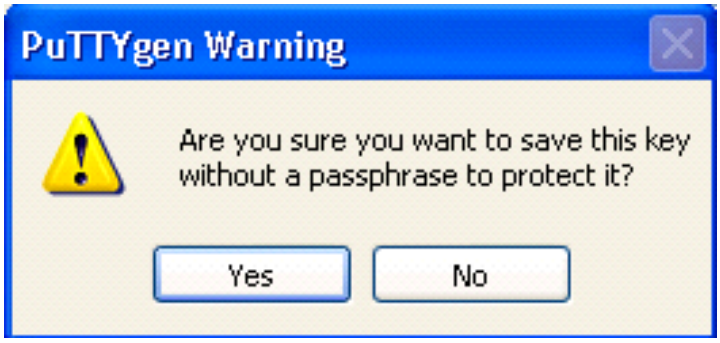
   After the key is generated, click **Save public key** to save the key in the **key.pub** file.

Figure 1-13 PuTTY Key Generate page (2)



Click **Save private key**. The **PuTTYgen Warning** dialog box is displayed. Click **Yes**. The private key is saved in the **private.ppk** file.

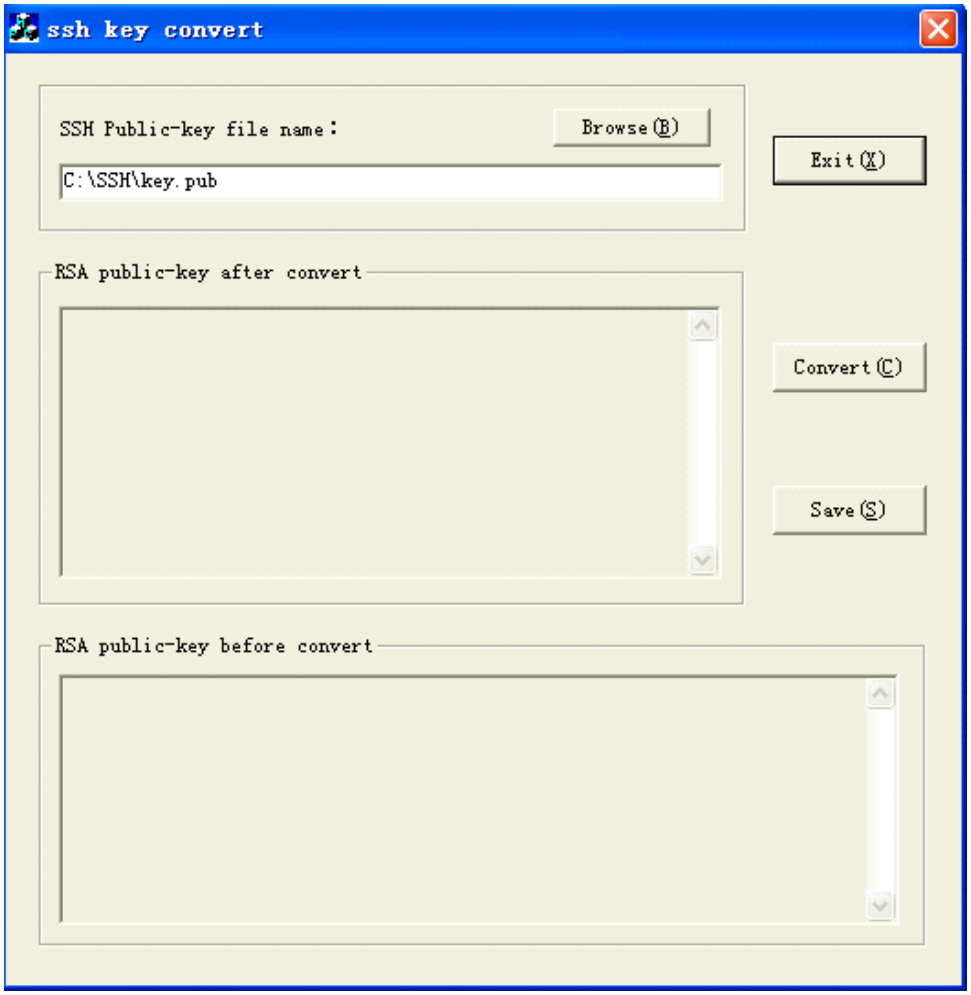
Figure 1-14 PuTTY Key Generate page (3)



2. Run **sshkey.exe** on the client. Convert the generated public key to the character string required for the device.

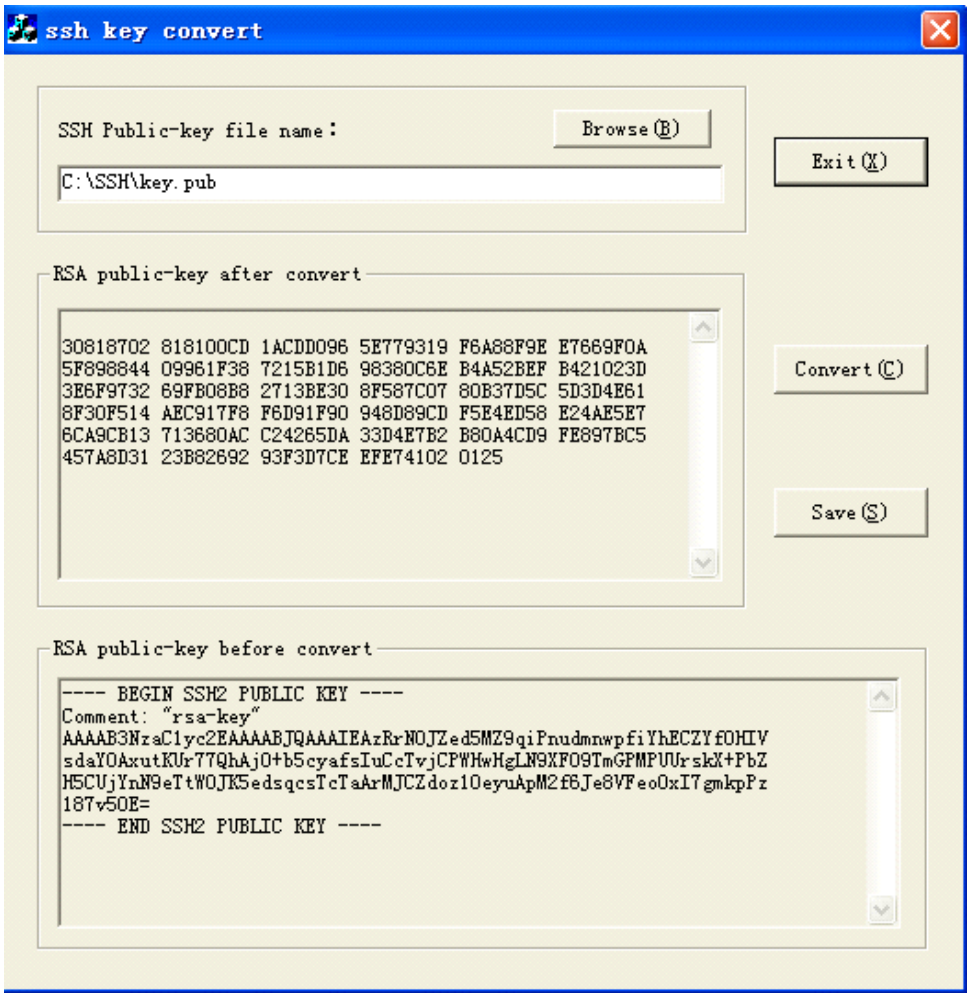
   Open the **key.pub** file required by SSH that is generated in the previous step.

Figure 1-15 ssh key converter page (1)



Click **Convert(C)**. You can see the public keys before and after conversion.

Figure 1-16 ssh key converter page (2)



Enter the RSA public key generated on PC2 to the SSH server.

```
[SSH Server] rsa peer-public-key rsakey001
[SSH Server-rsa-public-key] public-key-code begin
[SSH Server-rsa-key-code] 30818702 818100CD 1ACDD096 5E779319 F6A88F9E E7669F0A
[SSH Server-rsa-key-code] 5F898844 09961F38 7215B1D6 98380C6E B4A52BEF B421023D
[SSH Server-rsa-key-code] 3E6F9732 69FB08B8 2713BE30 8F587C07 80B37D5C 5D3D4E61
[SSH Server-rsa-key-code] 8F30F514 AEC917F8 F6D91F90 948D89CD F5E4ED58 E24AE5E7
[SSH Server-rsa-key-code] 6CA9CB13 713680AC C24265DA 33D4E7B2 B80A4CD9 FE897BC5
[SSH Server-rsa-key-code] 457A8D31 23B82692 93F3D7CE EFE74102 0125
[SSH Server-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

Bind the RSA public key of the STelnet client to the SSH user client002 on the SSH server.

```
[SSH Server] ssh user client002 assign rsa-key rsakey001
```

Step 3 Enable the STelnet service on the SSH server.

Enable the STelnet service.

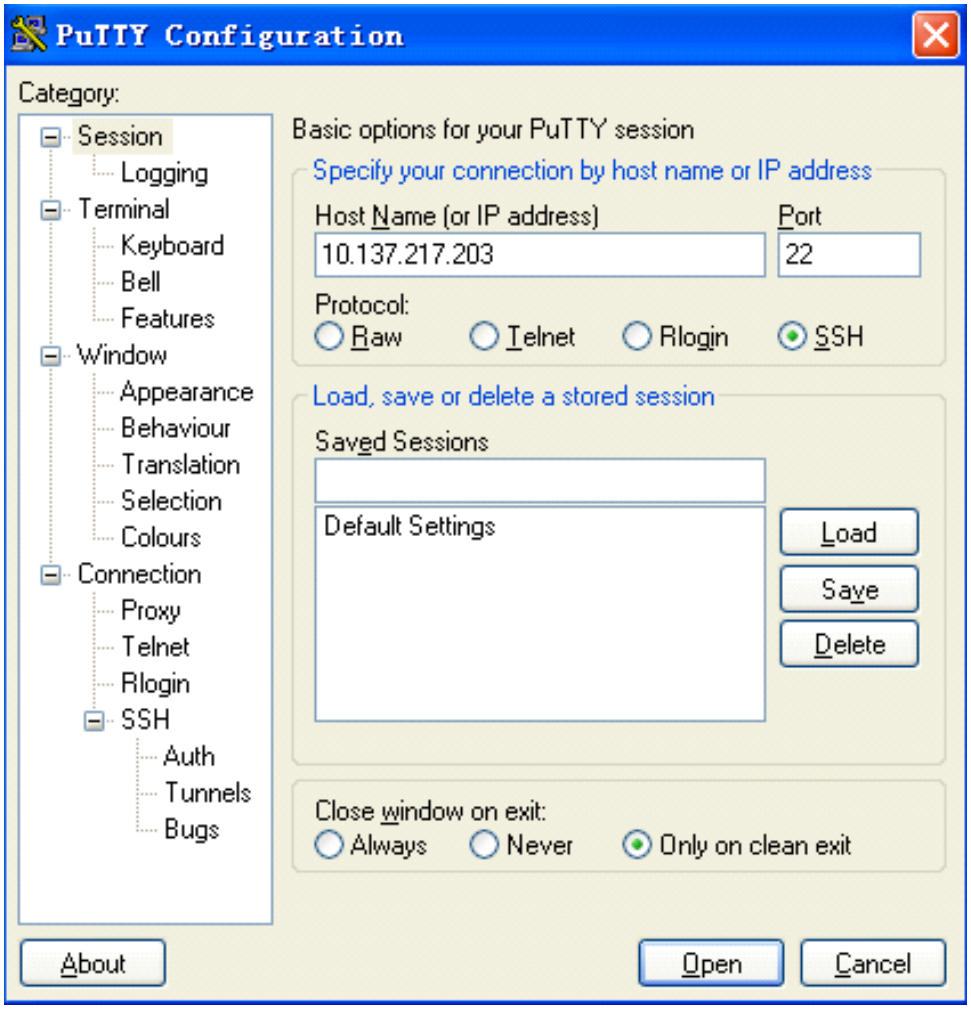
```
[SSH Server] stelnet server enable
```

Step 4 Verify the configuration.

- Log in to the SSH server as the **client001** user from PC1 using the password authentication mode.

Use the PuTTY software to log in to the device, enter the device IP address, and select the SSH protocol type.

Figure 1-17 PuTTY Configuration page - password authentication mode



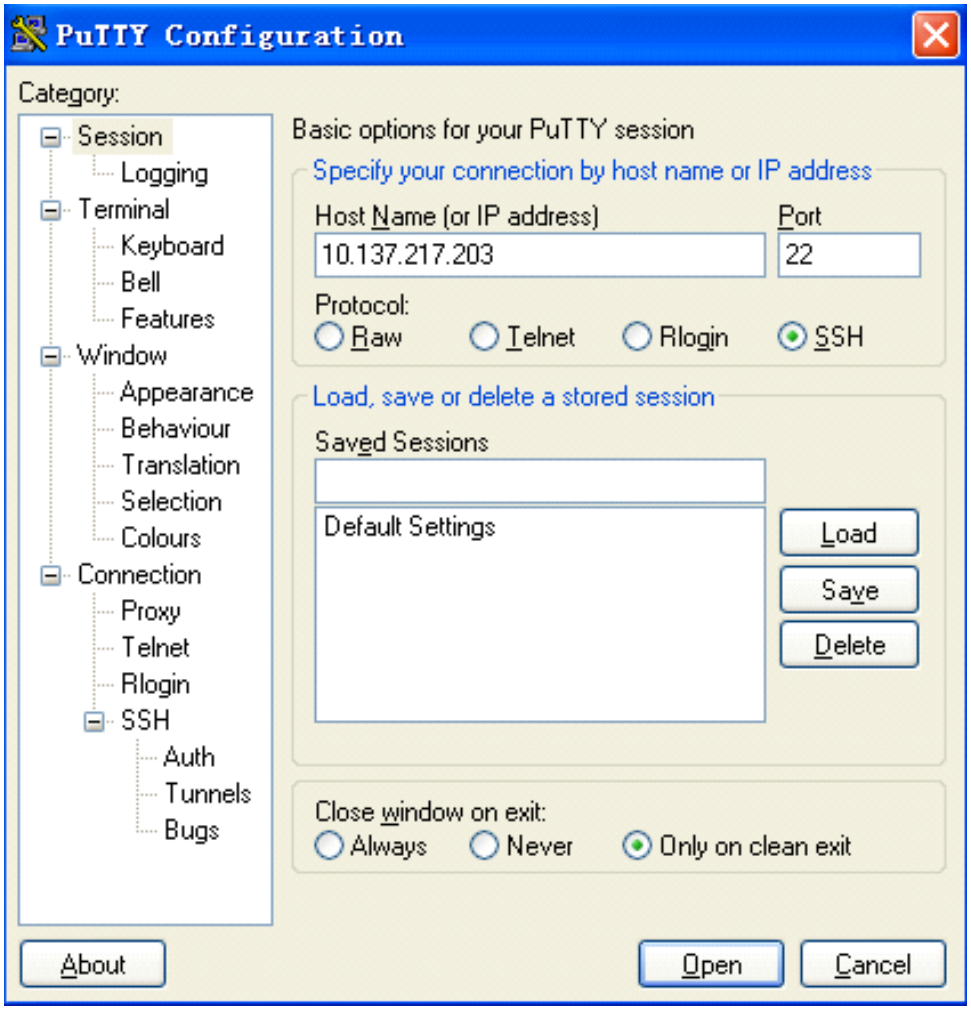
Click **Open**. Enter the user name and password at the prompt, and press **Enter**. You have logged in to the SSH server.

```
login as: client001
Sent username "client001"

client001@10.137.217.203's password:

<SSH Server>
```

- Log in to the SSH server as the **client002** user from PC2 using the RSA authentication mode.

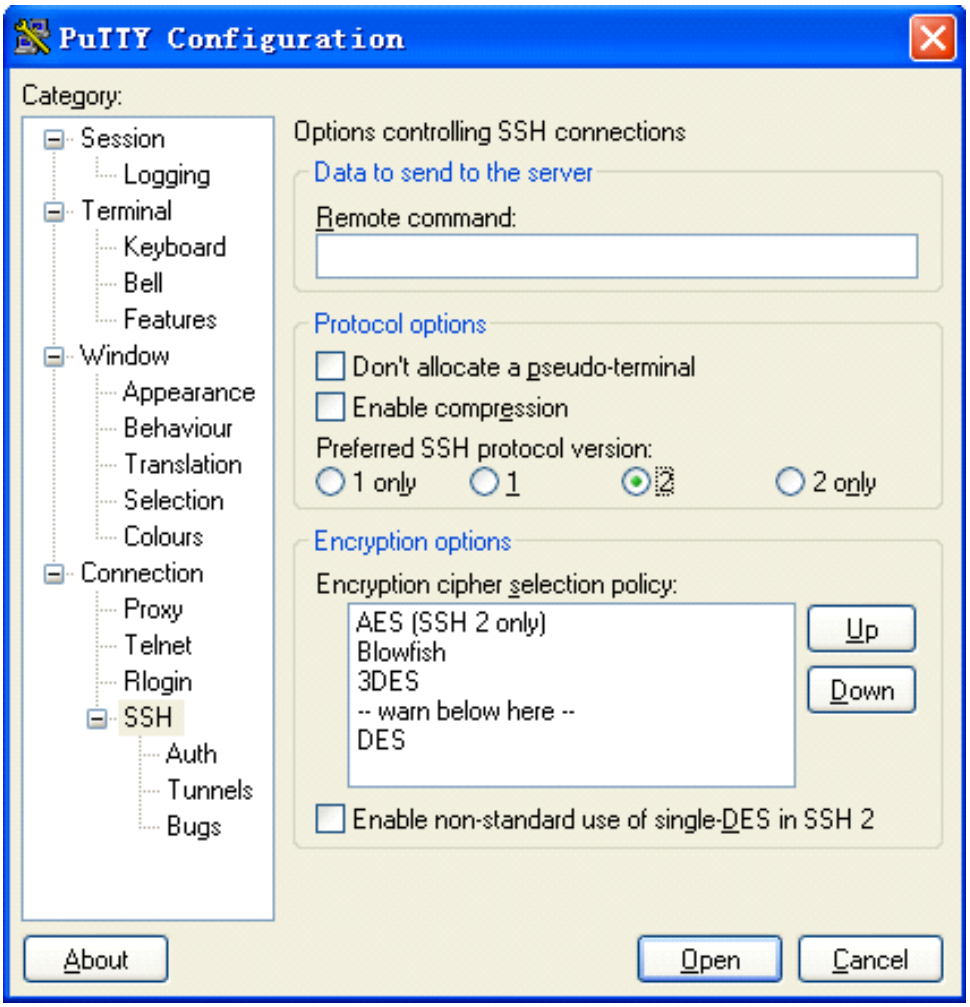
  # Use the PuTTY software to log in to the device, enter the device IP address, and select the SSH protocol type.

Figure 1-18 PuTTY Configuration page - RSA authentication mode (1)



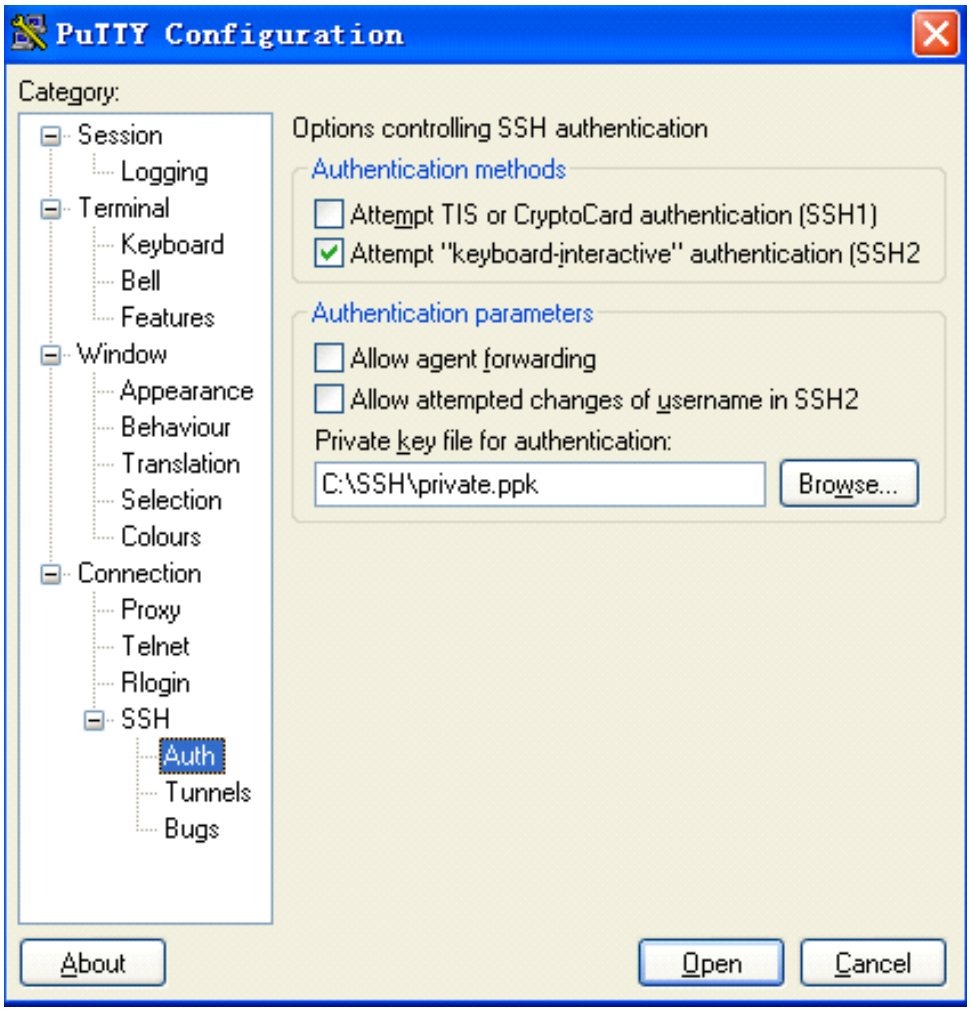
Choose **Connection** > **SSH** in the navigation tree. The page shown in **Figure 1-19** is displayed. Select **2** for **Preferred SSH protocol version**

Figure 1-19 PuTTY Configuration page - RSA authentication mode (2)



Choose **Connection** > **SSH** > **Auth** in the navigation tree. The page shown in **Figure 1-20** is displayed. Select the **private.ppk** file corresponding to the public key configured on the server.

Figure 1-20 PuTTY Configuration page - RSA authentication mode (3)



Click **Open**. Enter the user name at the prompt, and press **Enter**. You have logged in to the SSH server.

```
login as: client002
Authenticating with public key "rsa-key"

<SSH Server>
```

----End

Configuration Files

SSH server configuration file

```
#
 sysname SSH Server
#
 rsa peer-public-key rsakey001
  public-key-code begin
   308186
     028180
       CD1ACDD0 965E7793 19F6A88F 9EE7669F 0A5F8988 4409961F 387215B1 D698380C
       6EB4A52B EFB42102 3D3E6F97 3269FB08 B82713BE 308F587C 0780B37D 5C5D3D4E
```

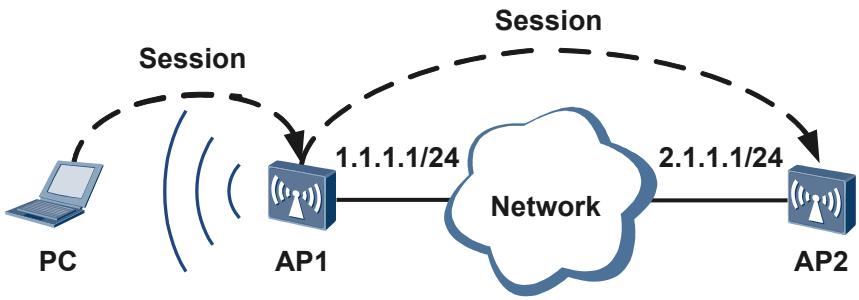
```
        618F30F5 14AEC917 F8F6D91F 90948D89 CDF5E4ED 58E24AE5 E76CA9CB 13713680
        ACC24265 DA33D4E7 B2B80A4C D9FE897B C5457A8D 3123B826 9293F3D7 CEEFE741
      0201
        25
  public-key-code end
 peer-public-key end
#
aaa
 local-user client001 password cipher %@%@~)5r!#>ZoLU0T^*IoFR'i_^*%@%@
 local-user client001 privilege level 3
 local-user client001 service-type ssh
 local-user client002 password cipher %@%@aG@2;Q)McUH{^TYF`o:Nm7,;%@%@
 local-user client002 privilege level 3
 local-user client002 service-type ssh
#
ssh user client002 assign rsa-key rsakey001
ssh user client002 authentication-type rsa
stelnet server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 5
 protocol inbound ssh
#
return
```

1.4.4.4 Example for Configuring the Device as the Telnet Client to Log In to Another Device

Networking Requirements

The user needs to manage and maintain AP2 remotely, as shown in **Figure 1-21**. However, the PC cannot directly log in to AP2 through Telnet. The user needs to log in to AP1 through Telnet, and then log in to AP2 from AP1 through Telnet. To prevent unauthorized devices from logging in to AP2 through Telnet, an ACL needs to be configured to allow only the Telnet connection from AP1 to AP2.

Figure 1-21 Networking diagram of configuring the device as the Telnet client to log in to another device



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the Telnet authentication mode and password on AP2.

2. Configure the AP2 to allow AP1 access with ACL.
3. Log in to AP2 from AP1 through Telnet.

Procedure

Step 1 Configure the Telnet authentication mode and password on AP2.

```
<Huawei> system-view
[Huawei] sysname AP2
[AP2] user-interface vty 0 4
[AP2-ui-vty0-4] user privilege level 15
[AP2-ui-vty0-4] authentication-mode password
[AP2-ui-vty0-4] set authentication password cipher
Enter Password(<6-16>):
Confirm Password:
[AP2-ui-vty0-4] quit
```

Step 2 Configure the AP2 to allow AP1 access with ACL.

```
[AP2] acl 2000
[AP2-acl-basic-2000] rule permit source 1.1.1.1 0
[AP2-acl-basic-2000] quit
[AP2] user-interface vty 0 4
[AP2-ui-vty0-4] acl 2000 inbound
[AP2-ui-vty0-4] quit
```

NOTE

It is optional to configure an ACL for Telnet services.

Step 3 Verify the configuration.

After the preceding configuration, you can log in to AP2 from AP1 through Telnet. You cannot log in to AP2 from other devices.

```
<Huawei> system-view
[Huawei] sysname AP1
[AP1] quit
<AP1> telnet 2.1.1.1
  Press CTRL_] to quit telnet mode
  Trying 2.1.1.1 ...
  Connected to 2.1.1.1 ...

Login authentication


Password:
<AP2>
```

----End

Configuration Files

AP2 configuration file

```
#
 sysname AP2
#
acl number 2000
 rule 5 permit source 1.1.1.1 0
#
user-interface vty 0 4
 acl 2000 inbound
 authentication-mode password
 user privilege level 15
```

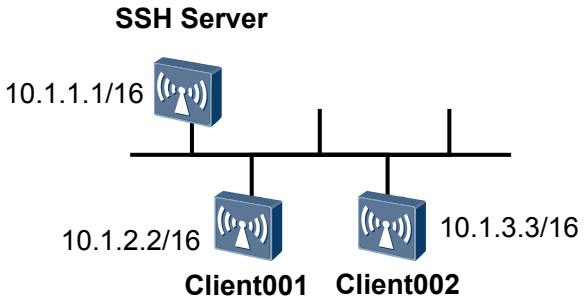
```
 set authentication password cipher %$%$]*6iWr7EVM|uc:"B/A=FF}tk%$%$
#
return
```

1.4.4.5 Example for Configuring the Device as the STelnet Client to Log In to Another Device

Networking Requirements

The enterprise requires that secure data exchange should be performed between the server and client. As shown in **Figure 1-22**, two login users **client001** and **client002** are configured and they use the password and RSA authentication modes respectively to log in to the SSH server. A new port number is configured and the default port number is not used.

Figure 1-22 Networking diagram of logging in to another device through STelnet



Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair on the SSH server to implement secure data exchange between the server and client.
2. Configure different authentication modes for the SSH users **client001** and **client002** on the SSH server.
3. Enable the STelnet service on the SSH server.
4. Configure the STelnet server type for the SSH users **client001** and **client002** on the SSH server.
5. Set the SSH server listening port number on the SSH server to prevent attackers from accessing the SSH service standard port and ensure security.
6. Log in to the SSH server as the **client001** and **client002** users through STelnet.

Procedure

Step 1 Generate a local key pair on the server.

```
<Huawei> system-view
[Huawei] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
```

```
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 2048]:1024
Generating keys...
........++++++++
..++++++++
............+++++++++
......+++++++++
```

Step 2 Create an SSH user on the server.

NOTE

There are four authentication modes for an SSH user: password, RSA, password-RSA, and all.

- If the authentication mode is password or password-RSA, configure a local user on the server with the same user name.
- If the authentication mode is RSA, password-RSA, or all, save the RSA public key generated on the SSH client to the server.

Configure the VTY user interface.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound all
[SSH Server-ui-vty0-4] user privilege level 5
[SSH Server-ui-vty0-4] quit
```

- Create an SSH user named **client001**.

  # Create an SSH user named **client001** and configure the password authentication mode for the user.Set the password of the **client001** user to **huawei@123**.

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client001 password cipher huawei@123
  [SSH Server-aaa] local-user client001 privilege level 3
  [SSH Server-aaa] local-user client001 service-type ssh
  [SSH Server-aaa] quit
  [SSH Server] ssh user client001 authentication-type password
  ```

- Create an SSH user named **client002**.

  # Create an SSH user named **client002** and configure the RSA authentication mode for the user.

  ```
  [SSH Server] aaa
  [SSH Server-aaa] local-user client002 password cipher Hello@123
  [SSH Server-aaa] local-user client002 privilege level 3
  [SSH Server-aaa] local-user client002 service-type ssh
  [SSH Server-aaa] quit
  [SSH Server] ssh user client002 authentication-type rsa
  ```

  # Generate a local key pair for Client002.

  ```
  <Huawei> system-view
  [Huawei] sysname client002
  [client002] rsa local-key-pair create
  The key name will be: Host
  The range of public key size is (512 ~ 2048).
  NOTES: If the key modulus is greater than 512,
         It will take a few minutes.
  Input the bits in the modulus[default = 2048]:1024
  Generating keys...
  ........++++++++
  ..++++++++
  ............+++++++++
  ......+++++++++
  ```

  # Check the public key in the RSA key pair generated on the client.

```
[client002] display rsa local-key-pair public

=====================================================
Time of Key pair created: 2012-08-06 17:17:37+00:00
Key name: Host
Key type: RSA encryption Key
=====================================================
Key code:
308188
  028180
    B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
    A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
    411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
    40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
    1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
    A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
    171896FB 1FFC38CD
  0203
    010001

=====================================================
Time of Key pair created: 2012-08-06 17:17:44+00:00
Key name: Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    DF8AFF3C 28213B94 2292852E E98657EE 11DE5AF4
    8A176878 CDD4BD31 55E05735 3080F367 A83A9034
    47D534CA 81250C1D 35401DC3 464E9E5F A50202CF
    A7AD09CD AC3F531C A763F0A0 4C8E51B9 18755400
    76AF4A78 225C92C3 01FE0DFF 06908363
  0203
    010001
```

Configure the RSA public key on the SSH server. (Information in bold in the **display** command output is the RSA public key. Copy the information to the server.)

```
[SSH Server] rsa peer-public-key rsakey001
[SSH Server-rsa-public-key] public-key-code begin
[SSH Server-rsa-key-code] 308188
[SSH Server-rsa-key-code] 028180
[SSH Server-rsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[SSH Server-rsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[SSH Server-rsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[SSH Server-rsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[SSH Server-rsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[SSH Server-rsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[SSH Server-rsa-key-code] 171896FB 1FFC38CD
[SSH Server-rsa-key-code] 0203
[SSH Server-rsa-key-code] 010001
[SSH Server-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

Bind the RSA public key of the STelnet client to the SSH user client002 on the SSH server.

```
[SSH Server] ssh user client002 assign rsa-key rsakey001
```

Step 3 Enable the STelnet service on the SSH server.

Enable the STelnet service.

```
[SSH Server] stelnet server enable
```

Step 4 Configure a new listening port number on the SSH server.

```
[SSH Server] ssh server port 1025
```

Step 5 Connect the STelnet client to the SSH server.

Enable the first authentication function on the SSH client upon the first login.

Enable the first authentication function for Client001.

```
<Huawei> system-view
[Huawei] sysname client001
[client001] ssh client first-time enable
```

Enable the first authentication function for Client002.

```
[client002] ssh client first-time enable
```

Log in to the SSH server from Client001 in password authentication mode by entering the user name and password.

```
[client001] stelnet 10.1.1.1 1025
Please input the username:client001
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it?[Y/N]:y
Save the server's public key?[Y/N]:y
The server's public key will be saved with the name 10.1.1.1. Please wait...

Enter password:
```

Enter the password. The following information indicates that you have logged in successfully:

```
<SSH Server>
```

Log in to the SSH server from Client002 in RSA authentication mode.

```
[client002] stelnet 10.1.1.1 1025
Please input the username: client002
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it?(Y/N):y
Save the server's public key?(Y/N):y
The server's public key will be saved with the name 10.1.1.1. Please wait...
<SSH Server>
```

If the user view is displayed, you have logged in successfully. If the message "Session is disconnected" is displayed, the login fails.

Step 6 Verify the configuration.

Attackers fail to log in to the SSH server using the default listening port number 22.

```
[client002] stelnet 10.1.1.1
Please input the username:client002
Trying 10.1.1.1 ...
Press CTRL+K to abort
Error: Failed to connect to the remote host.
```

Run the **display ssh server status** commands. You can see that the STelnet service has been enabled. Run the **display ssh user-information** command. Information about the configured SSH users is displayed.

Check the status of the SSH server.

```
[SSH Server] display ssh server status
 SSH version                         :1.99
 SSH connection timeout              :60 seconds
```

```
 SSH server key generating interval  :0 hours
 SSH Authentication retries          :3 times
 SFTP Server                         :Disable
 Stelnet server                      :Enable
 SSH server port                     :1025
```

Check information about SSH users.

```
[SSH Server] display ssh user-information
------------------------------------------------------------------------------
 Username         Auth-type          User-public-key-name
 ------------------------------------------------------------------------------
 client001        password           null
 client002        rsa                rsakey001
 ------------------------------------------------------------------------------
```

----End

Configuration Files

- SSH server configuration file

```
#
 sysname SSH Server
#
rsa peer-public-key rsakey001
 public-key-code begin
  308188
    028180
      B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB A443130F 7CDB95D8 4A4AE2F3
      D94A73D7 36FDFD5F 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B 40A35DE6
      2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5 1987178B 8C364D57 DD0AA24A A0C2F87F
      474C7931 A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2 171896FB 1FFC38CD
    0203
      010001
 public-key-code end
peer-public-key end
#
aaa
 local-user client001 password cipher %$%$S${AA4{(~(t-#&J%{$_Q,ulcf0!
`>I~Bk6~S&89Bb`rO.{rm%$%$
 local-user client001 privilege level 3
 local-user client001 service-type ssh
 local-user client002 password cipher %$%$Z~8xR1ice-hvVO->2jbQ#PG>B/"x@U
{|],CA:IPG9X^%FVMH%$%$
 local-user client002 privilege level 3
 local-user client002 service-type ssh
#
ssh user client002 assign rsa-key rsakey001
ssh user client002 authentication-type rsa
stelnet server enable
SSH server port 1025
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 5
 protocol inbound ssh
#
return
```

- Client001 configuration file

```
#
 sysname client001
#
ssh client first-time enable
#
return
```

- Client002 configuration file

```
#
 sysname client002
#
ssh client first-time enable
#
return
```

1.4.5 Common Configuration Errors

This section describes the common configuration errors and isolation methods.

1.4.5.1 Failing to Log In to the Telnet Server Through Telnet

Fault Description

The Telnet server fails to be logged in through Telnet.

Procedure

Step 1 Check whether the number of users who have logged in to the Telnet server reaches the upper limit.

Log in to the device through a console port. Run the **display users** command to check whether the current VTY channel is completely occupied. By default, a maximum number of five VTY channels are allowed. You can run the **display user-interface maximum-vty** command to check the maximum number of users allowed in the current VTY channel.

If the number of current users has reached the upper limit, run the **user-interface maximum-vty** 15 command to increase the maximum number of users allowed in the VTY channel to 15.

Step 2 Check whether an ACL has been configured on the VTY user interface of the device.

Run the **user-interface vty** command on the Telnet server to display the user interface view. Run the **display this** command to check whether an ACL has been configured on the VTY user interface. If yes, record the ACL number.

Run the **display acl** *acl-number* command on the Telnet server to check whether the Telnet client IP address is denied in the ACL. If yes, run the **undo rule** *rule-id* command in the ACL view to delete the deny rule, and then run the **rule permit source** *source-ip-address soucer-wildcard* command in the ACL view to permit the client IP address.

Step 3 Check the protocol configuration in the VTY user interface view.

Run the **user-interface vty** command on the Telnet server to display the user interface view. Run the **display this** command to check whether **protocol inbound** on the VTY user interface is set to **telnet** or **all**(By default, the system supports Telnet). If no, run the **protocol inbound** { **telnet** | **all** } command to enable Telnet users to connect to the device.

Step 4 Check whether login authentication is configured in the VTY user interface view.

- If the password authentication mode for login is configured in the VTY channel using the **authentication-mode password** command, you must enter the password upon login.

- If the AAA authentication mode is configured using the **authentication-mode aaa** command, you must run the **local-user** *user-name* **password** command to create a local AAA user.

----End

1.4.5.2 Failing to Log In to the SSH Server Through STelnet

Fault Description

The SSH server fails to be logged in through STelnet.

Procedure

Step 1 Check whether the SSH service is enabled on the SSH server.

Log in to the SSH server through STelnet. Run the **display ssh server status** command to check the SSH server configuration.

If the STelnet service is disabled, run the **stelnet server enable** command to enable the STelnet service on the SSH server.

Step 2 Check the protocol configuration in the VTY user interface view on the SSH server.

Run the **user-interface vty** command on the SSH server to display the user interface view. Run the **display this** command to check whether **protocol inbound** on the VTY user interface is set to **ssh** or **all**. If no, run the **protocol inbound** { **ssh** | **all** } command to enable STelnet users to connect to the device.

Step 3 Check whether the RSA public key is configured on the SSH server.

A local key pair must be configured when the device works as the SSH server.

Run the **display rsa local-key-pair public** command on the SSH server to check the current server key pair. If no information is displayed, the server key pair has not been configured. Run the **rsa local-key-pair create** command to create a key pair.

Step 4 Check whether an SSH user is configured on the SSH server.

Run the **display ssh user-information** command to view the configuration of the SSH user. If there is no configuration, run the **ssh user authentication-type** command in the system view to create an SSH user and configure the SSH user authentication mode.

Step 5 Check whether the number of users who have logged in to the SSH server reaches the upper limit.

Log in to the device through a console port. Run the **display users** command to check whether the current VTY channel is completely occupied. By default, a maximum number of five VTY channels are allowed. You can run the **display user-interface maximum-vty** command to check the maximum number of users allowed in the current VTY channel.

If the number of current users has reached the upper limit, run the **user-interface maximum-vty** 15 command to increase the maximum number of users allowed in the VTY channel to 15.

Step 6 Check whether an ACL is configured on the user interface of the SSH server.

Run the **user-interface vty** command on the SSH server to display the SSH user interface view. Run the **display this** command to check whether an ACL has been configured on the VTY user interface. If yes, record the ACL number.

Run the **display acl** *acl-number* command on the SSH server to check whether the SSH client IP address is denied in the ACL. If yes, run the **undo rule** *rule-id* command in the ACL view to delete the deny rule, and then run the **rule permit source** *source-ip-address soucer-wildcard* command in the ACL view to permit the client IP address.

Step 7 Check the SSH version on the SSH client and server.

Run the **display ssh server status** command on the SSH server to check the SSH version.

If the version is SSHv1, run the **ssh server compatible-ssh1x enable** command to configure the version compatibility function on the server.

Step 8 Check whether the first authentication function is enabled on the SSH client.

Run the **display this** command in the system view on the SSH client to check whether the first authentication function is enabled on the SSH client.

If no, an STelnet user fails to log in to the SSH server for the first time because verifying the RSA public key on the SSH server fails. Run the **ssh client first-time enable** command to enable the first authentication function on the SSH client.

----End

1.5 File Management

All files on the device are stored in storage devices and can be managed in multiple modes. The current device can function as a client to access files on other devices.

1.5.1 File System Overview

The file system manages storage devices and all files including configuration files and system software stored on them.

File System

The file system manages files and directories on storage devices. In the file system, users can create, delete, modify, and rename a file or a directory, and view contents of a file.

Storage Device

The device only supports the flash card.

Naming Rules for Files

A file name is a string of 1 to 64 case-sensitive characters. The file name formats are as follows:

- File name

  If the name of a file is in this format, the file is in the current working directory.

- Drive + Path + File name

  This file name format uniquely identifies a file in a specified path.

  In the format, **drive** indicates the storage device and can be set to **flash:**.

  In the file name, **path** indicates the directory and subdirectory. The directory name is case-insensitive. The space character and the following characters and cannot be used in the directory name: ~ * / \ : ' "

  The path can be an absolute path or relative path.

  - **flash:/my/test/** is an absolute path.
  - **selftest/** is related to the current working directory and indicates the **selftest** directory in the current working directory.

  For example, in the **dir flash:/my/test/mytest.txt** command, **flash:/my/test/** is an absolute path.

  To find the **mytest.txt** file from a directory related to the current working directory (**flash:/my/** for example), run the **dir test/mytest.txt** command.

  NOTE

  - In the file operation command format, **filename** indicates the file name.
  - In the file operation command format, **directory** indicates the path (**drive + path**).

1.5.2 File Management Modes

The device supports multiple file management modes. You can choose a proper file management mode based on service and security requirements.

Users can log in to a device or use the File Transfer Protocol (FTP), Trivial File Transfer Protocol (TFTP), Secure File Transfer Protocol (SFTP) mode to manage files.

Table 1-37 describes file management modes and their advantages and disadvantages.

Table 1-37 File management modes

Mode	Usage Scenario	Advantage	Disadvantage
Login to the device	In the scenario of managing storage devices, directories, and files, log in to the device through the console port, Telnet, or STelnet.This login mode is mandatory for storage device management.	You can log in to the device directly to manage storage devices, directories, and files.	Only files on the local device can be managed. File transfer is not supported.

Mode	Usage Scenario	Advantage	Disadvantage
FTP	The FTP mode is applicable to the file transfer scenario with low network security requirements. The FTP mode is widely used in version upgrade.	● The FTP mode is easy to configure and supports file transfer and operations on directories. ● The FTP mode supports file transfer between two file systems. ● The authorization and authentication functions are provided.	In FTP mode, data is transmitted in plain text, causing security risks.
TFTP	On the LAN of a lab, the TFTP mode can be used to load or upgrade versions online. The TFTP mode is applicable to the environment without complicated interactions between a client and a server.	● The memory usage in TFTP mode is less than that in FTP mode.	● In TFTP mode, the device can function only as a client. ● The TFTP mode supports only file transfer. ● In TFTP mode, data is transmitted in plain text, causing security risks, and no authorization or authentication function is provided.
SFTP	The SFTP mode is applicable to the scenario with high network security requirements. The SFTP mode is widely used in log download and file backup.	● Data is encrypted and protected. ● The SFTP mode supports file transfer and operations on directories.	Configurations are complicated.

The device can function as a server or client to manage files.

- When the device functions as a server, you can access the device on a terminal to manage files on the device and transfer files between the device and the terminal.
- When the device functions as a client, you can use the device to manage files on other devices and transfer files between the device and other devices.

NOTE

In TFTP mode, the device can function only as a client. In FTP, SFTP mode, the device can function both as a server and a client.

1.5.3 Local File Management

Users can use a terminal to log in to the device or use the FTP, SFTP mode to manage local files.

Context

NOTICE

When downloading files to the device or performing other operations on the device, ensure that the power supply of the device is workig properly; otherwise, the downloaded file or the file system may be damaged. As a result, the storage medium on the device may be damaged or the device cannot be properly started.

1.5.3.1 Logging In to the Device to Manage Files

Users can log in to the device through the console port, Telnet, or STelnet to manage storage devices, directories, and files. This login mode is mandatory for storage device management.

Pre-configuration Tasks

Before logging in to the device to manage files, complete the following tasks:

- Ensuring that routes are reachable between the terminal and the device.
- Ensuring that a user have logged in to the device using a terminal.

Configuration Process

After a user logs in to the device on a terminal, the user can perform operations on storage devices, directories, and files.

Users can perform the following operations in any sequence.

Procedure

- **Perform operations on directories.**

Table 1-38 Performing operations on directories

Operation	Command	Description
Display the current directory.	**pwd**	-
Change the current directory.	**cd** *directory*	-
Display files and subdirectories in a specified directory.	**dir** [**/all**] [*filename* | *directory*]	-

Operation	Command	Description
Create a directory.	**mkdir** *directory*	-
Delete a directory.	**rmdir** *directory*	● The directory to be deleted must be empty. ● A deleted directory and its files cannot be restored from the recycle bin.

- **Perform operations on files.**

Table 1-39 Performing operations on files

Operation	Command	Description
Display the file content.	**more** [**/binary**] *filename* [*offset*] [**all**]	-
Copy a file.	**copy** *source-filename destination-filename*	● Before copying a file, ensure that the storage space is sufficient for the file. ● If the destination file has the same name as an existing file, the system prompts you whether to overwrite the existing file.
Move a file.	**move** *source-filename destination-filename*	If the destination file has the same name as an existing file, the system prompts you whether to overwrite the existing file.
Rename a file.	**rename** *old-name new-name*	-
Compress a file.	**zip** *source-filename destination-filename*	-
Decompress a file.	**unzip** *source-filename destination-filename*	-
Delete a file.	**delete** [**/unreserved**] [**/force**] { *filename* | *devicename* }	This command cannot delete a directory. **NOTICE** In this command, **/unreserved** indicates that the file cannot be restored.

Operation	Command	Description
Restore a file.	**undelete** { *filename* | *devicename* }	If you run **delete** command without the **/unreserved** keyword, the file is moved to the recycle bin. You can run this command to restore the files in the recycle bin.
Remove a file from the recycle bin.	**reset recycle-bin** [*filename* | *devicename*]	To delete a file permanently, remove the file from the recycle bin.
Enter the system view.	**system-view**	To perform multiple operations at one time, run the **execute** *batch-filename* command in the system view. The batch file must be stored in the storage device first.
Execute a batch file.	**execute** *batch-filename*	

- **Perform operations on storage devices.**

  When the file system on a storage device fails, the terminal prompts the user to rectify the fault.

  When the file system fault cannot be rectified or the data on the storage device is unnecessary, you can format the storage device.

NOTICE

When a storage device is formatted, data on the storage device is cleared and cannot be restored. Therefore, you must format a storage device with caution.

Table 1-40 Performing operations on storage devices

Operation	Command	Description
Repair the storage device with the faulty file system.	**fixdisk** *drive*	If the system still reports the fault after this command is executed, the storage device is damaged.

- **Configure the notification mode of the file system.**

  When a user performs operations that may cause data loss or damage on a device, the system generates notifications or alarms. Users can configure the notification mode of the file system.

Table 1-41 Configuring the notification mode of the file system

Operation	Command	Description
Enter the system view.	**system-view**	-
Configure the notification mode of the file system.	**file prompt** { **alert** | **quiet** }	The default notification mode is alert. **NOTICE** If the notification mode is set to **quiet**, the system does not provide notifications when data is lost because of user misoperations such as deleting files. Therefore, this notification mode must be used with caution.

----End

1.5.3.2 Managing Files When the Device Functions as an FTP Server

Users can connect the local terminal to a remote device to manage files using FTP. FTP is widely used for file service operations such as version upgrade.

Pre-configuration Tasks

Before connecting to the FTP server to manage files, complete the following tasks:

- Ensuring that routes are reachable between the terminal and the device.
- Ensuring that the terminal functions as the FTP client.

Configuration Process

NOTE

The FTP protocol will bring risk to device security. The SFTP V2 mode is recommended.

Table 1-42 describes the procedure for managing files when the device functions as an FTP server.

Table 1-42 Managing files when the device functions as an FTP server

No.	Task	Description	Remarks
1	**Set FTP server parameters**	Configure FTP server parameters including the port number, source address, and timeout duration.	The three steps can be performed in any sequence.

No.	Task	Description	Remarks
2	**Configure local FTP user information**	Configure local FTP user information including the service type, user level, and authorized directory.	
3	**(Optional) Configure the FTP ACL**	Configure the ACL rule and FTP basic ACL, improving FTP access security.	
4	**Connect to the device using FTP**	Connect to the device using FTP on the terminal.	-

Default Parameter Settings

Table 1-43 Default parameter settings

Parameter	Default Value
FTP server function	Disabled
Listening port number	21
FTP user	No local user is created

Procedure

- **Set FTP server parameters.**

  Table 1-44 Setting FTP server parameters

Operation	Command	Description
Enter the system view.	**system-view**	-
(Optional) Specify a port number for the FTP server.	**ftp server port** *port-number*	The default port number is 21. If a new port number is configured, the FTP server disconnects from all FTP clients and uses the new port number to listen to connection requests. Attackers do not know the port number and cannot access the listening port of the FTP server.

Operation	Command	Description
Enable the FTP server function.	**ftp server enable**	By default, the FTP server function is disabled.
(Optional) Configure the source address of the FTP server.	**ftp server-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	After the source address of the FTP server is configured, incoming and outgoing packets are filtered, ensuring the device security. After the source address of the FTP server is configured, you must enter the source address to log in to the FTP server.
(Optional) Configure the timeout duration of the FTP server.	**ftp timeout** *minutes*	By default, the idle timeout duration is 30 minutes. During the timeout duration, if no operation is performed on the FTP server, the FTP client disconnects from the FTP server automatically.
(Optional) Specify physical interfaces on the FTP server to which clients can connect.	**ftp server permit interface** { *interface-type interface-number* }	By default, clients can connect to all the physical interfaces and BSS interfaces on the FTP server.

NOTE

- If the FTP service is enabled, the port number of the FTP service cannot be changed. To change the port number, run the **undo ftp server** command to disable the FTP service first.
- After operations on files are complete, run the **undo ftp server** to disable the FTP server function to ensure the device security.

- **Configure local FTP user information.**

  Before performing operations on files using FTP, configure the local user name and password, service type, and authorized directory on the FTP server.

  Table 1-45 Configuring local FTP user information

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the AAA view.	**aaa**	-

Operation	Command	Description
Configure the local user name and password.	**local-user** *user-name* **password cipher** *password*	By default, no local user exists in the system and anonymous FTP access is not supported. -
Configure the local user level.	**local-user** *user-name* **privilege level** *level*	**NOTE** The user level must be set to **3** or upper levels to ensure successful connection establishment.
Configure the service type for local users.	**local-user** *user-name* **service-type ftp**	By default, a local user can use any access type.
Configure authorized directory.	**local-user** *user-name* **ftp-directory** *directory*	By default, the FTP directory of a local user is empty. When multiple FTP users use the same authorized directory, you can use the **set default ftp-directory** *directory* command to configure a default directory for these FTP users. In this case, you do not need run the **local-user** *user-name* **ftp-directory** *directory* command to configure an authorized directory for each user.

- **(Optional) Configure the FTP ACL.**

  An ACL is composed of a list of rules such as the source address, destination address, and port number of packets. ACL rules are used to classify packets. After these rules are applied to routing devices, the routing devices determine the packets to be received and rejected.

  Users can configure a basic ACL to allow only specified clients to connect to the FTP server.

  NOTE

  The ACL rules are as follows:

  - Other devices that match the ACL rule can establish an FTP connection with the local device only when **permit** is used in the ACL rule.
  - When **deny** is used in the ACL rule, other devices that match the ACL rule cannot establish FTP connections with the local device.
  - When the ACL rule is configured but packets from other devices do not match the rule, other devices cannot establish FTP connections with the local device.
  - When the ACL contains no rule, any other devices can establish FTP connections with the local device.

Table 1-46 (Optional) Configuring the FTP ACL

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the ACL view.	**acl** [**number**] *acl-number*	**NOTE** FTP supports only basic ACLs (2000-2999).
Configure the ACL rule.	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **time-range** *time-name*] *	-
Return to the system view.	**quit**	-
Configure basic FTP ACLs.	**ftp acl** *acl-number*	-

- **Connect to the device using FTP.**

  Users can use the Windows CLI or third-party software to connect to the device from a terminal using FTP. The following describes how to connect to the device using the Windows CLI:

  - Run the **ftp** *ip-address* command to connect to the device using FTP.

    In the preceding command, *ip-address* indicates the IP address configured on the device. Routes between the terminal and the device are reachable.

  - Enter the user name and password as prompted and press **Enter**. If command prompt **ftp>** is displayed in the FTP client view, the user accesses the working directory on the FTP server. (The following information is only for reference.)

```
C:\Documents and Settings\Administrator> ftp 192.168.150.208
Connected to 192.168.150.208.
220 FTP service ready.
User(192.168.150.208:(none)):huawei
331 Password required for huawei.
Password:
230 User logged in.
ftp>
```

- **Run FTP commands to perform file-related operations.**

  After connecting to the FTP server, users can run FTP commands to perform file-related operations including performing operations on directories and files, configuring the file transfer mode, and viewing the online help about FTP commands.

  NOTE

  User rights are configured on the FTP server.

  Users can perform the following operations in any sequence.

Table 1-47 Running FTP commands to perform file-related operations

Operation	Command	Description
Change the working directory on the server.	**cd** *remote-directory*	-
Change the current working directory to its parent directory.	**cdup**	-
Display the working directory on the server.	**pwd**	-
Display or change the local working directory.	**lcd** [*local-directory*]	The **lcd** command displays the local working directory on the client, and the **pwd** command displays the working directory on the remote server.
Create a directory on the server.	**mkdir** *remote-directory*	The directory name can consist of letters and digits. The following special characters are forbidden: < > ? \ :
Delete a directory from the server.	**rmdir** *remote-directory*	-
Display information about the specified directory or file on the server.	**dir/ls** [*remote-filename* [*local-filename*]]	● The **ls** command displays only the directory or file name, and the **dir** command displays detailed directory or file information such as size and date when the directory or file is created. ● If no directory is specified in the command, the system searches for the file in user's authorized directories.
Delete a file from the server.	**delete** *remote-filename*	-
Upload a file.	**put** *local-filename* [*remote-filename*]	-
Download a file.	**get** *remote-filename* [*local-filename*]	-

Operation	Command	Description
Configure the file transfer mode is ASCII.	**ascii**	Either operation is feasible. ● The default file transfer mode is ASCII. ● The ASCII mode is used to transfer text files, and the binary mode is used to transfer programs, system software(such as files with name extension .cc, .bin, and .pat.), and database files.
Configure the file transfer mode is Binary.	**binary**	
Configure the data transmission mode is passive.	**passive**	Either operation is feasible. The default data transmission mode is active.
Configure the data transmission mode is active.	**undo passive**	
View the online help about FTP commands.	**remotehelp** [*command*]	-
Enable the verbose function.	**verbose**	After the verbose function is enabled, all FTP response messages are displayed on the FTP client.

- **(Optional) Change the login user.**

  The current user can switch to another user in the FTP client view. The new FTP connection is the same as that established by running the **ftp** command.

Operation	Command	Description
Change the current user in the FTP client view.	**user** *user-name* [*password*]	When the login user is switched to another user, the original user is disconnected from the FTP server.

- **Disconnect the FTP client from the FTP server.**

  Users can run different commands in the FTP client view to disconnect the FTP client from the FTP server.

Operation	Command	Description
Disconnect the FTP client from the FTP server and return to the user view.	**bye** or **quit**	Either operation is feasible.
Disconnect the FTP client from the FTP server and display the FTP client view.	**close** or **disconnect**	

----End

Checking the Configurations

- Run the **display ftp-server** command to check the FTP server configuration and status.
- Run the **display ftp-users** command to view information about the FTP users that log in to the FTP server.

1.5.3.3 Managing Files When the Device Functions as an SFTP Server

SFTP allows a terminal to connect to the remote device using SSH and ensures the security of data transfer during the system upgrading and log downloading processes.

Pre-configuration Tasks

Before connecting to the SFTP server to manage files, complete the following tasks:

- Ensuring that routes are reachable between the terminal and the device.
- The SSH client software has been installed on the terminal.

Configuration Process

NOTE

The SFTP V1 protocol will bring risk to device security. The SFTP V2 mode is recommended.

Table 1-48 describes the procedure for managing files when the device functions as an SFTP server.

Table 1-48 Managing files when the device functions as an SFTP server

No.	Task	Description	Remarks
1	**Set SFTP server parameters**	Generate local key pair, enable the SFTP server, and configure SFTP server parameters, including the listening port number, key pair updating time, SSH authentication timeout duration, and number of SSH authentication retries.	The three steps can be performed in any sequence.
2	**Configuring the VTY user interface for SSH users to log in to the device**	Configure the user authentication mode, SSH supporting, and other basic attributes on the VTY user interface.	
3	**Configure SSH user information**	Configure SSH user information including the SSH user creation, authentication mode.	
4	**Connect to the device using SFTP**	Connect to the device using the SSH client software on the terminal.	-

Default Parameter Settings

Table 1-49 Default parameter settings

Parameter	Default Value
SFTP server function	Disabled
Listening port number	22
Time for updating the key pair of the server	0, indicating the key pair of the server is never updated
SSH authentication timeout duration	60 seconds
Number of SSH authentication retries	3
SSH user	No SSH user is created

Procedure

- **Set SFTP server parameters.**

Table 1-50 Setting SFTP server parameters

Operation	Command	Description
Enter the system view.	**system-view**	-
Generate the local RSA key pair.	**rsa local-key-pair create**	- Run the **display rsa local-key-pair public** command to view the public key in the local RSA key pair. Configure the public key on the SSH server.
Enable the SFTP server function.	**sftp server enable**	By default, the SFTP server function is disabled.
(Optional) Configure the listening port number.	**ssh server port** *port-number*	By default, the listening port number is 22. If a new port number is configured, the SSH server disconnects from all SSH clients and uses the new port number to listen to connection requests. Attackers do not know the port number and cannot access the listening port of the SSH server.
(Optional) Configure the time for updating the key pair of the server.	**ssh server rekey-interval** *hours*	By default, the time for updating the key pair is 0. The value **0** indicates that the key pair is never updated. When the specified time is up, the key pair of the SSH server is updated, ensuring the server security.
(Optional) Configure the SSH authentication timeout duration.	**ssh server timeout** *seconds*	By default, the SSH authentication timeout duration is 60 seconds.
(Optional) Configure the number of SSH authentication retries.	**ssh server authentication-retries** *times*	By default, the number of SSH authentication retries is 3.
(Optional) Enable earlier versions to be compatible.	**ssh server compatible-ssh1x enable**	To forbid clients to access the device using the SSH1.3 to SSH1.99, run the **undo ssh server compatible-ssh1x enable** command to disable the compatibility with SSH1.X.

NOTE

- When the local RSA key pair is generated, two key pairs (a server key pair and a host key pair) are generated at the same time. Each key pair contains a public key and a private key. The length of the two key pairs ranges from 512 bits to 2048 bits.

- **Configuring the VTY user interface for SSH users to log in to the device.**

  SSH users use the VTY user interface to log in to the device using SFTP. Attributes of the VTY user interface must be configured.

Table 1-51 Configuring the VTY user interface for SSH users to log in to the device

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the VTY user interface view.	**user-interface vty** *first-ui-number* [*last-ui-number*]	-
Set the authentication mode of the VTY user interface to **AAA**.	**authentication-mode aaa**	By default, **password** authentication is used for console port login and **aaa** authentication is used for login on the VTY user interface. The authentication mode of the VTY user interface must be set to **AAA**. Otherwise, the **protocol inbound ssh** configuration fails and users cannot log in to the device.
Configure a VTY user interface that supports SSH.	**protocol inbound ssh**	By default, the VTY user interface supports Telnet. If no VTY user interface supports SSH, users cannot log in to the device.
Configure the user level.	**user privilege level** *level*	The user level must be set to **3** or upper levels to ensure successful connection establishment. If a local user uses password authentication, you can use the **local-user** *user-name* **privilege level** *level* command to set the level of the user to 3 or higher.

Operation	Command	Description
(Optional) Configure other attributes of the VTY user interface.	-	Other attributes of the VTY user interface are as follows: ● Maximum number of VTY user interfaces ● Restrictions on incoming calls and outgoing calls on the VTY user interface ● Terminal attributes on the VTY user interface For details, see **1.3.3 Configuring the VTY User Interface**.

- **Configure SSH user information.**

  Configure SSH user information including the authentication mode. Authentication modes including RSA, password, password-rsa, and all are supported.

  - The password-rsa authentication mode consists of the password and RSA authentication modes.
  - The all authentication mode indicates that SSH users only need to authenticated by password, or RSA.

  NOTE

  - If the SSH user uses the password authentication mode, only the SSH server needs to generate the RSA key. If the SSH user uses the RSA authentication mode, both the SSH server and client need to generate the RSA key and save and configure the public key of the peer end locally.

Table 1-52 Configuring SSH user information

Operation	Command	Description
Enter the system view.	**system-view**	-
Enter the AAA view.	**aaa**	-
Create SSH users.	**local-user** *user-name* **password cipher** *password*	-

Operation		Command	Description
Configure the SSH user level.		**local-user** *user-name* **privilege level** *level*	The local user level must be set to **3** or upper levels. This operation cannot be performed if the user level in the VTY interface view has been set to 3 or higher using the **user privilege level** *level* command.
Configure the service type for SSH users.		**local-user** *user-name* **service-type ssh**	-
Configure the authorized directory for SSH users.		**local-user** *user-name* **ftp-directory** *directory*	By default, the authorized directory for an SSH user is the root directory of the default storage device.
Return to the system view.		**quit**	-
Configure the authentication mode for SSH users.		**ssh user** *user-name* **authentication-type** { **password** | **rsa** | **password-rsa** | **all** }	-
If any one of the following authentication modes is configured for SSH users: ● rsa ● password-rsa	Enter the RSA public key view.	**rsa peer-public-key** *key-name*	-
	Enter the public key editing view.	**public-key-code begin**	-
	Edit the public key.	*hex-data*	● The public key must be a hexadecimal character string in the public key format generated by the SSH client software. For details, see SSH client software help. ● Copy and paste the RSA public key to the device that functions as the SSH server.

Operation		Command	Description
	Quit the public key editing view.	**public-key-code end**	-
	Return to the system view.	**peer-public-key end**	-
	Assign an RSA public key to an SSH user.	**ssh user** *user-name* **assign rsa-key** *key-name*	-

- **Connect to the device using SFTP.**

  The SSH client software supporting SFTP must be installed on the terminal to ensure that the terminal can connect to the device using SFTP to manage files. The following describes how to connect to the device using the OpenSSH and the Windows CLI.

  NOTE

  - For details how to install the OpenSSH, see the OpenSSH installation description.
  - To use the OpenSSH to connect to the device using SFTP, run the OpenSSH commands. For details about OpenSSH commands, see OpenSSH help.
  - Windows command prompt can identify commands supported by the OpenSSH only when the OpenSSH is installed on the terminal.

  Access the Windows CLI and run the commands supported by the OpenSSH to connect to the device using SFTP to manage files.

  If command prompt **sftp>** is displayed in the SFTP client view, the user accesses the working directory on the SFTP server. (The following information is only for reference.)

  ```
  C:\Documents and Settings\Administrator> sftp sftpuser@10.136.23.5
  Connecting to 10.136.23.5...
  The authenticity of host '10.136.23.5 (10.136.23.5)' can't be established.
  RSA key fingerprint is 46:b2:8a:52:88:42:41:d4:af:8f:4a:41:d9:b8:4f:ee.
  Are you sure you want to continue connecting (yes/no)? yes
  Warning: Permanently added '10.136.23.5' (RSA) to the list of known hosts.

  User Authentication
  Password:
  sftp>
  ```

- **Run SFTP commands to perform file-related operations.**

  In the SFTP client view, you can perform one or more file-related operations listed in **Table 1-53** in any sequence.

  NOTE

  In the SFTP client view, the system does not support predictive command input. Therefore, you must type commands in full name.

Table 1-53 Running SFTP commands to perform file-related operations

Operation	Command	Description
Change the user's current working directory.	**cd** [*remote-directory*]	-
Change the current working directory to its parent directory.	**cdup**	-
Display the user's current working directory.	**pwd**	-
Display the file list in a specified directory.	**dir/ls** [**-l** | **-a**] [*remote-directory*]	Outputs of the **dir** and **ls** commands are the same.
Delete directories from the server.	**rmdir** *remote-directory* &<1-10>	A maximum of 10 directories can be deleted at one time. Before running the **rmdir** command to delete directories, ensure that the directories do not contain any files. Otherwise, the deletion fails.
Create a directory on the server.	**mkdir** *remote-directory*	-
Change the name of a specified file on the server.	**rename** *old-name new-name*	-
Download a file from the remote server.	**get** *remote-filename* [*local-filename*]	-
Upload a local file to the remote server.	**put** *local-filename* [*remote-filename*]	-
Delete files from the server.	**remove** *remote-filename* &<1-10>	A maximum of 10 files can be deleted at one time.
View the help about SFTP commands.	**help** [**all** | *command-name*]	-

- **Disconnect the SFTP client from the SSH server.**

Operation	Command	Description
Disconnect the SFTP client from the SSH server.	**quit**	-

----End

Checking the Configurations

- Run the **display ssh user-information** [*username*] command to view SSH user information on the SSH server.
- Run the **display ssh server status** command to view the global configuration of the SSH server.
- Run the **display ssh server session** command to view the session information of the SSH client on the SSH server.

1.5.4 File Management on Other Devices

A device can function as a client to manage files on other devices in TFTP, FTP, SFTP mode.

Context

NOTICE

When downloading files to the device or performing other operations on the device, ensure that the power supply of the device is workig properly; otherwise, the downloaded file or the file system may be damaged. As a result, the storage medium on the device may be damaged or the device cannot be properly started.

1.5.4.1 Managing Files When the Device Functions as a TFTP Client

The device functions as a TFTP client and remotely connects to a TFTP server to upload and download files.

Pre-configuration Tasks

Before connecting to a device as a TFTP client to manage files, complete the following tasks:

- Ensuring that routes are reachable between the current device and the TFTP server.
- Obtaining the host name or IP address of the TFTP server and the directory for storing files to download or upload.

NOTE

You must choose a TFTP server with a long packet transmission timeout period, such as 3CDaemon and tftpd32; otherwise, file transfer may fail.

Configuration Process

NOTE

The TFTP protocol will bring risk to device security. The SFTP V2 mode is recommended.

Table 1-54 describes the procedure for managing files when the device functions as a TFTP client.

Table 1-54 Procedure for managing files when the device functions as a TFTP client

No.	Task	Description	Remarks
1	**(Optional) Configure the TFTP client source address**	Configure the TFTP client source address. The source address can be set to a source IP address or source interface information, ensuring communication security.	You can configure the TFTP client source address and TFTP ACL rule in any sequence.
2	**(Optional) Configure the TFTP ACL**	Configure the ACL rule and TFTP basic ACL, improving TFTP access security.	
3	**Run TFTP commands to upload or download files**	Upload and download files.	

Procedure

- **(Optional) Configure the TFTP client source address.**

  The source interface, for example, the loopback interface, must provide stable performance. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. After the client source address is configured as the source or destination address in the ACL rule, IP address differences and interface status impact are shielded, and incoming and outgoing packets are filtered.

  Table 1-55 Configuring the TFTP client source address

Operation	Command	Description
Enter the system view.	**system-view**	-
Configure the TFTP client source address.	**tftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	The TFTP client source address can be set to a source IP address or source interface information. If the source address is set to source interface information, configure an IP address for the interface for establishing TFTP connections.

- **(Optional) Configure the TFTP ACL.**

An ACL is composed of a list of rules such as the source address, destination address, and port number of packets. ACL rules are used to classify packets. After these rules are applied to routing devices, the routing devices determine the packets to be received and rejected.

An ACL can define multiple rules. ACLs are classified into basic ACLs, advanced ACLs, and Layer 2 ACLs.

NOTE

TFTP supports only the basic ACL whose number ranges from 2000 to 2999.

ACL rule:

- The local device can establish TFTP connections with other devices that match the ACL rule only when **permit** is used in the ACL rule.
- When **deny** is used in the ACL rule, the local device cannot establish TFTP connections with other devices that match the ACL rule.
- When the ACL rule is configured but packets from other devices do not match the rule, the local device cannot establish TFTP connections with other devices.
- When the ACL contains no rule, the local device can establish TFTP connections with any other devices.

Table 1-56 Configuring the TFTP ACL

Operation	Command	Description
Enter the system view.	**system-view**	-
Create an ACL and enter the ACL view.	**acl** [**number**] *acl-number*	By default, no ACL is created.
Configure the ACL rule.	**rule** [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **time-range** *time-name*] *	By default, no rule is configured for an ACL.
Return to the system view.	**quit**	-
Configure the TFTP ACL.	**tftp-server acl** *acl-number*	-

- **Run TFTP commands to upload or download files.**

Operation	Command	Description
Run the TFTP command to operate files.	**tftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* { **get** | **put** } *source-filename* [*destination-filename*]	- **get**: downloads a file. - **put**: uploads a file.

The source address or interface specified in the **tftp** command takes priority over that specified in the **tftp client-source** command. If you specify different source addresses or interfaces in the **tftp client-source** and **tftp** commands, the source address or interface

specified in the **tftp** command is used for communication. The source address or interface specified in the **tftp client-source** command applies to all TFTP connections. The source address or interface specified in the **tftp** command applies only to the current TFTP connection.

----End

Checking the Configuration

- Run the **display tftp-client** command to check source configurations of the TFTP client.
- Run the **display acl** { *acl-number* | **all** } command to check the ACL configurations of the TFTP client.

1.5.4.2 Managing Files When the Device Functions as an FTP Client

The device functions as an FTP client and remotely connects to an FTP server to transfer files and manage files and directories on the FTP server.

Pre-configuration Tasks

Before connecting to a device as an FTP client to manage files, complete the following tasks:

- Ensuring that routes are reachable between the current device and the FTP server.
- Obtaining the host name or IP address of the FTP server, FTP user name, and password.
- Obtaining the listening port number of the FTP server if the default listening port number is not used.

Configuration Process

NOTE

The FTP protocol will bring risk to device security. The SFTP V2 mode is recommended.

Table 1-57 describes the procedure for managing files when the device functions as an FTP client.

Table 1-57 Procedure for managing files when the device functions as an FTP client

No.	Task	Description	Remarks
1	**(Optional) Configure the FTP client source address**	Configure the FTP client source address. The source address can be set to a source IP address or source interface information, ensuring communication security.	Perform steps 1 and 2 in sequence. After the FTP connection is established, perform steps 3 and 4 in any sequence. To disconnect from the FTP server, perform step 5.
2	**Run FTP commands to connect to the FTP server**	-	

No.	Task	Description	Remarks
3	**Run FTP commands to perform file-related operations**	Run FTP commands to perform file-related operations including performing operations on directories and files, configuring the file transfer mode, and viewing the online help about FTP commands.	
4	**(Optional) Change the login user**	-	
5	**Disconnect the FTP client from the FTP server**	-	

Procedure

- **(Optional) Configure the FTP client source address.**

  The source interface, for example, the loopback interface, must provide stable performance. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. After the client source address is configured as the source or destination address in the ACL rule, IP address differences and interface status impact are shielded, and incoming and outgoing packets are filtered.

  The FTP client source address must be set to the loopback interface IP address or loopback interface information.

  Table 1-58 Configuring the FTP client source address

Operation	Command	Description
Enter the system view.	**system-view**	-
Configure the FTP client source address.	**ftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	You are advised to use the loopback interface IP address. When the FTP client source address is set to loopback interface information, configure an IP address for the loopback interface for establishing FTP connections.

- **Run FTP commands to connect to the FTP server.**

Run the corresponding command in the user view or FTP client view to connect to the FTP server.

Table 1-59 Running FTP commands to connect to the FTP server

Operation	Command	Description
Connect to the FTP server in the user view when the server IP address is an address.	**ftp** [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*]	Either operation is feasible. To enter the FTP client view, run the **ftp** command.
Connect to the FTP server in the FTP client view when the server IP address is an IPv4 address.	**ftp**	
	open [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*]	

NOTE

- The source address specified in the **ftp** command takes priority over that specified in the **ftp client-source** command on an IPv4 network. If you specify different source addresses in the **ftp client-source** and **ftp** commands, the source address specified in the **ftp** command is used for communication. The source address specified in the **ftp client-source** command applies to all TFTP connections. The source address specified in the **ftp** command applies only to the current TFTP connection.

Users must enter the correct user name and password to connect to the server.

- **Run FTP commands to perform file-related operations.**

  After connecting to the FTP server, users can run FTP commands to perform file-related operations including performing operations on directories and files, configuring the file transfer mode, and viewing the online help about FTP commands.

  NOTE

  User rights are configured on the FTP server.

  Users can perform the following operations in any sequence.

Table 1-60 Running FTP commands to perform file-related operations

Operation	Command	Description
Change the working directory on the server.	**cd** *remote-directory*	-

Operation	Command	Description
Change the current working directory to its parent directory.	**cdup**	-
Display the working directory on the server.	**pwd**	-
Display or change the local working directory.	**lcd** [*local-directory*]	The **lcd** command displays the local working directory on the client, and the **pwd** command displays the working directory on the remote server.
Create a directory on the server.	**mkdir** *remote-directory*	The directory name can consist of letters and digits. The following special characters are forbidden: < > ? \ :
Delete a directory from the server.	**rmdir** *remote-directory*	-
Display information about the specified directory or file on the server.	**dir/ls** [*remote-filename* [*local-filename*]]	● The **ls** command displays only the directory or file name, and the **dir** command displays detailed directory or file information such as size and date when the directory or file is created. ● If no directory is specified in the command, the system searches for the file in user's authorized directories.
Delete a file from the server.	**delete** *remote-filename*	-
Upload a file.	**put** *local-filename* [*remote-filename*]	-
Download a file.	**get** *remote-filename* [*local-filename*]	-
Configure the file transfer mode is ASCII.	**ascii**	Either operation is feasible. ● The default file transfer mode is ASCII. ● The ASCII mode is used to transfer text files, and the binary mode is used to transfer

Operation	Command	Description
Configure the file transfer mode is Binary.	**binary**	programs, system software(such as files with name extension .cc, .bin, and .pat.), and database files.
Configure the data transmission mode is passive.	**passive**	Either operation is feasible. The default data transmission mode is active.
Configure the data transmission mode is active.	**undo passive**	
View the online help about FTP commands.	**remotehelp** [*command*]	-
Enable the verbose function.	**verbose**	After the verbose function is enabled, all FTP response messages are displayed on the FTP client.

- **(Optional) Change the login user.**

  The current user can switch to another user in the FTP client view. The new FTP connection is the same as that established by running the **ftp** command.

Operation	Command	Description
Change the current user in the FTP client view.	**user** *user-name* [*password*]	When the login user is switched to another user, the original user is disconnected from the FTP server.

- **Disconnect the FTP client from the FTP server.**

  Users can run different commands in the FTP client view to disconnect the FTP client from the FTP server.

Operation	Command	Description
Disconnect the FTP client from the FTP server and return to the user view.	**bye** or **quit**	Either operation is feasible.

Operation	Command	Description
Disconnect the FTP client from the FTP server and display the FTP client view.	**close** or **disconnect**	

----End

Checking the Configurations

- Run the **display ftp-client** command to check source IP on the FTP client.

1.5.4.3 Managing Files When the Device Functions as an SFTP Client

SFTP is an SSH-based protocol that provides a secure file transfer capability. Configure the device as an SFTP client. The remote SSH server authenticates the SFTP client and encrypts data in bidirectional mode, ensuring secure file transfer and management of directories on the SSH server.

Pre-configuration Tasks

Before connecting to a device as an SFTP client to manage files, complete the following tasks:

- Ensuring that routes are reachable between the current device and the SSH server.
- Obtaining the host name or IP address of the SSH server and SSH user information.
- Obtaining the listening port number of the SSH server if the default listening port number is not used.

Configuration Process

Table 1-61 describes the procedure for managing files when the device functions as an SFTP client.

Table 1-61 Procedure for managing files when the device functions as an SFTP client

No.	Task	Description	Remarks
1	**(Optional) Configure the SFTP client source address**	Configure the SFTP client source address. The source address can be set to a source IP address or source interface information, ensuring communication security.	Steps 1, 2, and 3 can be performed in any sequence. Steps 4-6 need to be performed in sequence.

No.	Task	Description	Remarks
2	**Generate a local key pair**	Generate a local key pair and configure the public key on the SSH server. Perform this task only when the device logs in to the SSH server in RSA authentication mode.	
3	**Configure the initial SSH connection**	To configure the initial SSH connection, enable the initial authentication function or save the public key of the SSH server on the SSH client.	
4	**Run SFTP commands to connect to the SSH server**	-	
5	**Run SFTP commands to perform file-related operations**	Users can perform operations on directories and files on the SSH server and view the help about SFTP commands on the SFTP client.	
6	**Disconnect the SFTP client from the SSH server**	-	

Procedure

- **(Optional) Configure the SFTP client source address.**

  The source interface, for example, the loopback interface, must provide stable performance. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. After the client source address is configured as the source or destination address in the ACL rule, IP address differences and interface status impact are shielded, and incoming and outgoing packets are filtered.

  The SFTP client source address must be set to the loopback interface IP address or loopback interface information.

  Table 1-62 Configuring the SFTP client source address

Operation	Command	Description
Enter the system view.	**system-view**	-

Operation	Command	Description
Configure the SFTP client source address.	**sftp client-source** { **-a** *source-ip-address* | **-i** *interface-type interface-number* }	The default source address is 0.0.0.0. The client source address is set to the loopback interface IP address or loopback interface information.

- **Generate a local key pair.**

  NOTE

  Perform this step only when the device logs in to the SSH server in RSA authentication mode, not the password authentication mode.

  Table 1-63 Actions for generating a local key pair

Action	Command	Description
Enter the system view.	**system-view**	-
Generate the local RSA key pair.	**rsa local-key-pair create**	Run the **display rsa local-key-pair public** command to view the public key in the local RSA key pair. Configure the public key on the SSH server.

- **Configure the initial SSH connection.**

  By default, the client cannot connect to the SSH server because the client does not save the public key of the SSH server. Configure the initial SSH connection in either of the following ways:

  - Enable the initial authentication function on the client. With the function enabled, the client connects to the SSH server without checking the public key of the SSH server. When the initial SSH connection succeeds, the client automatically saves the public key of the SSH server for the next SSH connection. For details, see **Table 1-64**.
  - Save the public key of the SSH server on the client so that the client can authenticate the SSH server successfully. For details, see **Table 1-65**. This method ensures higher security but becomes more complex than the first method.

  Table 1-64 Actions for enabling first authentication for the SSH client

Action	Command	Description
Enter the system view.	**system-view**	-

Action	Command	Description
Enable first authentication for the SSH client.	**ssh client first-time enable**	By default, first authentication is disabled on the SSH client.

Table 1-65 Actions for configuring the SSH client to assign the RSA public key to the SSH server

Action	Command	Description
Enter the system view.	**system-view**	-
Enter the RSA public key view.	**rsa peer-public-key** *key-name*	-
Enter the public key editing view.	**public-key-code begin**	-
Edit the public key.	*hex-data*	● The public key must be a hexadecimal character string in the public key encoding format, and generated by the SSH server. ● After entering the public key editing view, you must enter the RSA public key that is generated on the server to the client.
Quit the public key editing view.	**public-key-code end**	● If no key public code hex-data is entered, the public key cannot be generated after you run this command. ● If the specified key *key-name* has been deleted, the system displays a message indicating that the key does not exist and returns to the system view directly when you run this command.
Return to the system view.	**peer-public-key end**	-

Action	Command	Description
Bind the RSA public key to the SSH server.	**ssh client** *servername* **assign rsa-key** *keyname*	If the SSH server public key saved in the SSH client does not take effect, run the **undo ssh client** *servername* **assign rsa-key** command to cancel the binding between the SSH server and RSA public key, and run this command to assign a new RSA public key to the SSH server.

- **Run SFTP commands to connect to the SSH server.**

  The SFTP client connect command has the same function with the STelnet client connect command. Both the clients can carry the source address, configure the keepalive function, and select a key exchange algorithm, an encryption algorithm, and an HMAC algorithm.

  Table 1-66 Running SFTP commands to connect to the SSH server

Operation	Command	Description
Enter the system view.	**system-view**	-
Access the server.	**sftp** [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port*] [[**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] | [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]	In most cases, only the IP address is specified in the commands.

  Command example:

  ```
  [Huawei] sftp 10.137.217.201
  ```

  When the SSH connection succeeds, **sftp-client>** is displayed, indicating the SFTP client view.

- **Run SFTP commands to perform file-related operations.**

  In the SFTP client view, you can perform one or more file-related operations listed in **Table 1-67** in any sequence.

  NOTE

  In the SFTP client view, the system does not support predictive command input. Therefore, you must type commands in full name.

Table 1-67 Running SFTP commands to perform file-related operations

Operation	Command	Description
Change the user's current working directory.	**cd** [*remote-directory*]	-
Change the current working directory to its parent directory.	**cdup**	-
Display the user's current working directory.	**pwd**	-
Display the file list in a specified directory.	**dir/ls** [**-l** | **-a**] [*remote-directory*]	Outputs of the **dir** and **ls** commands are the same.
Delete directories from the server.	**rmdir** *remote-directory* &<1-10>	A maximum of 10 directories can be deleted at one time. Before running the **rmdir** command to delete directories, ensure that the directories do not contain any files. Otherwise, the deletion fails.
Create a directory on the server.	**mkdir** *remote-directory*	-
Change the name of a specified file on the server.	**rename** *old-name new-name*	-
Download a file from the remote server.	**get** *remote-filename* [*local-filename*]	-
Upload a local file to the remote server.	**put** *local-filename* [*remote-filename*]	-
Delete files from the server.	**remove** *remote-filename* &<1-10>	A maximum of 10 files can be deleted at one time.
View the help about SFTP commands.	**help** [**all** | *command-name*]	-

- **Disconnect the SFTP client from the SSH server.**

Operation	Command	Description
Disconnect the SFTP client from the SSH server.	**quit**	-

----End

Checking the Configuration

- Run the **display sftp-client** command to check source IP of the SFTP client.

1.5.5 Configuration Examples

Examples of managing local files and files on other devices are provided.

1.5.5.1 Example of Logging In to the Device to Manage Files

Configuration Requirements

After logging in to the device through the console interface, Telnet, or STelnet, perform the following operations:

- View files and subdirectories in the current directory.
- Create the **test** directory, copy the **vrpcfg.zip** file to **test**, and rename **vrpcfg.zip** as **backup.zip**.
- View files in the **test** directory.

Procedure

Step 1 View files and subdirectories in the current directory.

```
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-           889  Mar 01 2012 14:41:56   private-data.txt
    1  -rw-         6,311  Feb 17 2012 14:05:04   backup.cfg
    2  -rw-         2,393  Mar 06 2012 17:20:10   vrpcfg.zip
    3  -rw-           812  Dec 12 2011 15:43:10   hostkey
    4  drw-             -  Mar 01 2012 14:41:46   compatible
    5  -rw-           540  Dec 12 2011 15:43:12   serverkey
...
6,144 KB total (5,372 KB free)
```

Step 2 Create the **test** directory, copy the **vrpcfg.zip** file to **test**, and rename **vrpcfg.zip** as **backup.zip**.

Create the **test** directory.

```
<Huawei> mkdir test
Info: Create directory flash:/test......Done
```

Copy the **vrpcfg.zip** file to **test** and rename **vrpcfg.zip** as **backup.zip**.

```
<Huawei> copy vrpcfg.zip flash:/test/backup.zip
Copy flash:/vrpcfg.zip to flash:/test/backup.zip?(y/n)[n]:y
100%  complete
Info: Copied file flash:/vrpcfg.zip to flash:/test/backup.zip...Done
```

NOTE

If no destination file name is specified, the destination file is set to the source file name by default.

Step 3 View files in the **test** directory.

Access the **test** directory.

```
<Huawei> cd test
```

View the current working directory.

```
<Huawei> pwd
flash:/test
```

View files in the **test** directory.

```
<Huawei> dir
Directory of flash:/test/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-          2,399  Mar 12 2012 11:16:44   backup.zip

6,144 KB total (2,973 KB free)
```

----End

Configuration File

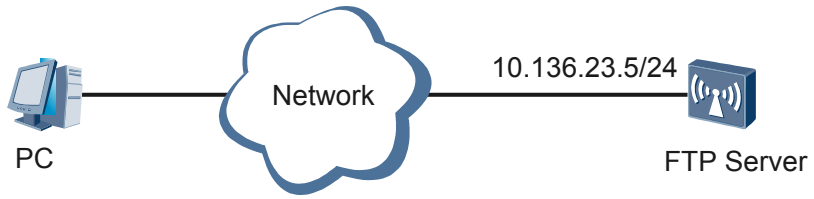
None

1.5.5.2 Example for Managing Files When the Device Functions as an FTP Server

Networking Requirements

As shown in **Figure 1-23**, routes between the PC and the device functioning as an FTP server are reachable. 10.136.23.5 is the IP address of VLANIF 1 on the FTP server. To transfer configuration files to the device, you must upload the files from the PC to the device functioning as the FTP server and save the device's configuration file **vrpcfg.zip** to the PC for backup.

Figure 1-23 Network for managing files when the device functions as an FTP server



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the FTP function and FTP user information including user name, password, user level, service type, and authorized directory on the FTP server.

2. Save the **vrpcfg.zip** file on the FTP server.
3. Connect to the FTP server on the PC.
4. Upload **newconfig.zip** to and download **vrpcfg.zip** from the FTP server.

Procedure

Step 1 Configure the FTP function and FTP user information on the FTP server.

```
<Huawei> system-view
[Huawei] ftp server enable
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: Succeeded in starting the FTP server
[Huawei] aaa
[Huawei-aaa] local-user admin1234 password cipher Helloworld@6789
[Huawei-aaa] local-user admin1234 privilege level 15
[Huawei-aaa] local-user admin1234 service-type ftp
[Huawei-aaa] local-user admin1234 ftp-directory flash:
[Huawei-aaa] quit
```

Step 2 Save the **vrpcfg.zip** file on the FTP server.

```
<Huawei> save
```

Step 3 Connect to the FTP server on the PC as the **admin1234** user whose password is **Helloworld@6789** and transfer files in binary mode.

Assume that the PC runs the Window XP operating system.

```
C:\Documents and Settings\Administrator> ftp 10.136.23.5
Connected to 10.136.23.5.
220 FTP service ready.
User (10.136.23.5:(none)): admin1234
331 Password required for admin1234.
Password:
230 User logged in.
ftp>
```

Step 4 Upload **newconfig.zip** to and download **vrpcfg.zip** from the FTP server.

Upload the **newconfig.zip** file to the FTP server.

```
ftp> put newconfig.zip
200 Port command okay.
150 Opening BINARY mode data connection for newconfig.zip
226 Transfer complete.
ftp: 832832 bytes sent in 136.34Seconds 560.79Kbytes/sec.
```

Download the **vrpcfg.zip** file.

```
ftp> get vrpcfg.zip
200 Port command okay.
150 Opening BINARY mode data connection for vrpcfg.zip.
226 Transfer complete.
ftp: 1257 bytes received in 0.03Seconds 40.55Kbytes/sec.
```

NOTE

The **devicesoft.cc** file to upload and the **vrpcfg.zip** file to download are stored in the local directory on the FTP client. Before uploading and downloading files, obtain the local directory on the client. The default FTP user's local directory on the Windows XP operating system is **C:\Documents and Settings\Administrator**.

Step 5 Verify the configuration.

Run the **dir** command on the FTP server to check the **newconfig.zip** file.

```
<Huawei> dir
Directory of flash:/
```

```
  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-             14  Mar 13 2012 14:13:38   back_time_a
    1  drw-              -  Mar 11 2012 00:58:54   logfile
    2  -rw-              4  Nov 17 2011 09:33:58   snmpnotilog.txt
    3  -rw-         11,238  Mar 12 2012 21:15:56   private-data.txt
    4  -rw-          1,257  Mar 12 2012 21:15:54   vrpcfg.zip
    5  -rw-             14  Mar 13 2012 14:13:38   back_time_b
    6  -rw-        832,832  Mar 13 2012 14:24:24   devicesoft.cc
    7  drw-              -  Oct 31 2011 10:20:28   sysdrv
    8  drw-              -  Feb 21 2012 17:16:36   compatible
    9  drw-              -  Feb 09 2012 14:20:10   selftest
   10  -rw-         19,174  Feb 20 2012 18:55:32   backup.cfg
   11  -rw-         23,496  Dec 15 2011 20:59:36   20111215.zip
   12  -rw-            588  Nov 04 2011 13:54:04   servercert.der
   13  -rw-            320  Nov 04 2011 13:54:26   serverkey.der
   14  drw-              -  Nov 04 2011 13:58:36   security
...
1,927,220 KB total (1,130,464 KB free)
```

Access the FTP user's local directory on the PC and check the **vrpcfg.zip** file.

----End

Configuration File

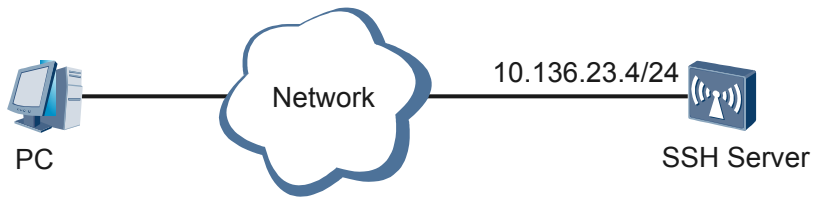
```
#
 ftp server enable
#
aaa
 local-user admin1234 password cipher %$%$k$Xg7H;w4HZP5nE4-E4(FcZQ%$%$
 local-user admin1234 privilege level 15
 local-user admin1234 ftp-directory flash:/
 local-user admin1234 service-type ftp
#
interface Vlanif1
 ip address 10.136.23.5 255.255.255.0
#
return
```

1.5.5.3 Example for Managing Files Using SFTP When the Device Functions as an SSH Server

Networking Requirements

As shown in **Figure 1-24**, routes between the PC and the device functioning as an SSH server are reachable. 10.136.23.4 is the management IP address on the SSH server. Configure the device as an SSH server so that the server can authenticate the client and encrypt data in bidirectional mode, preventing man-in-middle attacks and MAC/IP address spoofing to ensure secure file transfer.

Figure 1-24 Network for managing files using SFTP when the device functions as an SSH server



Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair and enable the SFTP server function on the SSH server so that the server and client can securely exchange data.
2. Configure the VTY user interface on the SSH server.
3. Configure SSH user information including the authentication mode, user name, and password.
4. Connect to the SSH server using the third-party software OpenSSH on the PC.

Procedure

Step 1 Generate a local key pair on the SSH server, and enable the SFTP server.

```
<Huawei> system-view
[Huawei] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
        will take a few minutes.
Input the bits in the modulus[default = 2048]:1024
Generating keys...
..........++++++++++++
.................++++++++++++
...++++++++
..........++++++++
[SSH Server] sftp server enable
```

Step 2 Configure the VTY user interface on the SSH server.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound all
[SSH Server-ui-vty0-4] quit
```

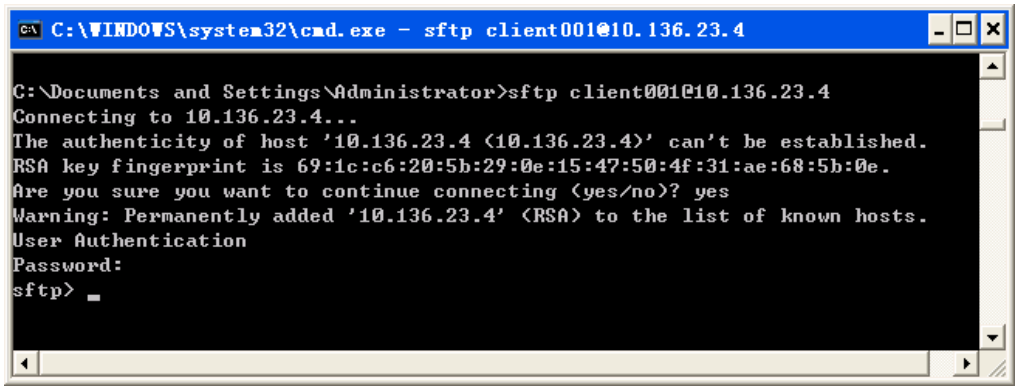
Step 3 Configure SSH user information including the authentication mode, user name, and password.

```
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password cipher Huawei@123
[SSH Server-aaa] local-user client001 privilege level 15
[SSH Server-aaa] local-user client001 service-type ssh
[SSH Server-aaa] quit
[SSH Server] ssh user client001 authentication-type password
```

Step 4 Connect to the SSH server using the third-party software OpenSSH on the PC.

The Windows CLI can identify OpenSSH commands only when the OpenSSH is installed on the PC.

Figure 1-25 Connecting to the SSH server



After connecting to the SSH server, the SFTP view is displayed. Users can run SFTP commands to perform file-related operations in the SFTP view.

----End

Configuration File

```
#
 sysname SSH Server
#
aaa
 local-user client001 password cipher %$%$k$Xg7H;w4HZP5nE4-E4(FcZQ%$%$
 local-user client001 privilege level 15
 local-user client001 service-type ssh
#
 sftp server enable
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound all
#
return
```

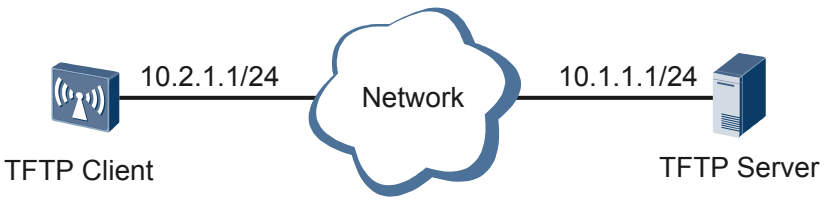
1.5.5.4 Example for Managing Files When the Device Functions as a TFTP Client

Networking Requirements

As shown in **Figure 1-26**, the remote device at 10.1.1.1/24 functions as the TFTP server. The device at 10.2.1.1/24 functions as the TFTP client. Routes between the device and the server are reachable.

You need to download configuration files from the TFTP server to the device and back up the current configuration file of the device to the TFTP server.

Figure 1-26 Network for managing files when the device functions as a TFTP client



Configuration Roadmap

The configuration roadmap is as follows:

1. Run the TFTP software on the TFTP server and configure the working directory.
2. Run TFTP commands to download **newconfig.zip** from and upload **vrpcfg.zip** to the TFTP server.

Procedure

Step 1 Run the TFTP software on the TFTP server and configure the working directory. (For details, see the appropriate third-party documentation.)

Step 2 Run TFTP commands to download **newconfig.zip** from and upload **vrpcfg.zip** to the TFTP server.

```
<Huawei> tftp 10.1.1.1 get newconfig.zip
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...
/100%
 93832832 bytes received in 271 seconds.
TFTP: Downloading the file successfully.
Now begins to save file, please wait......
Info: Transfer file in binary mode.
<Huawei> tftp 10.1.1.1 put vrpcfg.zip
Info: Transfer file in binary mode.
Uploading the file to the remote TFTP server. Please wait...
 100%
TFTP: Uploading the file successfully.
 2233264 bytes send in 57 seconds.
```

Step 3 Verify the configuration.

Run the **dir** command on the TFTP client to check the **newconfig.zip** file.

```
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-             14  Mar 13 2012 14:13:38   back_time_a
    1  drw-              -  Mar 11 2012 00:58:54   logfile
    2  -rw-              4  Nov 17 2011 09:33:58   snmpnotilog.txt
    3  -rw-         11,238  Mar 12 2012 21:15:56   private-data.txt
    4  -rw-          7,717  Mar 12 2012 21:15:54   vrpcfg.zip
    5  -rw-             14  Mar 13 2012 14:13:38   back_time_b
    6  -rw-        832,832  Mar 13 2012 14:24:24   newconfig.zip
    7  drw-              -  Oct 31 2011 10:20:28   sysdrv
    8  drw-              -  Feb 21 2012 17:16:36   compatible
    9  drw-              -  Feb 09 2012 14:20:10   selftest
   10  -rw-         19,174  Feb 20 2012 18:55:32   backup.cfg
   11  -rw-         43,496  Dec 15 2011 20:59:36   20111215.zip
   12  -rw-            588  Nov 04 2011 13:54:04   servercert.der
   13  -rw-            320  Nov 04 2011 13:54:26   serverkey.der
   14  drw-              -  Nov 04 2011 13:58:36   security
...
6,144 KB total (5,196 KB free)
```

Access the working directory on the TFTP server and check the **vrpcfg.zip** file.

----End

Configuration File

None

1.5.5.5 Example for Managing Files When the Device Functions as an FTP Client

Networking Requirements

As shown in **Figure 1-27**, the remote device at 10.1.1.1/24 functions as the FTP server. The device at 10.2.1.1/24 functions as the FTP client. Routes between the device and the server are reachable.

You need to download configuration files from the FTP server to the device and back up the current configuration file of the device to the FTP server.

Figure 1-27 Network for managing files when the device functions as an FTP client

Configuration Roadmap

The configuration roadmap is as follows:

1. Run the FTP software on the FTP server and configure FTP user information.
2. Connect to the FTP server.
3. Run FTP commands to download **newconfig.zip** from and upload **vrpcfg.zip** to the FTP server.

Procedure

Step 1 Run the FTP software on the FTP server and configure FTP user information. (For details, see the appropriate third-party documentation.)

Step 2 Connect to the FTP server.

```
<Huawei> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.

[Huawei-ftp]
```

Step 3 Run FTP commands to download **newconfig.zip** from and upload **vrpcfg.zip** to the FTP server.

```
[Huawei-ftp] get newconfig.zip
[Huawei-ftp] put vrpcfg.zip
[Huawei-ftp] quit
```

Step 4 Verify the configuration.

Run the **dir** command on the FTP client to check the **newconfig.zip** file.

```
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-             14  Mar 13 2012 14:13:38   back_time_a
    1  drw-              -  Mar 11 2012 00:58:54   logfile
    2  -rw-              4  Nov 17 2011 09:33:58   snmpnotilog.txt
    3  -rw-         11,238  Mar 12 2012 21:15:56   private-data.txt
    4  -rw-          7,717  Mar 12 2012 21:15:54   vrpcfg.zip
    5  -rw-             14  Mar 13 2012 14:13:38   back_time_b
    6  -rw-     832,832  Mar 13 2012 14:24:24   newconfig.zip
    7  drw-              -  Oct 31 2011 10:20:28   sysdrv
    8  drw-              -  Feb 21 2012 17:16:36   compatible
    9  drw-              -  Feb 09 2012 14:20:10   selftest
   10  -rw-         19,174  Feb 20 2012 18:55:32   backup.cfg
   11  -rw-         43,496  Dec 15 2011 20:59:36   20111215.zip
   12  -rw-            588  Nov 04 2011 13:54:04   servercert.der
   13  -rw-            320  Nov 04 2011 13:54:26   serverkey.der
   14  drw-              -  Nov 04 2011 13:58:36   security
...
6,144 KB total (5,196 KB free)
```

Access the working directory on the FTP server and check the **vrpcfg.zip** file.

----End

Configuration File

None

1.5.5.6 Example for Accessing Other Device Files Through SFTP (in Password Authentication Mode)

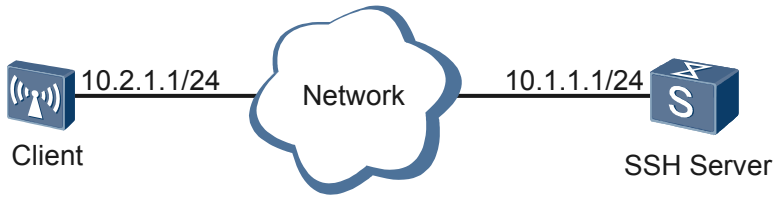
Networking Requirements

SSH guarantees secure file transfer on a traditional insecure network by authenticating the client and encrypting data in bidirectional mode. In SFTP mode, the client can securely connect to the SSH server and transfer files.

As shown in **Figure 1-28**, the routes between the SSH server and client are reachable. All devices mentioned in this example are Huawei devices.

It is required that the client should connect to the SSH server in password authentication mode to ensure secure access to files on the server.

Figure 1-28 Networking diagram of accessing other device files through SFTP



Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair on the SSH server and enable the SFTP server function to implement secure data exchange between the server and client.
2. Configure the user **client** on the SSH server to log in to the SSH server in password authentication mode.
3. Enable the user to log in to the SSH server through SFTP and access the files on the server.

Procedure

Step 1 Generate a local key pair on the SSH server and enable the SFTP server function.

```
<Quidway> system-view
[Quidway] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       it will take a few minutes.
Input the bits in the modulus[default = 2048]:1024
Generating keys...
..........+++++++++++
.................+++++++++++
...++++++++
..........++++++++
[SSH Server] sftp server enable
```

Step 2 Create an SSH user on the server.

Configure the VTY user interface.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound all
[SSH Server-ui-vty0-4] user privilege level 15
[SSH Server-ui-vty0-4] quit
```

Create an SSH user named **client**. Configure the password authentication mode for the user and set the password to **huawei@123**.

```
[SSH Server] aaa
[SSH Server-aaa] local-user client password cipher huawei@123
[SSH Server-aaa] local-user client service-type ssh
[SSH Server-aaa] quit
[SSH Server] ssh user client authentication-type password
```

Step 3 Connect the SFTP client to the SSH server.

Enable the first authentication function on the SSH client upon the first login.

Enable the first authentication function for Client.

```
<Huawei> system-view
[Huawei] sysname client
[client] ssh client first-time enable
```

Log in to the SSH server from Client in password authentication mode.

```
<client> system-view
[client] sftp 10.1.1.1
```

```
Please input the username: client
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it?[Y/N]:y
Save the server's public key?[Y/N]:y
The server's public key will be saved with the name 10.1.1.1. Please wait.
..

Enter password:
<sftp-client>
```

Step 4 Verify the configuration.

After the configuration, run the **display ssh server status** and **display ssh server session** commands on the SSH server. You can find that the SFTP service has been enabled and the SFTP client has connected to the SSH server. You can run the **display ssh user-information** command to check information about the SSH users on the server.

Check the status of the SSH server.

```
[SSH Server] display ssh server status
 SSH version                          :1.99
 SSH connection timeout               :60 seconds
 SSH server key generating interval   :0 hours
 SSH Authentication retries           :3 times
 SFTP Server                          :Enable
 Stelnet server                       :Disable
```

Check the SSH server connections.

```
[SSH Server] display ssh server session
-------------------------------------------------------------------------
 Conn    Ver   Encry     State  Auth-type        Username
 -------------------------------------------------------------------------
 VTY 1  2.0   AES       run    password         client
```

Check information about SSH users.

```
[SSH Server] display ssh user-information
 ------------------------------------------------------------------------------
 Username         Auth-type          User-public-key-name
 ------------------------------------------------------------------------------
 client           password           null
 ------------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file on the SSH server

```
#
 sysname SSH Server
#
aaa
 local-user client password cipher %$%$c|-D8KO4/,B[(FR.r!LHg]TK%$%$
 local-user client service-type ssh
#
 sftp server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
 protocol inbound all
```

```
#
return
```

- Configuration file on the SSH client

```
#
 sysname client
#
ssh client first-time enable
#
return
```

1.5.5.7 Example for Accessing Other Device Files Through SFTP (in RSA Authentication Mode)

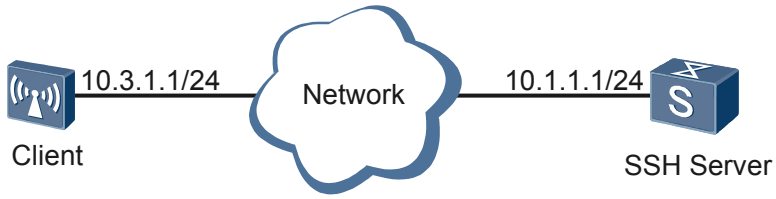
Networking Requirements

SSH guarantees secure file transfer on a traditional insecure network by authenticating the client and encrypting data in bidirectional mode. In SFTP mode, the client can securely connect to the SSH server and transfer files.

As shown in **Figure 1-29**, the routes between the SSH server and client are reachable. Huawei device is used as the SSH server in this example.

It is required that the client should connect to the SSH server in RSA authentication mode to ensure secure access to files on the server.

Figure 1-29 Networking diagram of accessing other device files through SFTP



Configuration Roadmap

The configuration roadmap is as follows:

1. Generate a local key pair on the SSH server and enable the SFTP server function to implement secure data exchange between the server and client.
2. Configure the user **client** on the SSH server to log in to the SSH server in RSA authentication mode.
3. Generate a local key pair on the client and configure the RSA public key generated on the client to the SSH server, which implements authentication on the client when the user logs in to the server from the client.
4. Enable the user **client** to log in to the SSH server through SFTP and access the files on the server.

Procedure

Step 1 Generate a local key pair on the SSH server and enable the SFTP server function.

```
<Quidway> system-view
[Quidway] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 2048]:1024
Generating keys...
..........++++++++++++
.................++++++++++++
...++++++++
..........++++++++
[SSH Server] sftp server enable
```

Step 2 Create an SSH user on the server.

Configure the VTY user interface.

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound all
[SSH Server-ui-vty0-4] user privilege level 15
[SSH Server-ui-vty0-4] quit
```

Create an SSH user named **client** and configure the RSA authentication mode for the user.

```
[SSH Server] aaa
[SSH Server-aaa] local-user client password cipher huawei@123
[SSH Server-aaa] local-user client service-type ssh
[SSH Server-aaa] quit
[SSH Server] ssh user client authentication-type rsa
```

Step 3 Generate a local key pair on the client and configure the RSA public key generated on the client to the SSH server.

Configure the client to generate a local key pair.

```
<Huawei> system-view
[Huawei] sysname client
[client] rsa local-key-pair create
The key name will be: Host
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Input the bits in the modulus[default = 2048]:1024
Generating keys...
..........++++++++++++
.................++++++++++++
...++++++++
..........++++++++
```

Check the RSA public key of the client.

```
[client] display rsa local-key-pair public

=====================================================
Time of Key pair created: 2012-08-25 15:17:31+00:00
Key name: Host
Key type: RSA encryption Key
=====================================================
Key code:
3048
```

```
  0241
    D6AA0DCB 11814574 D6894E48 C0D43CD4 31311082
    48A580C1 E6CC295C 8D00E1B0 85E02EC1 32D01F46
    EB051AA5 C5A96187 9BE4EAD2 5229D981 46107035
    D3050A97 57
  0203
    010001

=====================================================
Time of Key pair created: 2012-08-25 15:17:44+00:00
Key name: Server
Key type: RSA encryption Key
=====================================================
Key code:
3067
  0260
    B98B5088 7A44A21E 80C929DF 23F8FF16 DF7F6F06
    23B69CAA C3A2CE11 4F37F7D4 E8C56682 A9DB6705
    23C69B6A 5C5D9312 72E93890 D0861237 EC6468A0
    96AEB062 2B4874BB 57F8A69E 30003C61 9B37906C
    1C0E4C09 91C57F94 AECD5005 F7AC2281
  0203
    010001
```

Configure the RSA public key generated on the client to the SSH server. The **display** command output in bold indicates the RSA public key generated. Copy the key to the server side.

```
[SSH Server] rsa peer-public-key rsakey001
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.
[SSH Server-rsa-public-key] public-key-code begin
Enter "RSA key code" view, return last view with "public-key-code end".
[SSH Server-rsa-key-code] 3048
[SSH Server-rsa-key-code] 0241
[SSH Server-rsa-key-code] D6AA0DCB 11814574 D6894E48 C0D43CD4 31311082
[SSH Server-rsa-key-code] 48A580C1 E6CC295C 8D00E1B0 85E02EC1 32D01F46
[SSH Server-rsa-key-code] EB051AA5 C5A96187 9BE4EAD2 5229D981 46107035
[SSH Server-rsa-key-code] D3050A97 57
[SSH Server-rsa-key-code] 0203
[SSH Server-rsa-key-code] 010001
[SSH Server-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

Bind the RSA public key of the SSH client to the SSH user **client**.

```
[SSH Server] ssh user client assign rsa-key rsakey001
```

Step 4 Connect the SFTP client to the SSH server.

Enable the first authentication function for the SFTP client.

```
[client] ssh client first-time enable
```

Log in to the SSH server from the SFTP client in RSA authentication mode.

```
<client> system-view
[client] sftp 10.1.1.1
Please input the username: client
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it? [Y/N] :y
Save the server's public key? [Y/N] :y
The server's public key will be saved with the name 10.1.1.1. Please wait.
..

sftp-client>
```

Step 5 Verify the configuration.

After the configuration, run the **display ssh server status** and **display ssh server session** commands on the SSH server. You can find that the SFTP service has been enabled and the SFTP client has connected to the SSH server. You can run the **display ssh user-information** command to check information about the SSH users on the server.

Check the status of the SSH server.

```
[SSH Server] display ssh server status
 SSH version                          :1.99
 SSH connection timeout               :60 seconds
 SSH server key generating interval   :0 hours
 SSH Authentication retries           :3 times
 SFTP Server                          :Enable
 Stelnet server                       :Disable
```

Check the SSH server connections.

```
[SSH Server] display ssh server session
-------------------------------------------------------------------------
 Conn   Ver   Encry     State  Auth-type        Username
 -------------------------------------------------------------------------
 VTY 2  2.0   AES       run    rsa              client
 -------------------------------------------------------------------------
```

Check information about SSH users.

```
[SSH Server] display ssh user-information
 ------------------------------------------------------------------------------
 Username         Auth-type          User-public-key-name
 ------------------------------------------------------------------------------
 client           rsa                rsakey001
 ------------------------------------------------------------------------------
```

----End

Configuration File

- Configuration file on the SSH server

```
#
 sysname SSH Server
#
 rsa peer-public-key rsakey001
  public-key-code begin
    3048
      0241
        D6AA0DCB 11814574 D6894E48 C0D43CD4 31311082 48A580C1 E6CC295C 8D00E1B0
        85E02EC1 32D01F46 EB051AA5 C5A96187 9BE4EAD2 5229D981 46107035 D3050A97
        57
      0203
        010001
  public-key-code end
 peer-public-key end
#
aaa
 local-user client password cipher %$%$4var7p!aM*ULpu4#T=@-30'{%$%$
 local-user client service-type ssh
#
 ssh user client assign rsa-key rsakey001
 ssh user client authentication-type rsa
 sftp server enable
#
user-interface vty 0 4
 authentication-mode aaa
```

```
 user privilege level 15
 protocol inbound all
#
return
```

- Configuration file on the SSH client

```
#
 sysname client
#
ssh client first-time enable
#
return
```

1.5.6 Common Configuration Errors

This topic describes faults in logging in to the FTP server and uploading files to the FTP server.

1.5.6.1 Fault in Logging in to the FTP Server

Cause Analysis

- The FTP server is not running.
- The listening port number of the FTP server is not the default one, and no port number is specified when you log in to the FTP server.
- The authentication information, authorized directory, and user level of the FTP user are not configured.
- The number of online FTP users who have logged in to the FTP server reaches the upper threshold 5.
- An ACL is configured on the FTP server, and the FTP client IP address is not specified in the ACL.

Procedure

Step 1 Check whether the FTP server is running properly.

Run the **display ftp-server** command in any view to check the FTP server status.

- The following information indicates that the FTP server is not running:

```
<Huawei> display ftp-server
Info: The FTP server is already disabled
```

Run the **ftp server enable** command in the system view to start the FTP server.

```
<Huawei> system-view
[Huawei] ftp server enable
Warning: FTP is not a secure protocol, and it is recommended to use
SFTP.
Info: Succeeded in starting the FTP server
```

- The following information indicates that the FTP server is running properly:

```
<Huawei> display ftp-server
   FTP server is running
   Max user number                5
   User count                     0
   Timeout value(in minute)       30
   Listening port                 21
   Acl number                     0
   FTP server's source address    0.0.0.0
```

Step 2 Check whether the listening port number of the FTP server is the default port number 21.

1. Run the **display tcp status** command in any view to check the current TCP port listening status.

```
<Huawei> display tcp status
TCPCB     Tid/Soid Local Add:port         Foreign Add:port       VPNID  State
2a67f47c  6  /1    0.0.0.0:21            0.0.0.0:0              23553
Listening
2b72e6b8  115/4    0.0.0.0:22             0.0.0.0:0              23553
Listening
3265e270  115/1    0.0.0.0:23             0.0.0.0:0              23553
Listening
2a6886ec  115/23   10.137.129.27:23       10.138.77.43:4053      0
Establish
ed
2a680aac  115/14   10.137.129.27:23       10.138.80.193:1525     0
Establish
ed
2a68799c  115/20   10.137.129.27:23       10.138.80.202:3589     0
Establish
ed
```

2. Run the **display ftp-server** command in any view to check the listening port number of the FTP server.

```
<Huawei> display ftp-server
   FTP server is running
   Max user number                5
   User count                     0
   Timeout value(in minute)       30
   Listening port              21
   Acl number                     0
   FTP server's source address    0.0.0.0
```

If the listening port number is not 21, run the **ftp server port** command to set the listening port number to 21.

```
<Huawei> system-view
[Huawei] undo ftp server
Info: Succeeded in closing the FTP server.
[Huawei] ftp server port 21
[Huawei] ftp server enable
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: Succeeded in starting the FTP server
```

Alternatively, enter the port number configured on the server when you set up an FTP connection on the FTP client.

Step 3 Check whether the authentication information, authorized directory, and user level of the FTP user are correctly configured.

The FTP user name, password, authorized directory, and user level must be configured. If the FTP authorized directory and user level are not configured, login fails.

1. Run the **aaa** command to enter the AAA view.
2. Run the **local-user** *user-name* **password cipher** *password* command to configure the local FTP user name and password.
3. Run the **local-user** *user-name* **ftp-directory** *directory* command to specify an FTP authorized directory for the FTP user.
4. Run the **local-user** *user-name* **privilege level** *level* command to set the FTP user level. The user level must be set to **3** or upper levels to ensure successful connection establishment.

The service type is optional. By default, the system supports all service types. If you set the **service-type** parameter, only the service types that you set are available to FTP user.

Run the **local-user** *user-name* **service-type ftp** command to set the service types for the FTP user.

Step 4 Check whether the number of online FTP users who have logged in to the FTP server reaches the upper threshold.

Run the **display ftp-users** command to check the number of online FTP users.

Step 5 Check the ACL rule on the FTP server.

Run the **display ftp-server** command to check the ACL rule on the FTP server.

If an ACL is configured on the FTP server, only IP addresses specified in the ACL can log in to the FTP server.

----End

1.5.6.2 Failure in Uploading Files to the FTP Server

Cause Analysis

- The FTP source or destination directory name consists of unsupported characters.
- Space of the FTP root directory is insufficient.

Procedure

Step 1 Check whether the FTP source and destination directory names consist of unsupported characters.

The following characters and spaces are forbidden: ~ */ \ : ' "

If the directory names consist of any unsupported characters, modify the directory names.

Step 2 Check whether space of the FTP root directory is insufficient.

Run the **dir** command on the FTP server to check the free space of the FTP root directory.

If the space of the FTP root directory is insufficient, run the **delete /unreserved** command in the user view to delete unnecessary files.

----End

1.6 Configuring System Startup

When the device is powered on, system software starts and configuration files are loaded. To ensure smooth running of the device, manage system software and configuration files efficiently.

1.6.1 System Startup Overview

The system loads the system software and configuration file during a startup. If a patch file is specified for next startup, the system also loads the specified patch file.

System startup scenarios are as follows:

- Version upgrade: Upgrade the system software to a later version.

  To add new features, optimize existing features, or solve problems in the current version, you need to upgrade the device. To upgrade the device, load the upgrade system software and restart the device.

- Version rollback: Degrade the software to an earlier version.

  If an error occurs after the upgrade, perform version rollback to restore normal service operating. You need to load earlier version system software and restart the device.

- First startup: When a new device is deployed on a network, you can load an existing configuration file on the device to meet user needs.

  A new device contains only factory configurations. To connect a new device to the network and deploy services on it, you have to spend a lot of time on device configuration. To save time on device configuration, specify a configuration file that meets user needs for the device and restart the device.

- Patch update: Specify the patch file to be loaded after an upgrade.

  You can specify a new patch file when upgrading the device. The patch takes effect immediately when the upgrade is complete.

NOTE

- The upgrade of a device is closely related to the released software versions. The corresponding upgrade guide is released with each new version and you can upgrade the device according to the guide. To obtain the upgrade guides, visit **http://support.huawei.com/enterprise** and download the upgrade guide based on the product name and version.
- For details about commands used for device upgrade, see "Basic Configurations Commands - Upgrade Commands" in the *Huawei Wireless Access Points Command Reference*.

System Software

The device software includes Boot software and system software. After the device is powered on, it runs the Boot software to initialize the hardware. Then the device runs the system software. The system software provides drivers and adaptation functions for hardware, and offers services features. The Boot software and system software are prerequisite for device startup and operation, providing support, management, and services for the device.

A device upgrade includes Boot software upgrade and system software upgrade.

NOTE

The Boot software is included in the system software package of the device. The Boot software is automatically upgraded in system software upgrade.

Configuration File

A configuration file is a collection of command lines. The current configurations are saved in configuration files, and continue to take effect after the device restarts. You can view configurations in configuration files or upload the files to other devices to implement batch configuration.

A configuration file is in the text format and meets the following requirements:

- The configuration file saves configuration commands.
- Only non-default parameters are stored in the configuration file, which saves the space.

- The commands used in the same command view form a section. Sections are separated by blank lines or comment lines beginning with comment signs (#). There can be one or multiple blank or comment lines.
- Sections are arranged in the order of global configurations, interface-based configurations, protocol configurations, and user interface configurations.
- The configuration file name extension must be .cfg or .zip. In addition, the configuration file must be saved to the root directory of the storage device.

The following table describes the factory configuration, configuration file and current configuration.

Concept	Description	Command
Factory configuration	The device is delivered with basic configurations so that it can start and work properly when there is no configuration file or the configuration file is lost or damaged. These configurations are called factory configurations.	-
Configuration file	When the device is powered on, the device reads the configuration file from the default directory to boot the system. Therefore, the configuration in the file is called the initial configuration. If no configuration file is stored in the default directory, the device uses the default parameters for initialization. By default, the device uses the factory configuration for initialization.	- Run the **display startup** command to check the current and next startup configuration files. - Run the **display saved-configuration** command to check the configuration file for next startup.
Current configuration	The configurations that are valid during the device running are called current configurations.	Run the **display current-configuration** command to check the current configuration.

If you modify the current configuration and want to use the modified configuration as the next startup configuration, run the **save** command to save the new configuration to the default storage device.

NOTE

If a command in incomplete form is configured, the system saves the command to the configuration file in its complete form, which may cause the command to have more than 510 characters. (The maximum length of a command supported by the system is 510 characters.) The incomplete command cannot be recovered after the system restarts.

Patch File

A patch is a kind of software compatible with the system software. It is used to remove a few issues in the software that need to be solved immediately. Patches can also fix errors or improve

adaptation of the system software. For example, patches can fix defects of the system and optimize some functions to meet service requirements.

The patches are released in patch files. A patch file may contain one or more patches with different functions. When patch files are loaded from the storage device to the patch area in the memory, they are assigned unique sequence number for users to identify, manage, and operate the patches.

Patch classification

According to impact on services, patches can be classified into hot patch and cold patch.

- Hot patch (HP): The services are not interrupted when the HP is loaded and activated, which reduces upgrade costs and eliminates upgrade risks.
- Cold Patch (CP): You must restart the device for the CP to take effect. Services are interrupted during the restart.

According to patch dependency, patches can be classified into incremental and non-incremental patches.

- An incremental patch is dependent on previous patches. A new patch file contains all the patch information in the previous patch file. You can install the patch file without uninstalling the original patch file.
- A non-incremental patch is exclusive in the current system. To install another patch file when there is already one, uninstall the existing patch file, and then install and run the new patch file.

NOTE

The currently released patches are hot patches and incremental patches. All the patches mentioned in the subsequent sections are hot patches and incremental patches unless otherwise specified.

Status of Patches

Each patch has its own state that can only be changed with command line.

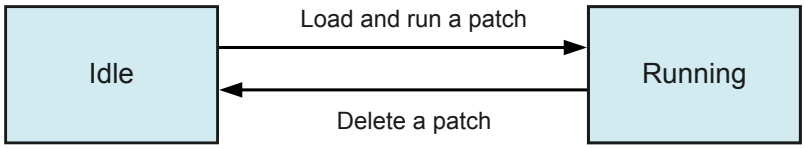
Table 1-68 describes the patch status.

Table 1-68 Status of patches

Status	Description	Patch Status Transition
Idle	The patch file is saved to the storage device but has not been loaded to the patch area.	When a patch in the storage device is loaded to the patch area, the patch is in the running state.
Running	When a patch is stored in the patch area and runs permanently, the patch is in the running state. If a board is reset, the running patch on the board remains in the running state.	You can unload the patch that is in the running state so that it can be deleted from the patch area.

Figure 1-30 shows patch status transition.

Figure 1-30 Patch status transition



Installing Patches

Installing patches is a way of upgrading a device. Patches can be installed in the following ways:

- The hot patches are generally installed while the device is running without interrupting services. This is an advantage of hot patches.

  NOTE

  For details on how to install patches, see the corresponding release notes. For details about commands used for device upgrade, see "Basic Configurations Commands - Upgrade Commands" in the *Huawei Wireless Access Points Command Reference*.

- Another way is to specify a patch file for next startup, which is described in this chapter. The patch file takes effect after the device reboots. The method is often used during a system upgrade.

1.6.2 Managing Configuration Files

You can perform operations such as saving the configuration file and backing up the configuration file.

Pre-configuration Tasks

Before managing configuration files, complete the following task:

- Logging in to the device.

Configuration Process

Perform one or multiple of the following tasks:

1.6.2.1 Saving the Configuration File

Context

You can run commands to modify the current configuration of the device, but the modified configuration will be lost after the device restarts. To enable the new configuration to take effect after a restart, save the current configuration in the configuration file before restarting the device. Use either of the following methods to save the current configuration:

- Configure the automatic save function.
- Manually save the configuration.

Procedure

- Save the configurations automatically.

  NOTICE

  The **autosave interval** command cannot be used together with the **autosave time** command.

  - Run:
    autosave interval *value*

    Automatic saving of configurations is enabled.

    By default, automatic saving of configurations is disabled. The *value* parameter can be set to **on** or **off**. The value **on** enables automatic saving of configurations, and the value **off** disables this function.
  - Run:
    autosave interval { *time* | **configuration** *time* }

    The system is configured to save the configurations at a specified interval.

    If **interval** *time* is specified, the system saves the configurations at the specified interval regardless of whether the configuration is changed.
    - The default interval is 0 seconds, indicating that the system does not save the configurations automatically.
    - After the automatic save function is enabled, the default interval is 30 minutes if *time* is not specified.
  - Run:
    autosave time { *value* | *time-value* }

    The system is configured to save the configurations at a specified time.

    When the automatic save function is enabled, the modified configuration is saved at the specified time. When the automatic save function is disabled, the system does not save the configurations automatically and you need to manually save the modified configuration.

  NOTE

  In automatic save mode, the system automatically saves configurations to the current startup configuration file. You can run the **display startup** command to check the name of the current startup configuration file.

- Save the configurations manually.
  - Run:
    save [**all**] [*configuration-file*]

    The current configuration is saved.

    The configuration file name extension must be .zip or .cfg. The system startup file must be stored in the root directory of the storage device.

    Run the **save all** command to save all the current configurations, including the configurations of the boards that are not running, to the current storage directory.

NOTE

- If you do not specify *configuration-file* when saving the configuration file for the first time, the system asks you whether to save the configuration file as **vrpcfg.zip**.
- If you do not specify *configuration-file*, configurations are saved to the current startup configuration file. You can run the **display startup** command to check the name of the current startup configuration file.
- You can run the **pwd (user view)** command in the user view to check the current storage directory.
- You can run the **cd (user view)** command in the user view to modify the current storage directory.

----End

Checking the Configuration

Based on the configuration file name, you can transfer the configuration file to the client or server through TFTP, FTP, or SFTP. For details, see **1.5 File Management**.

1.6.2.2 Comparing Configuration Files

Context

You can compare the current configuration file with the next startup configuration file to check whether they are consistent and determine whether to set the current configuration file as the next startup configuration file.

The system displays the different content starting from the first different character to the end of the file. By default, the system displays 120 characters. If the different content contains less than 120 characters, the system displays only the content from the first different character to the end of the file.

If the next startup configuration file is unavailable or empty, the system displays a message indicating that the files fail to be read.

NOTE

The configuration file name extension must be .cfg or .zip.

Procedure

- Run:

  compare configuration [*configuration-file* [*current-line-number save-line-number*]]

  The system starts to check whether the current configurations are identical with the next startup configuration file or the specified configuration file.

  If parameters are not specified, the configuration files are compared from the first line. The parameters *current-line-number* and *save-line-number* are used to continue the comparison, neglecting the differences, after differences are found.

----End

1.6.2.3 Backing Up the Configuration File

Context

If the device is damaged unexpectedly, the configuration file cannot be recovered. You can back up the configuration file in advance using one of the following methods:

- Copying the content in the display on the screen
- Backing up the configuration file to the storage device
- Backing up the configuration file through TFTP
- Backing up the configuration file through FTP

Procedure

- Copying the content in the display on the screen

  Run the **display current-configuration** command and copy all command outputs to a .txt file. The configuration file is backed up in the hard disk of the maintenance terminal.

  NOTE

  If a configuration is too long, it may be displayed in two lines on the terminal screen, depending on the terminal software. When copying a two-line configuration from the screen to a .txt file, ensure that the configuration is displayed in only one line. Otherwise, configuration restoration may fail when the .txt file is used.

- Backing up the configuration file to the storage device

  The current configuration file can be backed up immediately to the flash memory of the device. After the device starts, run the following commands to back up the configuration file to the flash memory of the device:

  ```
  <Huawei> save config.cfg
  <Huawei> copy config.cfg backup.cfg
  ```

- Backing up the configuration file through TFTP

  1. Start the TFTP server program when the device works as the TFTP client.

     Start the TFTP server program on the PC. Set the path for transmitting the configuration file, and the IP address and interface number of the TFTP server.

  2. Transfer the configuration file.

     Run the **tftp** command in the user view to back up the specified configuration file.

     ```
     <Huawei> tftp 10.110.24.254 put flash:/config.cfg backup.cfg
     ```

- Backing up the configuration file through FTP

  1. Start the FTP service when the device works as the FTP server.

     Enable the FTP server function on the device. Create an FTP user with the name **huawei** and password **ASdasd@15481erp**. The user is authorized to access the flash directory.

     ```
     <Huawei> system-view
     [Huawei] ftp server enable
     Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
     Info: Succeeded in starting the FTP server
     [Huawei] aaa
     [Huawei-aaa] local-user huawei password cipher ASdasd@15481erp
     [Huawei-aaa] local-user huawei ftp-directory flash:
     [Huawei-aaa] local-user huawei service-type ftp
     [Huawei-aaa] local-user huawei privilege level 15
     ```

2. On the maintenance terminal, initiate an FTP connection to the device.

   On the PC, set up an FTP connection to the device through the FTP client. Assume that the device IP address is 10.110.24.254.

   ```
   C:\Documents and Setting\Administrator> ftp 10.110.24.254
   Connected to 10.110.24.254.
   220 FTP service ready.
   User (10.110.24.254:(none)): huawei
   331 Password required for huawei.
   Password:
   230 User logged in.
   ```

3. Configure transfer parameters.

   If the FTP user is authenticated, the FTP client displays the prompt character of **ftp>**. Enter **binary** following the prompt character, and specify the path where the uploaded file is to be saved on the FTP client.

   ```
   ftp> binary
   200 Type set to I.
   ftp> lcd c:\temp
   Local directory now C:\temp.
   ```

4. Transfer the configuration file.

   On the PC, run the **get** command to load the configuration file to the specified path and save the file as **backup.cfg**.

   ```
   ftp> get flash:/config.cfg backup.cfg
   ```

5. Check whether the **config.cfg** and **backup.cfg** files have the same size. If they have the same size, the backup is successful.

----End

1.6.2.4 Recovering the Configuration File

Context

When incorrect configurations are performed and functions are not normal, you can use one of the following methods:

- Recovering the configuration file that is backed up in the storage device
- Recovering the configuration file that is backed up on the PC through TFTP
- Recovering the configuration file that is backed up on the PC through FTP

NOTE

After recovering the configuration file, you must restart the device to make the file take effect. Run the **startup saved-configuration** command to specify the next startup configuration file. If the configuration file name is unchanged, you do not need to run this command. Run the **reboot** command to restart the device.

Procedure

- Recovering the configuration file that is backed up in the flash memory

  This step recovers the backup configuration file stored in the flash memory of the device to the current system configuration file. When the device is working properly, run the following command:

```
<Huawei> copy flash:/backup.cfg flash:/config.cfg
```

- Recovering the configuration file that is backed up on the PC through TFTP

  Perform this operation when the device functions as the TFTP client. This operation is similar to the operation in **Backing up the configuration file through TFTP**. The difference is that the **tftp** command containing the **get** parameter in the recovery procedure downloads the **backup.cfg** file on the PC to the flash memory of the device.

- Recovering the configuration file that is backed up on the PC through FTP

  Perform this operation when the device works as the FTP server. This operation is similar to the operation in **Backing up the configuration file through FTP**. The difference is that the **put** command in the recovery procedure uploads the **backup.cfg** file on the PC to the flash memory of the device.

----End

1.6.2.5 Clearing the Configuration File

Context

You need to delete the configuration file when:

- The software and configuration file do not match after the device software is upgraded.
- The configuration file is damaged or an incorrect configuration file is loaded.

NOTICE

Exercise caution when you run the **reset saved-configuration** command. You are advised to run this command under the guide of Huawei technical support personnel.

Procedure

- Run the **reset saved-configuration** command to clear the next startup configuration file and cancel the configuration file used for next startup. The default device configurations are restored.

  NOTE

  - If the current startup configuration file is the same as the next startup configuration file when you run the **reset saved-configuration** command, the current startup configuration file is also cleared.
  - After you run this command and manually restart the device, the system displays a message asking you whether to save the configurations. Select N to clear the configurations.
  - If you do not use the **startup saved-configuration** command to specify a new configuration file containing correct configurations or do not save the configuration file after running the **reset saved-configuration** command, the device uses factory configurations for startup. If the device does not have factory configurations, it uses default configurations for startup.
  - If the next startup configuration file is empty, the device displays a message indicating that the file does not exist.

----End

1.6.3 Configuring System Startup Files

Configure the device to use the specified configuration file or patch software for the next startup.

Pre-configuration Tasks

Before configuring the system startup files, complete the following tasks:

- Starting the device and logging in to the device locally or remotely.
- Saving the startup files in the root directory of the device.

Context

Before specifying the files for next startup, you can run the **display startup** command to view the specified files for next startup.

- If no configuration file is specified for next startup, the device will start with the default configuration file (vrpcfg.zip for example). If no configuration file is stored in the default directory, the device uses the default parameters for initialization. The configuration file name extension must be .cfg or .zip. In addition, the configuration file must be saved to the root directory of the storage device.
- A patch file uses .pat as the file name extension. The specified patch file to be loaded for next startup must also be saved to the root directory of the storage device.

Procedure

- Run:
  startup saved-configuration *configuration-file*

  The configuration file for next startup is specified.

  The device reads the configuration file from the root directory of the storage device for initialization when powered on.
- (Optional) Run:
  startup patch *patch-name*

  The patch file for next startup is specified.

----End

Checking the Configuration

After the configuration is complete, run the **display startup** command to view the configuration file and patch file for next startup.

1.6.4 Restarting the Device

To make sure the specified system software and files take effect, restart the device after system startup configuration is complete.

Pre-configuration Tasks

Before restarting the device, complete the following tasks:

- Configuring system startup files.

Context

Use either of the following methods to restart the device:

- Restart the device immediately after configuration: The device restarts immediately after the reboot command is run.
- Restart the device at scheduled time: The device can be restarted at a specified time later. When the configuration is complete, you can configure the device to restart at time when few services are running to minimize the impact of device restart on services.

The device records information about every restart, including the number of device restart, details, and causes. Run the **display reset-reason** command to view the device restart information.

NOTICE

- Do not restart the device unless necessary because device restart causes service interruption in a short time.
- Save the current configuration so that it will take effect after the device restarts.

Procedure

- Restart the Device Immediately

  In the user view, run the **reboot** [**fast**] command to restart the device.

  - The **fast** parameter indicates quick restart of the device. The system does not ask you whether to save the configuration file in fast startup.
- Restart the Device at Scheduled Time

  In the user view, run the **schedule reboot** { **at** *time* | **delay** *interval* } command to restart the device at scheduled time.

  - **at** *time* specifies the specific time to restart the device.
  - **delay** *interval* specifies the waiting time before restarting the device.

----End

1.6.5 Configuration Examples

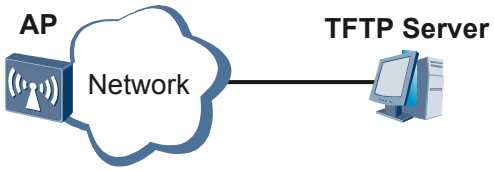
This topic describes the examples for Configuring System Startup.

1.6.5.1 Example for Backing Up the Configuration File

Networking Requirements

As shown in **Figure 1-31**, a user logs in to the device and backs up the configuration file to the TFTP server. So the configuration file can be recovered in case that the device is damaged.

Figure 1-31 Networking diagram of backing up the configuration file



Configuration Roadmap

The configuration roadmap is as follows:

1. Save the configuration file.
2. Back up the configuration file through TFTP.

Procedure

Step 1 Save configurations to the **config.cfg** file.

```
<Huawei> save config.cfg
```

Step 2 Back up the configuration file through TFTP.

1. Start the TFTP server program.

   Start the TFTP server program on the PC. Set the path for transmitting the configuration file, and the IP address and port number of the TFTP server.

2. Transfer the configuration file.

   Run the **tftp** command in the user view to back up the specified configuration file.

   ```
   <Huawei> tftp 10.110.24.254 put flash:/config.cfg backup.cfg
   ```

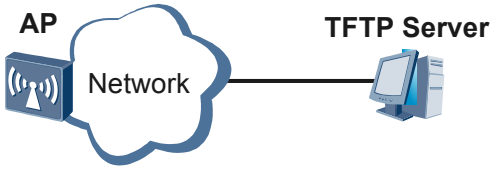
----End

1.6.5.2 Example for Recovering the Configuration File

Networking Requirements

As shown in **Figure 1-32**, a user logs in to the device and finds that some incorrect configurations cause errors in the system. To recover the original configuration, the user downloads the configuration file saved in the TFTP server to the device and specifies the configuration file for the next startup.

Figure 1-32 Network diagram of recovering the configuration file



Configuration Roadmap

The configuration roadmap is as follows:

1. Recover the configuration file that is backed up on the PC through TFTP.
2. Specify the recovered configuration file for the next startup.

Procedure

Step 1 Recover the configuration file that is backed up on the PC through TFTP.

1. Start the TFTP server program.

   Start the TFTP server program on the PC. Set the path for transmitting the configuration file, and the IP address and port number of the TFTP server.

2. Transfer the configuration file.

   Run the **tftp** command in the user view.

   ```
   <Huawei> tftp 10.110.24.254 get backup.cfg config.cfg
   ```

Step 2 Specify the recovered configuration file for the next startup.

```
<Huawei> startup saved-configuration config.cfg
```

----End

1.7 Configuring Fit/Fat Switching

You can switch an AP from a fat AP to a fit AP or a fit AP to a fat AP as required.

1.7.1 Fit/Fat Switching Overview

A fit/fat switching is implemented by loading the system software file of the fat AP or fit AP.

AP models that support fit/fat switching

The following AP models support fit/fat switching:

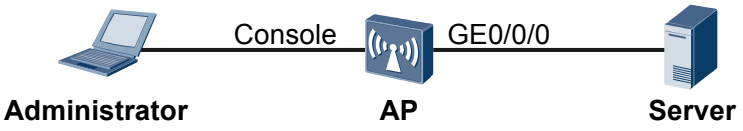
- AP3010DN-AGN
- AP5010SN-GN, AP5010DN-AGN
- AP6010SN-GN, AP6010DN-AGN
- AP6510DN-AGN, AP6510DN-AGN-US
- AP6610DN-AGN, AP6610DN-AGN-US

Loading the system software file on an AP

An AP has a different file system from those on other network devices and a small storage space. The AP must load the system software file online from a file server for an upgrade, but cannot download the system software file in the format of .bin to the storage device on the AP.

An AP can implement fit/fat switching by loading the system software file from a TFTP, an FTP, or SFTP server, as shown in **Figure 1-33**.

Figure 1-33 Fit/Fat switching networking



The administrator uses a console cable to connect the PC to the console interface of the device and connect GE0/0/0 of the device to the server. The administrator then configures fit/fat switching on the AP. The AP loads the system software file online from the server through GE0/0/0 to complete the fit/fat switching.

Version Restrictions

APs support fat AP from V200R003 and do not support cross-version fit/fat switching. For example, a V200R002 fit AP must be upgraded to a V200R003 fit AP and then switched to a fat AP. A fat AP must be switched to a V200R003 fit AP and then rolled back to a V200R002 fit AP.

NOTE

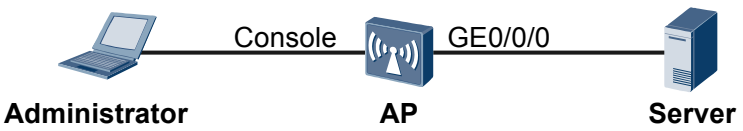
- The upgrade of a device is closely related to the released software versions. The corresponding upgrade guide is released with each new version and you can upgrade the device according to the guide. To obtain the upgrade guides, visit **http://support.huawei.com/enterprise** and download the upgrade guide based on the product name and version.
- For details about device upgrade commands, see *Huawei Wireless Access Points Command Reference - Basic Configuration Commands - Device Upgrade*.

1.7.2 Switching a Fit AP to a Fat AP

Context

A fit AP cannot be switched to a fat AP by the AC. The administrator must connect a PC to the console port on the AP to log in to the AP, connect GE0/0/0 on the AP to a TFTP, FTP, or SFTP server, and switch the fit AP to a fat AP, as shown in **Figure 1-34**.

Figure 1-34 Fit/Fat switching networking



Pre-configuration Tasks

Before switching a fit AP to a fat AP, complete the following task:

- Uploading the fit AP system software file to the TFTP, FTP, or SFTP server

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ap-mode-switch prepare
```

The file system on the fit AP allows for switching the fit AP to a fat AP.

Step 3 Run:

```
ap-mode-switch check
```

The file system on the fit AP is checked whether a fit AP allows for switching to a fat AP.

NOTICE

If not, do not perform the following steps. Otherwise, the AP file system may be damaged and the AP cannot properly start.

Step 4 Perform any of the following steps to switch a fit AP to a fat AP based on the user network:

- Run:
  ap-mode-switch tftp *filename server-ip-address*

  The AP is connected to a TFTP server to download the system software file to switch a fit AP to a fat AP.
- Run:
  ap-mode-switch ftp *filename server-ip-address user-name password* [*port*]

  The AP is connected to an FTP server to download the system software file to switch a fit AP to a fat AP.
- Run:
  ap-mode-switch sftp *filename server-ip-address user-name password* [*port*]

  The AP is connected to an SFTP server to download the system software file to switch a fit AP to a fat AP.

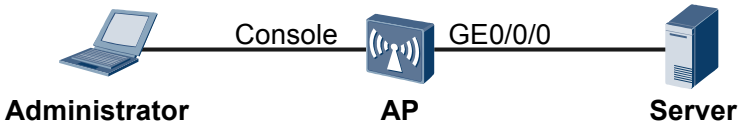
----End

1.7.3 Switching a Fat AP to a Fit AP

Context

The administrator must connect a PC to the console port on the AP to log in to the AP, connect GE0/0/0 on the AP to a TFTP, FTP, or SFTP server, and switch the fat AP to a fit AP, as shown in **Figure 1-35**.

Figure 1-35 Fit/Fat switching networking



Pre-configuration Tasks

Before switching a fat AP to a fit AP, complete the following task:

- Uploading the fit AP system software file to the TFTP, FTP, or SFTP server

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ap-mode-switch check
```

The file system on the fat AP is checked whether a fat AP allows for switching to a fit AP.

NOTICE

If not, do not perform the following steps. Otherwise, the AP file system may be damaged and the AP cannot properly start.

Step 3 Perform any of the following steps to switch a fat AP to a fit AP based on the user network:

- Run:
  ap-mode-switch tftp *filename server-ip-address*

  The AP is connected to a TFTP server to download the system software file to switch a fat AP to a fit AP.
- Run:
  ap-mode-switch ftp *filename server-ip-address user-name password* [*port*]

  The AP is connected to an FTP server to download the system software file to switch a fat AP to a fit AP.
- Run:
  ap-mode-switch sftp *filename server-ip-address user-name password* [*port*]

  The AP is connected to an SFTP server to download the system software file to switch a fat AP to a fit AP.

----End

1.7.4 Checking the Configuration

Context

After a fit/fat AP switchover is complete, run the following command to check the version information.

Procedure

- Run the **display version** [**slot** *slot-id*] command to check the device version.

----End

2 Configuration Guide - Interface Management

About This Chapter

This document describes the principles and configurations of interfaces supported by the Access Point and provides configuration examples.

2.1 Basic Configuration for Interfaces
This section interface types, interface numbering rules, and configuration parameters to facilitate interface management.

2.2 Ethernet Interface Configuration
Ethernet is flexible, simple, and easy to implement, and therefore it becomes an important local area network (LAN) networking technology. You need to configure Ethernet interfaces when using Ethernet technology to establish LANs.

2.3 Logical Interface Configuration
The information provided here on logical interface types, configuration procedures, and configuration examples can help you make full use of logical interfaces.

2.1 Basic Configuration for Interfaces

This section interface types, interface numbering rules, and configuration parameters to facilitate interface management.

2.1.1 Interface Basics

This section describes the interface types and numbering rules.

Interfaces of a device are used to exchange data and interact with other network devices. Interfaces are classified into management interface, physical interface, logical interfaces, and radio interface.

- Management interfaces

  Management interfaces are used to log in to devices. Users can use management interfaces to configure and manage devices. Management interfaces do not transmit service data.

  The console interface is a management interface. **Table 2-1** describes functions of the console interface.

  Table 2-1 Description of management interfaces

Interface	Description	Application
Console interface	A data connection equipment (DCE) interface that complies with the EIA/TIA-232 standard.	The console interface is connected to the COM serial interface of a configuration terminal to set up an on-site configuration environment.
mini USB interface	Complies with the USB 1.0 standard.	The mini USB interface is connected to the USB interface of a PC through a mini USB cable to set up an on-site configuration environment.

  NOTE

  This chapter only describes physical and logical interfaces. For detailed configurations of management interfaces, see "Basic Configuration" in the Huawei Wireless Access Points Configuration Guide.

- Physical interfaces

  Physical interfaces exist on interface cards and transmit service data

  Currently, physical interfaces on the device are Layer 2 Ethernet interfaces, which are connected to other network devices.

  Table 2-2 describes the physical interfaces supported by the device.

Table 2-2 Description of physical interfaces

Type	Interface	Description
Layer 2 Ethernet interface	GE interface	A LAN-side GE interface works at the data link layer, provides a maximum of 1000 Mbit/s transmission rate, processes Layer 2 protocol packets, and implements Layer 2 forwarding.

- Logical interfaces

  Logical interfaces are manually configured interfaces and can be used to exchange data but do not exist physically.

  Table 2-3 describes the logical interfaces that the router supports.

Table 2-3 Description of logical interfaces

Interface Type	Description
VLANIF interface	A VLANIF interface has Layer 3 features and enables VLANs to communicate after being assigned an IP address.
Loopback interface	A loopback interface is always Up and can be configured with a 32-bit subnet mask.
Null interface	A null interface is used to filter routes because any data packets received by the null interface are discarded.
WLAN-BSS interface	A WLAN-BSS interface is a logical interface used to provide wireless services for WLAN users. Similar to a Layer 2 Ethernet interface of the Hybrid type, the WLAN-BSS interface has Layer 2 attributes and can be configured with multiple Layer 2 protocols.

- Radio interfaces

  Radio interfaces are used to send or receive radio signals. They allow the device to provide wireless services. **Table 2-4** describes the radio interfaces supported by the device.

Table 2-4 Description of radio interfaces

Interface	Description
2.4 GHz radio interface	Based on IEEE 802.11 series standards, the 2.4 GHz radio interface uses the 2.4 GHz frequency band as a transmission medium to transmit wireless data.
5 GHz radio interface	Based on IEEE 802.11 series standards, the 5 GHz radio interface uses the 5 GHz frequency band as a transmission medium to transmit wireless data.

NOTE

This section describes only the physical and logical interfaces of the device. For details about parameter configurations of the radio interfaces, see **4.6.3.9 Configuring a Radio** in the *Huawei Wireless Access Points Configuration Guide-WLAN Service*.

Interface Numbering Rules

- Numbering Rules for Management Interfaces

  The following table lists the numbers of the management interfaces.

  Table 2-5 Management interface numbers

Interface	Number
Console interface	Console 0

- Numbering Rules for Physical Interfaces

  The device's physical interfaces are numbered in the format *slot ID*/*subcard ID*/*interface sequence number*.

  - *slot ID*: indicates the slot where an interface is located. The value is 0.
  - *subcard ID*: indicates the ID of a subcard. The value is 0.
  - *interface sequence number*: indicates the sequence number of an interface on the device. The value is 0.

2.1.2 Configuring Basic Interface Parameters

This section describes how to configure basic interface parameters, including interface description and traffic statistics collection interval, and how to shut down and enable an interface.

2.1.2.1 Entering the Interface View

Context

To configure an interface, enter the interface view.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

interface-type interface-number specifies the type and number of an interface.

NOTE

If the specified interface does not exist, this command creates the interface and displays the interface view.

----End

2.1.2.2 Configuring an Interface Description

Context

To facilitate device management and maintenance, you can configure descriptions for interfaces. An interface description can contain the device where the interface is located, interface type, and remote device. For example: To-[DeviceB]GE-0/0/1 indicates that an interface of this device is connected to GE0/0/1 of device B.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
description description
```

The description is configured for the interface.

NOTE

The interface description is displayed from the first non-space character.

----End

2.1.2.3 Configuring the Traffic Statistics Collection Interval

Context

By setting the traffic statistics collection interval, you can collect and analyze packet statistics. According to traffic statistics, you can take measures to prevent network congestion and service interruption.

- When congestion occurs, you can set the statistics collection interval on an interface to 300 seconds or less (30 seconds if congestion worsens). Then observe traffic distribution on the interface within a short period of time. Take measures to data packets that cause congestion to control the rate of the packets.
- When the network bandwidth is sufficient and services are running properly, set the statistics collection interval on an interface to more than 300 seconds. If traffic parameters on an interface are out of the specified range, change the statistics collection interval to observe the traffic statistics in real time.

NOTE

- The interval set in the system view takes effect on all the interfaces that use the default interval.
- The interval set in the interface view takes effect only on this interface.
- The interval set in the interface view takes precedence over the interval set in the system view.

Procedure

- Configure the global traffic statistics collection intervals in the system view.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     set flow-stat interval *interval-time*

     The global traffic statistics collection interval is set.

     By default, the global traffic statistics collection interval is 300s.
- Configure the traffic statistics collection interval on an interface.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     set flow-stat interval *interval-time*

     The traffic statistics collection interval is set on the interface.

     By default, the traffic statistics collection interval on an interface is 300s.

----End

2.1.2.4 Enabling or Disabling an Interface

Context

After modifying parameters of an interface, run the **shutdown** and **undo shutdown** commands, or run the **restart** command to make the modification take effect.

NOTE

- Running the **shutdown** and **undo shutdown** commands is equivalent to running the **restart** command. Running the shutdown command does not modify or delete interface configurations..
- A NULL interface is always Up and cannot be enabled or disabled by commands.
- A loopback interface is always Up and cannot be enabled or disabled by commands.

Procedure

- Disable an interface.

1. Run:
   system-view

   The system view is displayed.
2. Run:
   interface *interface-type interface-number*

   The interface view is displayed.
3. Run:
   shutdown

   The interface is disabled.

   By default, an interface is enabled.

NOTICE

- Disabling an interface during data transmission will cause data frame loss or service interruption. Exercise caution when you use the **shutdown** command.

- Enable an interface.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     undo shutdown

     The interface is enabled.

     By default, an interface is enabled.

----End

2.1.2.5 Checking the Configuration

Procedure

- Run the **display interface** [*interface-type* [*interface-number*]] command to check information about an interface, including interface running status, basic interface configuration, and packet forwarding on the interface.
- Run the **display interface brief** [**main**] command to check brief information about interfaces, including the physical status, protocol status, bandwidth usage in the inbound and outbound directions during a certain period, and the number of error packets sent and received.

- Run the **display ip interface** [*interface-type interface-number*] command to check the IP configuration of an interface.
- Run the **display default-parameter interface** *interface-type interface-number* command to check the default configuration of an interface.
- Run the **display interface description** [*interface-type* [*interface-number*]] command to check the description of an interface.
- Run the **display interface** [*interface-type*] **counters** { **inbound** | **outbound** } command to check statistics about packets received and transmitted on a physical interface.

----End

2.1.3 Maintaining Interfaces

To view statistics about traffic sent and received on an interface within a period, first clear existing traffic statistics on the interface.

2.1.3.1 Clearing Interface Traffic Statistics

Context

To monitor the status of an interface or locate faults on the interface, collect traffic statistics on the interface. Before collecting traffic statistics on an interface within a period, clear the existing traffic statistics on this interface.

NOTICE

Interface statistics cannot be restored after they are cleared. Confirm your action before you perform the operations.

Procedure

- Run the **reset counters interface** [*interface-type* [*interface-number*]] command to clear the interface statistics.
- Run the **reset counters interface** [*interface-type* [*interface-number*]] command to clear the interface statistics.
- Run the **reset counters if-mib interface** [*interface-type* [*interface-number*]] command to clear traffic statistics on the network management interface.

----End

2.2 Ethernet Interface Configuration

Ethernet is flexible, simple, and easy to implement, and therefore it becomes an important local area network (LAN) networking technology. You need to configure Ethernet interfaces when using Ethernet technology to establish LANs.

2.2.1 Ethernet Interface Overview

Ethernet interfaces are used on LANs.

Physical interfaces on the device are Layer 2 Ethernet interfaces working at the data link layer. You cannot configure IP addresses for these interfaces. These interfaces can forward the received packets at Layer 2 or be added to a VLAN to forward packets at Layer 3 through corresponding VLANIF interfaces. Layer 2 Ethernet interfaces of the device include Ethernet electrical interfaces and optical interfaces.

Only GE0/0/0 on the AP6610DN-AGN is a combo interface on which SFP indicates the optical interface and ETH indicates the electrical interface. The SFP interface and ETH interface cannot be used simultaneously. If you connect the SFP interface to a peer optical interface, GE0/0/0 functions as the the SFP optical interface; if you connect the ETH interface to a peer electrical interface, GE0/0/0 functions as the the ETH electrical interface. If you connect both SFP and ETH interfaces to peer optical and electrical interfaces, GE0/0/0 functions as the SFP optical interface.

Table 2-6 lists the attributes of Ethernet interfaces.

Table 2-6 Attributes of Ethernet interfaces

Interface Type	Rate (Mbit/s)	Duplex Mode	Auto-Negotiation	Traffic Control	Traffic Control Negotiation
Gigabit Ethernet (GE) electrical interface	10	Full-duplex/ half-duplex	Supported	Supported	Supported
	100	Full-duplex/ half-duplex			
	1000	Full-duplex			
SFP optical interface	1000	Full-duplex	Supported	Not supported	Not supported

NOTE

By default, an Ethernet interface works in auto-negotiation mode, which is recommended. If the negotiation succeeds, the interfaces on both ends of the link work in the same duplex mode and at the same speed.

2.2.2 Default Configuration

This section describes the default configuration of common Ethernet interface parameters.

Table 2-7 Default configuration of Ethernet interfaces

Parameter	Default Value
Working mode of combo interfaces	Auto, in which a combo interface can automatically switch between the optical and electrical interface modes.
Media Dependent Interface (MDI) mode	Auto, in which an interface can automatically identify the type of the connected network cable
Auto-negotiation	Auto-negotiation
Duplex Mode	Auto-negotiation mode: negotiated by the local and remote interfaces Non-auto-negotiation mode: full-duplex mode
Rate	Auto-negotiation mode: negotiated by the local and remote interfaces Non-auto-negotiation mode: maximum rate supported by an interface

2.2.3 Configuring an Ethernet Interface

This section describes the procedures for configuring an ethernet interface.

2.2.3.1 Configuring the MDI Type of an Interface

Context

Twisted pairs used to connect Ethernet devices include:

- Straight-through cable: connects devices of different types, such as a switch and a PC or a switch and a router.
- Crossover network: connects devices of the same type, such as two PCs, two switches, or two routers.

An interface supports the following medium dependent interface (MDI) types, which determine the cable type allowed on the interface:

- Auto
- Normal
- Across

By default, an interface works in auto mode. When the device fails to identify the network cable type on an interface, set the MDI type manually.

When setting the MDI type on an interface, pay attention to the following points:

- When a straight-through cable is used, the local and remote interfaces must use different MDI types, for example, across mode on one end and normal mode on the other end.

- When a crossover cable is used, the local and remote interfaces must use the same MDI type. For example, both ends must use the across or normal mode, or at least one end uses the auto mode.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The Ethernet interface view is displayed.

Step 3 Run:

```
mdi { across | auto | normal }
```

The MDI type is configured for the Ethernet interface.

By default, an Ethernet interface works in auto mode and automatically identifies the network cable type.

----End

2.2.3.2 Configuring the Auto-Negotiation Function

Context

The auto-negotiation function allows interfaces on both ends of a link to select the same operating parameters by exchanging capability information. The parameters include the duplex mode and rate. When the negotiation succeeds, the two interfaces use the same duplex mode and work at the same rate. In non-auto negotiation mode, the operating parameters must be set manually.

For details about the auto-negotiation configuration supported by Ethernet interfaces, see **2.2.1 Ethernet Interface Overview**.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Configure the auto-negotiation function.

- Run:
  ```
  negotiation auto
  ```
  The Ethernet interface is configured to work in auto-negotiation mode.

- Run:
  undo negotiation auto

  The Ethernet interface is configured to work in non-auto negotiation mode.

By default, an Ethernet interface works in auto-negotiation mode.

NOTE

The interfaces on both ends of a link must have the same negotiation mode.

----End

2.2.3.3 Configuring the Duplex Mode for an Ethernet Interface

Context

For details about the duplex modes that various Ethernet interfaces support, see **2.2.1 Ethernet Interface Overview**.

Duplex modes include:

- Half-duplex mode: An Ethernet interface only receives or sends data within the specified maximum transmission distance at a time.
- Full-duplex mode: An Ethernet interface receives and sends data at the same time. The maximum throughput in the full-duplex mode doubles that in the half-duplex mode, and there is no limit on the maximum transmission distance.

You can set the duplex mode for an Ethernet electrical interface in either the auto-negotiation or non-auto negotiation mode.

- In auto-negotiation mode, interfaces on both ends of a link negotiate their duplex mode. If the negotiated duplex mode is not the required one, you can set the duplex mode manually. For example, two interfaces support both the full-duplex mode and half-duplex mode. If the two interfaces negotiate to work in half-duplex mode, but they are required to work in full-duplex mode, run the **auto duplex full** command to set the full-duplex mode for the two interfaces.
- In non-auto negotiation mode, you can manually set the required duplex mode for interfaces.

NOTE

The interfaces on both ends of a link must have the same duplex mode.

Procedure

- Setting the duplex mode in auto-negotiation mode

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The Ethernet interface view is displayed.
  3. Run:
     negotiation auto

The Ethernet interface is configured to work in auto-negotiation mode.

4. Run:
   auto duplex { **full** | **half** }*
   The duplex mode in auto-negotiation mode is set for the Ethernet interface.

By default, interfaces on both ends of a link negotiate their duplex mode.

- Setting the duplex mode in non-auto negotiation mode

  1. Run:
     system-view
     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*
     The Ethernet interface view is displayed.
  3. Run:
     undo negotiation auto
     The Ethernet interface is configured to work in non-auto negotiation mode.
  4. Run:
     duplex { **full** | **half** }
     The duplex mode is set for the Ethernet interface.

  By default, an Ethernet interface works in full-duplex mode.

2.2.3.4 Configuring the Rate for an Ethernet Interface

Context

For details about the rates that various Ethernet interfaces support, see **2.2.1 Ethernet Interface Overview**.

You can set the interface rate in either the auto-negotiation or non-auto negotiation mode.

- In auto-negotiation mode, interfaces on both ends of a link negotiate their interface rates. You can set the auto-negotiation rate range to limit the negotiated rate. For example, if two interfaces negotiate to work at a rate of 100 Mbit/s, but they are required to work at a rate of 10 Mbit/s to prevent network traffic congestion, you can run the **auto speed 10** command to set the rate of the interfaces to 10 Mbit/s.
- In non-auto negotiation mode, you must set the rate for interfaces so that the two devices can communicate.

NOTE

- In auto-negotiation mode, you can set the rate only for electrical interfaces.
- In non-auto negotiation mode, you can set the rate for electrical and optical interfaces.
- The interfaces on both ends of a link must have the same rate.

Procedure

- Configuring interface rate in auto-negotiation mode

  1. Run:
     system-view

The system view is displayed.

2. Run:
   interface *interface-type interface-number*

   The Ethernet interface view is displayed.

3. Run:
   auto speed { **10** | **100** | **1000** }*

   The rate is set for the Ethernet interface.

By default, interfaces on both ends of a link negotiate their interface rates.

- Configuring the interface rate in the non-auto negotiation mode

  1. Run:
     system-view

     The system view is displayed.

  2. Run:
     interface *interface-type interface-number*

     The Ethernet interface view is displayed.

  3. Run:
     undo negotiation auto

     The Ethernet interface is configured to work in non-auto negotiation mode.

  4. Run:
     speed { **10** | **100** | **1000** }

     The rate is set for the Ethernet interface.

  By default, an Ethernet interface works at the maximum rate.

2.2.3.5 Configuring Logs and Thresholds for Outbound and Inbound Bandwidth Usage

Context

The bandwidth usage represents the load on a device. If the bandwidth usage exceeds the threshold, bandwidth of the device is insufficient for services and needs expansion. For example, if the bandwidth usage exceeds 95%, an alarm is generated to indicate that bandwidth resources are used up. Services may be interrupted before system expansion. You can set the upper and lower thresholds for bandwidth usage. When the bandwidth usage exceeds the lower threshold, the system generates a log. When the bandwidth usage exceeds the upper threshold, the system triggers an alarm.

The lower threshold must be smaller than the upper threshold. For example, you can set the lower threshold to 80% and the upper threshold to 95%. When the bandwidth usage exceeds 80%, the system generates a log, alerting users that the system needs expansion. When the bandwidth usage exceeds 95%, the system generates an alarm to prevent service interruption.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
log-threshold { input-rate | output-rate } bandwidth-in-use [ resume-rate resume-threshold ]
```

The log thresholds for the outbound or inbound bandwidth usage on the interface are configured.

By default, the log thresholds of the outbound and inbound bandwidth usage are both 100.

NOTE

Maintain a proper gap between the *bandwidth-in-use* and *resume-threshold* values to prevent log flapping.

Step 4 Run:

```
trap-threshold { input-rate | output-rate } bandwidth-in-use [ resume-rate resume-threshold ]
```

The alarm thresholds for the outbound or inbound bandwidth usage on the interface are configured.

By default, the alarm thresholds of the outbound and inbound bandwidth usage are both 100.

NOTE

Maintain a proper gap between the *bandwidth-in-use* and *resume-threshold* values to prevent alarm flapping.

----End

2.2.3.6 Checking the Configuration

Procedure

- Run the **display interface** [*interface-type* [*interface-number*]] command to check information about an interface, including interface running status, basic interface configuration, and packet transmitted through the interface.
- Run the **display interface brief** [**main**] command to check brief information about interfaces, including the physical status, protocol status, bandwidth usage in the inbound and outbound directions during a certain period of time, and the number of error packets sent and received on each interface.
- Run the **display interface description** [*interface-type* [*interface-number*]] command to check the interface description.
- Run the **display interface ethernet brief** [**main**] command to check brief information about Ethernet interfaces, including the physical status, negotiation mode, duplex mode, rate, and average bandwidth usage in the inbound and outbound directions on each interface within the last period of time.

----End

2.2.4 Maintaining Ethernet Interfaces

This section describes how to maintain Ethernet interfaces, including using the loopback function to check the interface and deleting interface statistics.

2.2.4.1 Configuring Loopback Detection

Context

NOTICE

- After the loopback detection is enabled on an interface using the **loopback** command, the Ethernet interface or link on the interface cannot function properly. When the loopback detection test is complete, run the **undo loopback** command to disable it immediately.

Loopback detection needs to be enabled for special function testing, for example, Ethernet interface diagnosis. When loopback detection is enabled on an Ethernet interface, the interface works in the full-duplex mode. When loopback detection is disabled, the interface restores to the default configuration.

Table 2-8 describes the loopback detection classification.

Table 2-8 Loopback detection classification

Type	Description
Internal loopback	Packets sent from an interface are sent back to the local device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
loopback internal
```

Internal loopback detection is configured on the Ethernet interface.

By default,internal loopback detection is disabled on an Ethernet interface.

----End

2.2.4.2 Clearing Interface Statistics

Context

To monitor the status of an interface or locate faults on the interface, collect traffic statistics on the interface. Before collecting traffic statistics on an Ethernet interface, clear the existing traffic statistics on this interface.

NOTICE

Interface statistics cannot be restored after they are cleared. Confirm your action before you perform the operations.

Procedure

- Run the **reset counters interface** [*interface-type* [*interface-number*]] command to clear interface statistics.
- Run the **reset counters if-mib interface** [*interface-type* [*interface-number*]] command to clear statistics on the network management interface.

----End

2.2.5 Common Configuration Errors

This section describes the common configuration errors and provides the troubleshooting methods.

2.2.5.1 Local and Remote Interfaces Have Different Duplex Modes, Rates, and Negotiation modes

Fault Description

An interface frequently alternates between Up and Down.

Troubleshooting Procedure

1. Run the
   display interface [*interface-type* [*interface-number*]]
   command to check the duplex mode, speed, and negotiation mode of the interface.
   - View the **Negotiation** field.
     a. ENABLE: indicates that the interface works in auto-negotiation mode.
     b. DISABLE: indicates that the interface works in non-auto negotiation mode.

     The two interfaces must work in the same negotiation mode. Run the **negotiation auto** command in the interface view to enable auto negotiation on the interfaces. If the fault persists, disable auto negotiation and forcibly set the same speed and duplex mode on the interfaces.

- View the **Speed** field. If the two interfaces work at different speeds in the non-auto negotiation state, run the **speed** command in the interface view to set the same rate on the two interfaces.
- View the **Duplex** field. If the two interfaces work in different duplex modes in non-auto negotiation mode, run the **duplex** command in the interface view to set the same duplex mode on the two interfaces.

2.3 Logical Interface Configuration

The information provided here on logical interface types, configuration procedures, and configuration examples can help you make full use of logical interfaces.

2.3.1 Logical Interfaces

Logical interfaces do not exist physically. They are manually configured for data exchange.

This topic describes logical interfaces supported by devices.

Table 2-9 Logical interface types

Interface Type	Description	Configuration Reference
VLANIF interface	A VLANIF interface has Layer 3 features and enables VLANs to communicate after being assigned an IP address.	**3.5 VLAN Configuration** in "Network Interconnection" of the Huawei Wireless Access Points Configuration Guide
Loopback interface	A loopback interface is always Up and can be configured with a 32-bit subnet mask.	-
Null interface	A null interface is used to filter routes because any data packets received by the null interface are discarded.	-
WLAN-BSS interface	A WLAN-BSS interface is a logical interface used to provide wireless services for WLAN users. Similar to a Layer 2 Ethernet interface of the Hybrid type, the WLAN-BSS interface has Layer 2 attributes and can be configured with multiple Layer 2 protocols.	**4.6.3.6 Configuring a WLAN-BSS Interface** in "WLAN Service" of the Huawei Wireless Access Points Configuration Guide

2.3.2 Configuring a Logical Interface

This section describes the procedures for configuring a logical interface.

2.3.2.1 Configuring a Loopback Interface

A loopback interface is always Up at the physical layer and link layer unless it is manually shut down. You can configure loopback interfaces to enhance network reliability.

Context

The loopback interface has the following features:

- A loopback interface is always Up at the physical layer and link layer unless it is manually shut down. It has the loopback feature.
- The loopback interface can be configured with the mask of all 1s.

Based on the preceding features, the loopback interface has the following applications.

- The IP address of a loopback interface is specified as the source address of packets to improve network reliability.
- The loopback interface can be configured with the mask of 255.255.255.255 to save IP address resources.

Pre-Configuration

Before configuring a loopback interface, complete the following task:

- Powering on the device and performing self-check

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface loopback loopback-number
```

A loopback interface is created and the loopback interface view is displayed.

Step 3 Run:

```
ip address ip-address { mask | mask-length }
```

The IP address of the loopback interface is configured.

Step 4 (Optional) Run:

```
trigger trap { linkup | linkdown }
```

The device is configured to report alarms to the network management system.

----End

Checking the Configuration

- Run the **display interface loopback** [*loopback-number*] command to check the status of a loopback interface.

2.3.2.2 Configuring a NULL Interface

A NULL interface is always Up once created automatically by the system. It does not forward packet but can be used to filter packet.

Context

A NULL0 interface is created automatically. The NULL0 interface is always Up and cannot forward packets. Any packets sent to the NULL0 interface are discarded. If the next hop of a static route to a network segment is a null interface, all the data packets destined for this network segment are discarded. Therefore, the packets that you want to filter out can be sent to the NULL0 interface directly without configuring the access control list.

For example, run the following static route configuration command to discard packets sent to the network segment of 192.101.0.0.

```
[Huawei] ip route-static 192.101.0.0 255.255.0.0 NULL 0
```

Pre-Configuration

Before configuring a NULL interface, complete the following task:

- Powering on the device and performing self-check

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface null 0
```

The NULL interface view is displayed.

The NULL interface stays in the Up state. It cannot forward data packets. You cannot configure an IP address for it or encapsulate it with protocols.

----End

Checking the Configuration

- Run the **display interface null** [**0**] command to check the status of a null interface.

2.3.2.3 Configuring the MTU on an Interface

Context

The size of data packets is limited at the network layer. Upon receiving an IP packet to be sent, the network layer checks to which local interface the packet needs to be sent and obtains the maximum transmission unit (MTU) configured on the interface. Then the network layer compares the MTU with the packet length. If the packet length is longer than the MTU, the network layer disassembles the packet to fragments, each no longer than the MTU.

- If the MTU is too small whereas the packet size is large, the packet is split into many fragments. Therefore, the packet may be discarded due to insufficient QoS queue length.
- If the MTU is too large, packets are transmitted slowly or even lost.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
mtu mtu
```

The MTU of the Ethernet interface is configured.

By default, the MTU of an Ethernet interface is 1500 bytes.

NOTICE

After changing the MTU on an interface by using the **mtu** command, run the **restart** command in the interface view to restart the interface for the configuration to take effect.

----End

3 Configuration Guide - Network Interconnection

About This Chapter

This document describes the Network Interconnection configuration procedures and provides configuration examples.

3.1 Network Interconnection Configuration Overview
This section describes network interconnection configurations to help you learn features and basic concepts.

3.2 Ethernet Switching Overview
This section describes the basic concept of Ethernet and Ethernet switching.

3.3 IP Routing Basic Configuration
You can configure IP routing to learn about basic parameters for IP routing.

3.4 MAC Address Table Configuration
This chapter provides the basics for MAC address table configuration, configuration procedure, and configuration examples.

3.5 VLAN Configuration
VLANs have advantages of broadcast domain isolation, security hardening, flexible networking, and good extensibility.

3.6 IP Address Configuration
Network devices can communicate at the network layer only after they are configured with IP addresses.

3.7 ARP Configuration
The Address Resolution Protocol (ARP) maps IP addresses to MAC addresses so that Ethernet frames can be transmitted on a physical network.

3.8 DHCP Configuration
DHCP dynamically manages and configures clients in a concentrated manner. It ensures proper IP address allocation and improves IP address use efficiency.

3.9 DNS Configuration

This chapter describes the principles, basic functions and configuration procedures of DNS on the access point, and provides configuration examples.

3.10 IP Performance Configuration

You can optimize IP performance by adjusting parameters on the network.

3.11 Static Route Configuration

Static routes apply to simple networks. Proper static routes can improve network performance and ensure bandwidth for important applications.

3.12 Managing IP Routing Tables

This section describes how to manage IP routing tables. Through this section, you can understand the traffic forwarding paths.

3.1 Network Interconnection Configuration Overview

This section describes network interconnection configurations to help you learn features and basic concepts.

Table 3-1 describes software feature classifications and basic concepts.

Table 3-1 Feature classification

Category	Description
Ethernet switching	Describes VLAN management and MAC address management, including: ● **3.4 MAC Address Table Configuration** ● **3.5 VLAN Configuration** See **3.2 Ethernet Switching Overview** for basic concepts of Ethernet switching.
IP service	Describes ARP configuration, IPv4 address manual configuration, dynamic IP address assignment, and setting parameters for IP packets to optimize network performance. ● **3.6 IP Address Configuration** ● **3.7 ARP Configuration** ● **3.8 DHCP Configuration** ● **3.9 DNS Configuration** ● **3.10 IP Performance Configuration**
IP routing	Describes IPv4 static routes and IP routing table management, including: ● **3.11 Static Route Configuration** ● **3.12 Managing IP Routing Tables** See **3.3.1 Introduction to IP Routing** for IP routing basic concepts.

3.2 Ethernet Switching Overview

This section describes the basic concept of Ethernet and Ethernet switching.

3.2.1 Introduction to Ethernet Switching

Definition

The earliest Ethernet standard was the DEC-Intel-Xerox (DIX) standard jointly developed by the Digital Equipment Corporation (DEC), Intel, and Xerox in 1982. After years of development, Ethernet has become the most widely used local area network (LAN) type, and many Ethernet standards have been put into use, including standard Ethernet (10 Mbit/s), fast Ethernet (100 Mbit/s), gigabit Ethernet (1000 Mbit/s), and 10G Ethernet (10 Gbit/s). IEEE 802.3 was defined based on Ethernet and is compatible with Ethernet standards.

In the TCP/IP suite, the IP packet encapsulation format on an Ethernet network is defined in RFC 894, and the IP packet encapsulation format on an IEEE 802.3 network is defined in RFC 1042. Currently, the format defined in RFC 894 is most commonly used. This format is called Ethernet_II or Ethernet DIX.

NOTE

To distinguish Ethernet frames of the two types, Ethernet frames defined in RFC 894 are called Ethernet_II frames and Ethernet frames defined in RFC 1042 IEEE 802.3 are called frames in this document.

History

In 1972, when Robert Metcalfe (father of Ethernet) was hired by Xerox, his first job was to connect computers in Xerox's Palo Alto Research Center (PARC) to the Advanced Research Projects Agency Network (ARPANET), progenitor of the Internet. In 1972 also, Robert Metcalfe designed a network to connect computers in the PARC. That network was based on the Aloha system (a radio network system) and connected many computers in the PARC, so Metcalfe originally named the network Alto Aloha network. The Alto Aloha network started operating in May 1973, and Metcalfe then gave it an official name Ethernet, which is the prototype of Ethernet. The network operated at a rate of 2.94 Mbit/s and used thick coaxial cable as transmission medium. In June 1976, Metcalfe and his assistant David Boggs published a paper *Ethernet Distributed Packet Switching for Local Computer Networks*. At the end of 1977, Metcalfe and his three co-workers were gained a patent on "Multipoint data communication system with collision detection." Since then, Ethernet was known to the public.

As Ethernet technology develops rapidly, Ethernet has become the most widely used LAN technology and replaced most of other LAN standards, such as token ring, fiber distributed data interface (FDDI), and attached resource computer network (ARCNET). After rapid development of 100M Ethernet in the 20th century, gigabit Ethernet and even 10G Ethernet are now expanding their applications as promoted by international standardization organizations and industry-leading enterprises.

Purpose

Ethernet is a universal communication protocol standard used for local area networks (LANs). This standard defines the cable type and signal processing method used for LANs.

Ethernet networks are broadcast networks established based on the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism. Collisions restrict Ethernet performance. Early Ethernet devices such as hubs work at the physical layer, and cannot confine collisions to a particular scope. This restricts network performance improvement. Working at the data link layer, switches are able to confine collisions to a particular scope. Switches help improve Ethernet performance and have replaced hubs as mainstream Ethernet devices. However, switches do not restrict broadcast traffic on the Ethernet. This affects Ethernet performance. Dividing a LAN into virtual local area networks (VLANs) on switches or using Layer 3 switches can solve this problem.

As a simple, cost-effective, and easy-to-implement LAN technology, Ethernet has become the mainstream in the industry. Gigabit Ethernet and even 10G Ethernet make Ethernet the most promising network technology.

3.2.2 Basic Concepts of Ethernet

This section describes the basic concept of Ethernet.

3.2.2.1 Ethernet Network Layers

Ethernet uses passive medium and transmits data in broadcast mode. It defines protocols used on the physical layer and data link layer, interfaces between the two layers, and interfaces between the data link layer and upper layers.

Physical Layer

The physical layer determines basic physical attributes of Ethernet, including data coding, time scale, and electrical frequency.

The physical layer is the lowest layer in the Open Systems Interconnection (OSI) reference model and is closest to the physical medium (communication channel) that transmits data. Data is transmitted on the physical layer in binary bits (0 or 1). Transmission of bits depends on transmission devices and physical media, but the physical layer does not refer to a specific physical device or a physical media. Actually, the physical layer is located above a physical medium and provides the data link layer with physical connections to transmit original bit streams.

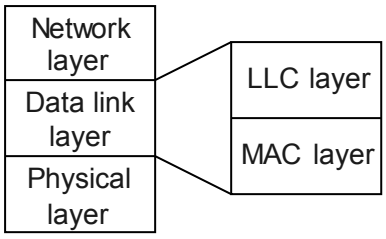
Data Link Layer

The data link layer is the second layer in the OSI reference model, located between the physical layer and network layer. The data link layer obtains service from the physical layer and provides service for the network layer. The basic service that the data link layer provides is to reliably transmit data from the network layer of a source device to the network layer of an adjacent destination device.

The physical layer and data link layer depend on each other. Therefore, different working modes of the physical layer must be supported by corresponding data link layer modes. This hinders Ethernet design and application.

Some organizations and vendors propose to divide the data link layer into two sub-layers: the Media Access Control (MAC) sub-layer and the Logical Link Control (LLC) sub-layer. Then different physical layers correspond to different MAC sub-layers, and the LLC sub-layer becomes totally independent, as shown in **Figure 3-1**.

Figure 3-1 Hierarchy of Ethernet data link layer



The following sections describe concepts involved in the physical layer and data link layer.

3.2.2.2 Introduction to Ethernet Cable Standards

Introduction to Ethernet Cable Standards

Currently, mature Ethernet physical layer standards are:

- 10BASE-2
- 10BASE-5
- 10BASE-T
- 10BASE-F
- 100BASE-T4
- 100BASE-TX
- 100BASE-FX
- 1000BASE-SX
- 1000BASE-LX
- 1000BASE-TX
- 10GBASE-LR
- 10GBASE-SR

In the preceding standards, 10, 100, 1000 and 10G stand for transmission rates, and BASE represents baseband.

- 10M Ethernet cable standards

  Table 3-2 lists the 10M Ethernet cable standards defined in IEEE 802.3.

  Table 3-2 10M Ethernet cable standards

Name	Cable	Maximum Transmission Distance
10BASE-5	Thick coaxial cable	500 m
10BASE-2	Thin coaxial cable	200 m
10BASE-T	Twisted pair cable	100 m
10BASE-F	Fiber	2000 m

  NOTE

  Coaxial cables have a fatal defect: Devices are connected in series and therefore a single-point failure can cause the breakdown of the entire network. As the physical standards of coaxial cables, 10BASE-2 and 10BASE-5 have fallen into disuse.

- 100M Ethernet cable standards

  100M Ethernet is also called Fast Ethernet (FE). Compared with 10M Ethernet, 100M Ethernet has a faster transmission rate at the physical layer, but they have no difference at the data link layer.

  Table 3-3 lists the 100M Ethernet cable standards.

Table 3-3 100M Ethernet cable standards

Name	Cable	Maximum Transmission Distance
100Base-T4	Four pairs of Category 3 twisted pair cables	100 m
100Base-TX	Two pairs of Category 5 twisted pair cables	100 m
100Base-FX	Single-mode fiber or multi-mode fiber	2000 m

Both 10Base-T and 100Base-TX apply to Category 5 twisted pair cables. They have different transmission rates. The 10Base-T transmits data at 10 Mbit/s, whereas the 100Base-TX transmits data at 100 Mbit/s.

The 100Base-T4 is rarely used now.

- Gigabit Ethernet cable standards

  Gigabit Ethernet is developed on the basis of the Ethernet standard defined in IEEE 802.3. Based on the Ethernet protocol, Gigabit Ethernet increases the transmission rate to 10 times the FE transmission rate, reaching 1 Gbit/s. **Table 3-4** lists the Gigabit Ethernet cable standards.

Table 3-4 Gigabit Ethernet cable standards

Interface Name	Cables	Maximum Transmission Distance
1000Base-LX	Single-mode fiber or multi-mode fiber	316 m
1000Base-SX	Multi-mode fiber	316 m
1000Base-TX	Category 5 twisted pair cable	100 m

Gigabit Ethernet technology can upgrade the existing Fast Ethernet from 100 Mbit/s to 1000 Mbit/s.

The physical layer of Gigabit Ethernet uses 8B10B coding. In traditional Ethernet technology, the data link layer delivers 8-bit data sets to its physical layer. After processing the data sets, the physical layer sends them to the data link layer. The data sets are still 8 bits after processing.

The situation is different on the Gigabit Ethernet of optical fibers. The physical layer maps the 8-bit data sets transmitted from the data link layer to 10-bit data sets and then sends them out.

- 10G Ethernet cable standards

  10G Ethernet is currently defined in supplementary standard IEEE 802.3ae, which will be combined with IEEE 802.3 later. **Table 3-5** lists the 10G Ethernet cable standards.

Table 3-5 10G Ethernet cable standards

Name	Cables	Maximum Transmission Distance
10GBASE-T	CAT-6A or CAT-7	100 m
10GBase-LR	Single-mode optical fiber	10 km
10GBase-SR	Multi-mode optical fiber	Several hundred meters

3.2.2.3 CSMA/CD

- Definition of CSMA/CD

  Ethernet was originally designed to connect computers and other digital devices on a shared physical line. The computers and digital devices can access the shared line only in half-duplex mode. Therefore, a mechanism of collision detection and avoidance is required to prevent multiple devices from contending for the line. This mechanism is called the carrier Sense Multiple Access with Collision Detection (CSMA/CD).

  The concept of CSMA/CD is described as follows:

  - CS: carrier sense

    Before transmitting data, a station checks whether the line is idle to reduce chances of collision.

  - MA: multiple access

    Data sent by a station can be received by multiple stations.

  - CD: collision detection

    If two stations transmit electrical signals at the same time, the voltage amplitude doubles the normal amplitude as signals of the two stations accumulate. The situation results in collision.

    The stations stop transmission after detecting the collision, and resume the transmission after a random delay.

- CSMA/CD working process

  CSMA/CD works as follows:

  1. A station continuously detects whether the shared line is idle.
     - If the line is idle, the station sends data.
     - If the line is in use, the station waits until the line becomes idle.
  2. If two stations send data at the same time, a collision occurs on the line, and signals on the line become unstable.
  3. After detecting the instability, the station immediately stops sending data.
  4. The station sends a series of disturbing pulses. After a period of time, the station resumes the data transmission.

     The station sends disturbing pulses to inform other stations, especially the station that sends data at the same time, that a collision occurred on the line.

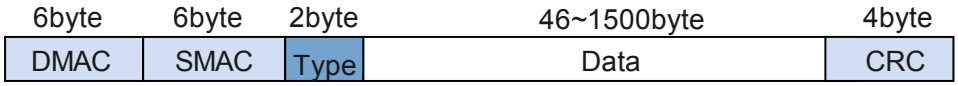
After detecting a collision, the station waits for a random period of time, and then resumes the data transmission.

3.2.2.4 Minimum Frame Length and Maximum Transmission Distance

Due to the limitation of the CSMA/CD algorithm, an Ethernet frame must be longer than or equal to a specified length. On the Ethernet, the minimum frame length is 64 bytes, which is determined jointly by the maximum transmission distance and the collision detection mechanism.

The use of minimum frame length can prevent the following situation: station A finishes sending the last bit, but the first bit does not arrive at station B, which is far from station A. Station B considers that the line is idle and begins to send data, leading to a collision.

Figure 3-2 Ethernet_II frame format



The upper layer protocol must ensure that the Data field of a packet contains at least 46 bytes, so that the total length of the Data field, the 14-byte Ethernet frame header, and the 4-byte check code at the frame tail can reach the minimum frame length, as shown in **Figure 3-2**. If the Data field is less than 46 bytes, the upper layer must pad the field to 46 bytes.

3.2.2.5 Duplex Modes of Ethernet

The physical layer of Ethernet can work in either half-duplex or full-duplex mode.

- Half-duplex mode

  The behalf-duplex mode has the following features:

  - Data only be sent or received at any time.
  - The CSMA/CD mechanism is used.
  - The maximum transmission distance is limited.

  Hubs work in half-duplex mode.

- Full-duplex mode

  After Layer 2 switches replace hubs, the shared Ethernet changes to the switched Ethernet, and the half-duplex mode is replaced by the full-duplex mode. As a result, the transmission rate increases greatly, and the maximum throughput doubles the transmission rate.

  The full-duplex mode solves the problem of collisions and eliminates the need for the CSMA/CD mechanism.

  The full-duplex mode has the following features:

  - Data can be sent and received at the same time.
  - The maximum throughput doubles the transmission rate.
  - This mode does not have the limitation on the transmission distance.

All network cards, Layer 2 devices (except hubs), and Layer 3 devices produced support the full-duplex mode.

The following hardware components are required to realize the full-duplex mode:

- Full-duplex network cards and chips
- Physical media with separate data transmission and receiving channels
- Point-to-point connection

3.2.2.6 Auto-Negotiation of Ethernet

- Purpose of auto-negotiation

  The earlier Ethernet adopts the 10 Mbit/s half-duplex mode; therefore, mechanisms such as CSMA/CD are required to guarantee system stability. With development of technologies, the full-duplex mode and 100M Ethernet emerge, which greatly improve the Ethernet performance. How to achieve the compatibility between the earlier and new Ethernet networks becomes a new problem.

  The auto-negotiation technology is introduced to solve this problem. In auto-negotiation, the devices on two ends of a link can choose the same operation parameters by exchanging information. The main parameters to be negotiated are mode (half-duplex or full-duplex), speed, and flow control. After the negotiation succeeds, the devices on two ends operate in the negotiated mode and rate.

  The auto-negotiation of duplex mode and speed is defined in the following standards:

  - 100M Ethernet standard: IEEE 802.3u

    In IEEE 802.3u, auto-negotiation is defined as an optional function.
  - Gigabit Ethernet standard: IEEE 802.3z

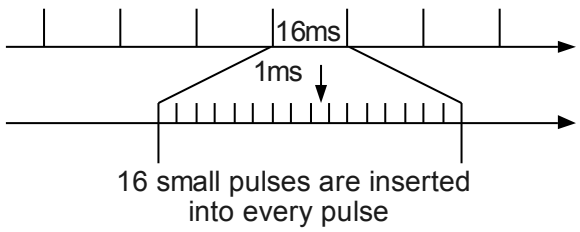
    In IEEE 802.3z, auto-negotiation is defined as a mandatory and default function.

- Principle of auto-negotiation

  Auto-negotiation is an Ethernet procedure by which two connected devices choose common transmission parameters. It allows a network device to transmit the supported operating mode to the peer and receives the operating mode from the peer. In this process, the connected devices first share their capabilities regarding these parameters and then choose the highest performance transmission mode they both support.

  When no data is transmitted over a twisted pair on an Ethernet network, pulses of high frequency are transmitted at an interval of 16 ms to maintain the connections at the link layer. These pulses form a Normal Link Pulse (NLP) code stream. Some pulses of higher frequency can be inserted in the NLP to transmit more information. These pulses form a Fast Link Pulse (FLP) code stream, as shown in **Figure 3-3**. The basic mechanism of auto-negotiation is to encapsulate the negotiation information into FLP.

Figure 3-3 Pulse insertion



Similar to an Ethernet network that uses twisted pair cables, an Ethernet network that uses optical modules and optical fibers also implements auto-negotiation by sending code streams. These code streams are called Configuration (C) code streams. Different from electrical interfaces, optical interfaces do not negotiate traffic transmission rates and they work in duplex mode. Optical interfaces only negotiate flow control parameters.

If auto-negotiation succeeds, the Ethernet card activates the link. Then, data can be transmitted on the link. If auto-negotiation fails, the link is unavailable.

If one end does not support auto-negotiation, the other end that supports auto-negotiation adopts the default operating mode, which is generally 10 Mbit/s half-duplex.

Auto-negotiation is implemented based on the chip design at the physical layer. As defined in IEEE 802.3, auto-negotiation is implemented in any of the following cases:

- A faulty link recovers.
- A device is power recycled.
- Either of two connected devices resets.
- A renegotiation request packet is received.

In other cases, two connected devices do not always send auto-negotiation code streams. Auto-negotiation does not use special packets or bring additional protocol costs.

- Auto-negotiation rules for interfaces

  Two connected interfaces can communicate with each other only when they are working in the same working mode.

  - If both interfaces work in the same non-auto-negotiation mode, the interfaces can communicate.
  - If both interfaces work in auto-negotiation mode, the interfaces can communicate through negotiation. The negotiated working mode depends on the interface with lower capability (specifically, if one interface works in full-duplex mode and the other interface works in half-duplex mode, the negotiated working mode is half-duplex). The auto-negotiation function also allows the interfaces to negotiate about the flow control function.
  - If a local interface works in auto-negotiation mode and the remote interface works in a non-auto-negotiation mode, the negotiated working mode of the local interface depends on the working mode of the remote interface.

3.2.2.7 Collision Domain and Broadcast Domain

Collision Domain

On a legacy Ethernet network using thick coaxial cables as a transmission medium, multiple nodes on a shared medium share the bandwidth on the link and compete for the right to use the link. A network collision occurs when more than one node attempts to send a packet on this link at the same time. The carrier sense multiple access with collision detection (CSMA/CD) mechanism is used to solve the problem of collisions. Once a collision occurs on a link, the CSMA/CD mechanism prevents data transmission on this link within a specified time. Collisions are inevitable on an Ethernet network, and the probability that collision occurs increases when more nodes are deployed on a shared medium. All nodes on a shared medium constitute a collision domain. All the nodes in a collision domain compete for bandwidth. Packets sent from

a node, including unicast, multicast, and broadcast packets, can reach all the other nodes in the collision domain.

Broadcast Domain

Packets are broadcast in a collision domain, which results in a low bandwidth efficiency and degrades packet processing performance of network devices. Therefore, broadcasting of packets must be restricted. For example, the ARP protocol sends broadcast packets to obtain MAC addresses mapping specified IP addresses. The all 1s MAC address FFFF-FFFF-FFFF is the broadcast MAC address. All nodes must process data frames with this MAC address as the destination MAC address. A broadcast domain is a group of nodes, among which broadcast packet from one node can reach all the other nodes. A network bridge forwards unicast packets according to its MAC address table and forwards broadcast packets to all its ports. Therefore, nodes connected to all ports of a bridge belong to a broadcast domain, but each port belongs to a different collision domain.

3.2.2.8 MAC Sub-layer

Functions of the MAC Sub-layer

The MAC sub-layer has the following functions:

- Provides access to physical links.

  The MAC sub-layer is associated with the physical layer. That is, different MAC sub-layers provide access to different physical layers.

  Ethernet has two types of MAC sub-layers:

  - Half-duplex MAC: provides access to the physical layer in half-duplex mode.
  - Full-duplex MAC: provides access to the physical layer in full-duplex mode.

  The two types of MAC sub-layers are integrated in a network interface card. After the network interface card is initialized, auto-negotiation is performed to choose an operation mode, and then a MAC sub-layer is chosen according to the operation mode.

- Identifies stations at the data link layer.

  The MAC sub-layer reserves a unique MAC address for each station.

  The MAC sub-layer uses a MAC address to uniquely identify a station.

  MAC addresses are managed by Institute of Electrical and Electronics Engineers (IEEE) and allocated in blocks. An organization, generally a device manufacturer, obtains a unique address block from IEEE. The address block is called an Organizationally Unique Identifier (OUI). Using the OUI, the organization can allocate MAC addresses to 16777216 devices.

  A MAC address has 48 bits, which are generally expressed in 12-digit dotted hexadecimal notation. For example, the 48-bit MAC address 000000001110000011111100001110011000000000110100 is represented by 00e0.fc39.8034.

  The first 6 digits in dotted hexadecimal notation stand for the OUI, and the last 6 digits are allocated by the vendor. For example, in 00e0.fc39.8034, 00e0.fc is the OUI allocated by IEEE to Huawei, and 39.8034 is the address number allocated by Huawei.

  The second bit of a MAC address indicates whether the address is globally unique or locally unique. Ethernet uses globally unique MAC addresses.

  MAC addresses are divided into the following types:

- Physical MAC address

  A physical MAC address is burned into hardware (such as a network interface card) and uniquely identifies a terminal on the Ethernet.

- Broadcast MAC address

  A broadcast MAC address indicates all the terminals on a network.

  The 48 bits of a broadcast MAC address are all 1s, such as ffff.ffff.ffff.

- Multicast MAC address

  A multicast MAC address indicates a group of terminals on a network.

  The eighth bit of a multicast MAC address is 1, such as 00000001101110110011101010111010101111101010100**0**.

- Transmits data over the data link layer. After receiving data from the LLC sub-layer, the MAC sub-layer adds the MAC address and control information to the data, and then transmits the data to the physical link. In the process, the MAC sub-layer provides other functions such as the check function.

  Data is transmitted at the data link layer as follows:

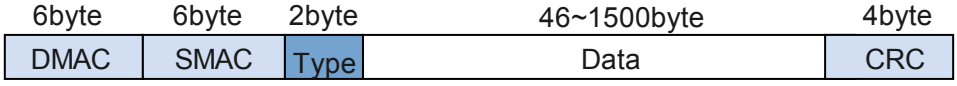
  1. The upper layer delivers data to the MAC sub-layer.
  2. The MAC sub-layer stores the data in the buffer.
  3. The MAC sub-layer adds the destination MAC address and source MAC address to the data, calculates the length of the data frame, and forms an Ethernet frame.
  4. The Ethernet frame is sent to the peer according to the destination MAC address.
  5. The peer compares the destination MAC address with entries in the MAC address table.
     - If a matching entry is found, the frame is accepted.
     - If no matching entry is found, the frame is discarded.

  The preceding describes frame transmission in unicast mode. After an upper-layer application is added to a multicast group, the data link layer generates a multicast MAC address according to the application, and then adds the multicast MAC address to the MAC address table. The MAC sub-layer receives frames with the multicast MAC address and transmits the frames to the upper layer.

Ethernet Frame Structure

- Format of an Ethernet_II frame

  Figure 3-4 Format of an Ethernet_II frame



  The fields of a Ethernet_II frame are described as follows:

  - DMAC

    It indicates the destination MAC address. DMAC specifies the receiver of the frame.

- SMAC

  It indicates the source MAC address. SMAC specifies the station that sends the frame.

- Type

  The 2-byte Type field identifies the upper layer protocol of the Data field. The receiver can know the meaning of the Data field according to the Type field.

  Ethernet allows multiple protocols to coexist on a LAN. The hexadecimal values in the Type field of an Ethernet_II frame stand for different protocols.

  - Frames with the Type field value 0800 are IP frames.
  - Frames with the Type field value 0806 are Address Resolution Protocol (ARP) frames.
  - Frame with the Type field value 8035 are Reverse Address Resolution Protocol (RARP) frames.
  - Frames with the Type field value 8137 are Internetwork Packet Exchange (IPx) and Sequenced Packet Exchange (SPx) frames.

- Data

  The minimum length of the Data field is 46 bytes, which ensures that the frame is at least 64 bytes in length. The 46-byte Data field is required even if only 1-byte information needs to be transmitted.

  If the payload of the Data field is less than 46 bytes, the Data field must be padded to 46 bytes.

  The maximum length of the Data field is 1500 bytes.

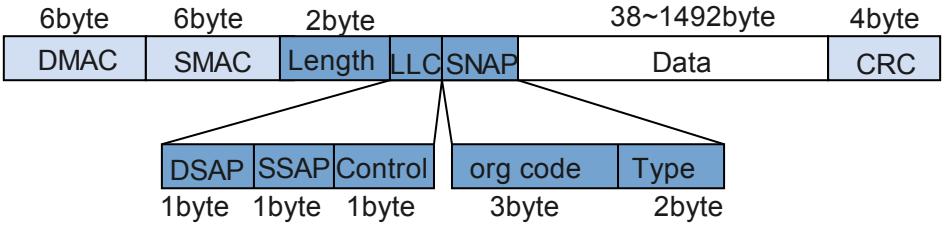
- CRC

  The Cyclic Redundancy Check (CRC) field provides an error detection mechanism.

  Each sending device calculates a CRC code containing the DMAC, SMAC, Type, and Data fields. Then the CRC code is filled into the 4-byte CRC field.

- Format of an IEEE 802.3 frame

Figure 3-5 Format of an IEEE 802.3 frame



As shown in **Figure 3-5**, the format of an IEEE 802.3 frame is similar to that of an Ethernet_II frame except that the Type field is changed to the Length field in an IEEE 802.3 frame, and the LLC field and the Sub-Network Access Protocol (SNAP) field occupy 8 bytes of the Data field.

- Length

  The Length field specifies the number of bytes in the Data field.

- LLC

The LLC field consists of three sub-fields: Destination Service Access Point (DSAP), Source Service Access Point (SSAP), and Control.

- SNAP

  The SNAP field consists of the Org Code field and the Type field. Three bytes in the Org Code field are all 0s. The Type field functions the same as the Type field in Ethernet_II frames.

For description about other fields, see the description of Ethernet_II frames.

Based on the values of DSAP and SSAP, IEEE 802.3 frames can be divided into the following types:

- If DSAP and SSAP are both 0xff, the IEEE 802.3 frame changes to a Netware-Ethernet frame that carries NetWare data.
- If DSAP and SSAP are both 0xaa, the IEEE 802.3 frame changes to an Ethernet_SNAP frame.

  Ethernet_SNAP frames can be encapsulated with data of multiple protocols. The SNAP can be considered as an extension of the Ethernet protocol. SNAP allows vendors to define their own Ethernet transmission protocols.

  The Ethernet_SNAP standard is defined by IEEE 802.1 to guarantee interoperability between IEEE 802.3 LANs and Ethernet networks.
- Other values of DSAP and SSAP indicate IEEE 802.3 frames.

3.2.2.9 LLC Sub-layer

The MAC sub-layer supports two types of frame: IEEE 802.3 frames and Ethernet_II frames. In an Ethernet_II frame, the Type field identifies the upper layer protocol. Therefore, only the MAC sub-layer is required on a device, and the LLC sub-layer does not need to be realized.

In an IEEE 802.3 frame, the LLC sub-layer defines useful features in addition to traditional services of the data link layer. All these features are provided by the sub-fields of DSAP, SSAP, and Control.

The following lists three types of point-to-point services:

- Connectionless service

  Currently, the Ethernet implements this service.
- Connection-oriented service

  A connection is set up before data is transmitted. The reliability of data is guaranteed during the transmission.
- Connectionless data transmission with acknowledgement

  A connection is not required before data transmission. The acknowledgement mechanism is used to improve the reliability.

The following is an example that describes the applications of SSAP and DSAP. Assume that terminals A and B use connection-oriented services. Data is transmitted in the following process:

1. A sends a frame to B to require the establishment of a connection with B.
2. If B has enough resources, it returns an acknowledgement message that contains a Service Access Point (SAP). The SAP identifies the connection required by A.

3. After receiving the acknowledgement message, A knows that B has set up a local connection with A. After creating a SAP, A sends a message containing the SAP to B. The connection is set up.
4. The LLC sub-layer of A encapsulates the data into a frame. The DSAP field is filled in with the SAP sent by B; the SSAP field is filled in with the SAP created by A. Then the LLC sub-layer sends the frame to the MAC sub-layer of A.
5. The MAC sub-layer of A adds the MAC address and the Length field into the frame, and then sends the frame to the data link layer.
6. After the frame is received at the MAC sub-layer of B, the frame is transmitted to the LLC sub-layer. The LLC sub-layer figures out the connection to which the frame belongs according to the DSAP field.
7. After checking and acknowledging the frame based on the connection type, the LLC sub-layer of B transmits the frame to the upper layer.
8. After the frame reaches its destination, A instructs B to release the connection by sending a frame. At this time, the communications end.

3.2.3 Switching on Ethernet

This section describes Ethernet switching.

3.2.3.1 Layer 2 Switching

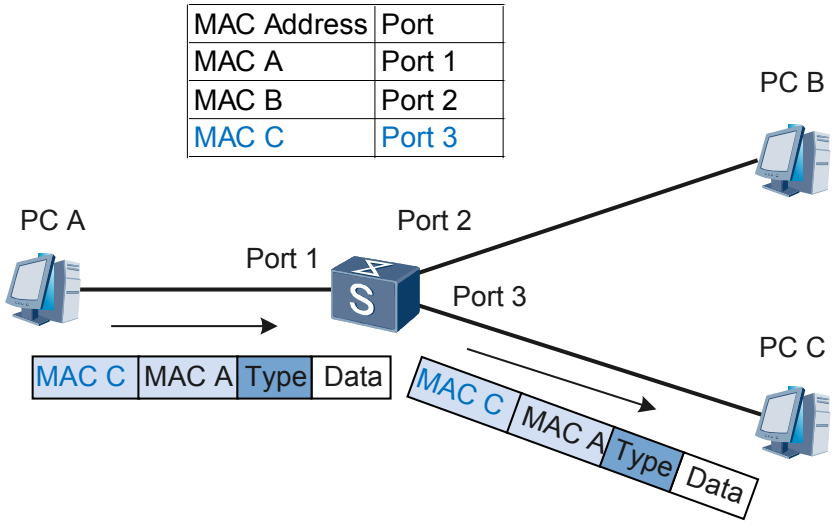
A Layer 2 device works at the second layer of the OSI model and forwards data packets based on media access control (MAC) addresses. Ports on a Layer 2 device send and receive data independently and belong to different collision domains. Collision domains are isolated at the physical layer so that collisions will not occur between hosts (or networks) connected through this Layer 2 device due to uneven traffic rates on these hosts (or networks).

A Layer 2 device parses and learns source MAC addresses of Ethernet frames and maintains a mapping table of MAC addresses and ports. This table is called a MAC address table. When receiving an Ethernet frame, the device searches for the destination MAC address of the frame in the MAC table to determine through which port to forward this frame.

1. When the Layer 2 device receives an Ethernet frame, it records the source MAC address and the inbound port of the frame in the MAC address table to guide Layer 2 forwarding. If the same MAC address entry exists in the MAC address table, the device resets the aging time of the entry. An aging mechanism is used to maintain entries in the MAC address table. Entries that are not updated within the aging time are deleted from the MAC address table.
2. The device looks up the MAC address table based on the destination MAC address of the Ethernet frame. If no matching entry is found, the device forwards the frame to all its ports except the port from which the frame is received. If the destination MAC address of the frame is a broadcast address, the device forwards the frame to all its ports except the port from which the frame is received. If a matching entry is found in the MAC address table, the device forwards the frame to the port specified in the entry.

According to the preceding forwarding process, a Layer 2 device maintains a MAC address table and forwards Ethernet frames based on destination MAC addresses. This forwarding mechanism fully uses network bandwidth and improves network performance. **Figure 3-6** shows an example of Layer 2 switching

Figure 3-6 Layer 2 switching example



Although Layer 2 devices can isolate collision domains, they cannot isolate broadcast domains. As described in the Layer 2 forwarding process, broadcast packets and packets that do not match nay entry in the MAC address table are forwarded to all ports (except the port from which the frame is received). Packet broadcasting consumes much bandwidth on network links and brings security issues. Routers can isolate broadcast domains, but high costs and low forwarding performance of routers limit the application of routers in Layer 2 forwarding. The virtual local area network (VLAN) technology is introduced to solve this problem in Layer 2 switching.

3.2.3.2 Layer 3 Switching

Background of Layer 3 Switches

In early stage of network deployment, most local area networks (LANs) were established using Layer 2 switches, and routers completed communication between LANs. At that time, intra-LAN traffic accounted for most of network traffic and little traffic was transmitted between LANs. A few routers were enough to handle traffic transmission between LANs.

As data communication networks expand and more services emerge on the networks, increasing traffic needs to be transmitted between networks. Routers cannot adapt to this development trend because of their high costs, low forwarding performance, and small port quantities. New devices capable of high-speed Layer 3 forwarding are required. Layer 3 switches are such devices.

Routers use CPUs to complete Layer 3 forwarding, whereas Layer 3 switches use hardware to complete Layer 3 forwarding. Hardware forwarding has a much higher performance than software forwarding (CPU based forwarding). Switches cannot replace routers in all scenarios because routers provide rich interface types, good service class control, and powerful routing capabilities that Layer 3 switches cannot provide.

Layer 3 Forwarding Mechanism

Layer 3 switches divide a Layer 2 network into multiple VLANs. They implement Layer 2 switching within the VLANs and Layer 3 IP connectivity between VLANs. Two hosts on different networks communicate with each other through the following process:

1. Before the source host starts communicating with the destination host, it compares its own IP address with the IP address of the destination host. If IP addresses of the two hosts have the same network ID (calculated by an AND operation between the IP addresses and masks), the hosts are located on the same network segment. In this case, the source host sends an Address Resolution Protocol (ARP) request to the destination host. After receiving an ARP reply from the destination host, the source host obtains the MAC address of the destination host and sends packets to this destination MAC address.
2. If the source and destination hosts are located on different network segments, the source host sends an ARP request to obtain the MAC address mapping the gateway IP address. After receiving an ARP reply from the gateway, the source host sends packets to the MAC address of the gateway. In these packets, the source IP address is the IP address of the source host, and destination IP address is still the IP address of the destination host.

The following is the detailed Layer 3 switching process.

As shown in **Figure 3-7**, the source and destination hosts connect to the same Layer 3 switch but belong to different VLANs (network segments). Both the two hosts are located on the directly connected network segments of the Layer 3 switch, so the routes to the IP addresses of the hosts are direct routes.

Figure 3-7 Layer 3 forwarding

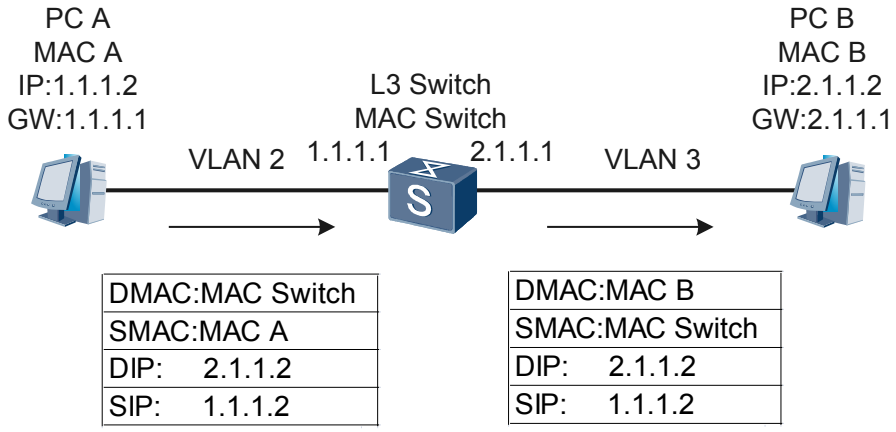


Figure 3-7 shows the MAC addresses, IP addresses, and gateway addresses of the hosts, MAC address of the Layer 3 switch, and IP addresses of Layer 3 interfaces configured in VLANs on the Layer 3 switch. The process of a ping from PC A to PC B is as follows (the Layer 3 switch has not created any MAC address entry):

1. PC A finds that the destination IP address 2.1.1.2 (PC B) is on a different network segment than its own IP address. Therefore, PC A sends an ARP request to request for the MAC address mapping the gateway address 1.1.1.1.
2. L3 Switch receives the ARP request from PC A and finds that 1.1.1.1 is the IP address of its own Layer 3 interface. L3 switch then sends an ARP reply to PC A. The ARP reply carries the MAC address of its Layer 3 interface (MAC Switch). In addition, L3 switch adds the mapping between the IP address and MAC address of PC A (1.1.1.2 and MAC A) to its ARP table. The IP address and MAC address of PC A are carried in the ARP request sent from PC A.
3. After PC A receives the ARP reply from the gateway (L3 Switch), it sends an ICMP request packet. In the ICMP request packet, the destination MAC address (DMAC) is MAC Switch;

the source MAC address (SMAC) is MAC A; the source IP address (SIP) is 1.1.1.2; the destination IP address (DIP) is 2.1.1.2.

4. When L3 Switch receives the ICMP request packet, it updates the matching MAC address entry according to the source MAC address and VLAN ID of the packet. Then L3 Switch looks up the MAC address table according to the destination MAC address and VLAN ID of the packet and finds the entry with the MAC address of its Layer 3 interface, the packet needs to be forwarded at Layer 3. Then L3 Switch looks up Layer 3 forwarding entries of the switching chip to guide Layer 3 forwarding.
5. The switching chip loops up Layer 3 forwarding entries according to the destination IP address of the packet. The entry lookup fails because no entry has been created. The switching chip then sends the packet to the CPU for software processing.
6. The CPU looks up the software routing table according to the destination IP address of the packet and finds a directly connected network segment, network segment of PC B. Then the CPU looks up its ARP table, and the lookup still fails. Therefore, L3 Switch sends an ARP request to all ports in VLAN 3 (network segment of PC B), to request the MAC address mapping IP address 2.1.1.2.
7. After PC B receives the ARP request from L3 Switch, it checks the ARP request and finds that 2.1.1.2 is its own IP address. PC B then sends an ARP reply carrying its MAC address (MAC B). Meanwhile, PC B records the mapping between the IP address and MAC address of L3 Switch (2.1.1.1 and MAC Switch) in its ARP table.
8. When L3 Switch receives the ARP reply from PC B, it records the mapping between the IP address and MAC address of PC B (2.1.1.2 and MAC B) in its ARP table. L3 Switch changes the destination MAC address in the ICMP request packet sent from PC A to MAC B and changes the source MAC address to its own MAC address (MAC Switch), and then sends the ICMP request to PC B. The Layer 3 forwarding entry containing the IP address and MAC address of PC B, outbound VLAN ID, and outbound port is also added to the Layer 3 forwarding of the switching chip. Subsequent packets sent from PC A to PC B are directly forwarded according to this hardware entry.
9. When PC B receives the ICMP request packet from L3 Switch, it sends an ICMP reply packet to PC A. The forwarding process for the ICMP reply packet is similar to that for the ICMP request packet except that the ICMP reply packet is directly forwarded to PC A by the switching chip according to the hardware entry. The reason is that L3 Switch has obtained the mapping between the IP address and MAC address of PC A and added matching Layer 3 forwarding entry to the L3 forwarding table of the switching chip.
10. Subsequent packets exchanged between PC A and PC B are forwarded following the same process: MAC address table lookup, Layer 3 forwarding table lookup, and hardware forwarding by the switching chip.

In a summary, a Layer 3 switch provides high-speed Layer 3 switching through one routing process (forwarding the first packet to the CPU and creating a hardware Layer 3 forwarding entry) and multiple switching processes (hardware forwarding of subsequent packets).

3.3 IP Routing Basic Configuration

You can configure IP routing to learn about basic parameters for IP routing.

3.3.1 Introduction to IP Routing

Routing is the basic element of data communication networks. It is the process of selecting paths on a network along which packets are sent from a source to a destination.

Routes are classified into the following types based on the destination address:

- Network segment route: The destination is a network segment. The subnet mask of an IPv4 destination address is less than 32 bits or the prefix length of an IPv6 destination address is less than 128 bits.
- Host route: The destination is a host. The subnet mask of an IPv4 destination address is 32 bits or the prefix length of an IPv6 destination address is 128 bits.

Routes are classified into the following types based on whether the destination is directly connected to a router:

- Direct route: The router is directly connected to the network where the destination is located.
- Indirect route: The router is indirectly connected to the network where the destination is located.

Routes are classified into the following types based on the destination address type:

- Unicast route: The destination address is a unicast address.
- Multicast route: The destination address is a multicast address.

3.3.2 Principles

This section describes the implementation of IP Routing.

3.3.2.1 Routers and Routing Principles

On the Internet, network connecting devices control traffic and ensure data transmission quality. Common network connecting devices include hubs, bridges, switches, and routers. These network devices have similar basic principles. The following uses a router as an example to describe basic principles.

As a typical network connecting device, a router selects routes and forwards packets. Upon receiving a packet, a router selects a proper path, which has one or multiple hops, to send the packet to the next router according to the destination address in the packet. The last router is responsible for sending the packet to the destination host.

A route is a path along which packets are sent from the source to the destination. When multiple routes are available to send packets from a router to the destination, the router can select the optimal route from an IP routing table to forward the packets. Optimal route selection depends on the routing protocol preferences and metrics of routes. When multiple routes have the same routing protocol preference and metric, load balancing can be implemented among these routes to relieve network pressure. When multiple routes have different routing protocol preferences and metrics, route backup can be implemented among these routes to improve network reliability.

3.3.2.2 Routing Table and FIB Table

Routers forward packets based on routing tables and forwarding information base (FIB) tables. Each router maintains at least one routing table and one FIB table. Routers select routes based on routing tables and forward packets based on FIB tables.

Routing Table

Each router maintains a local core routing table, and each routing protocol maintains its routing table.

- Local core routing table

  A router uses the local core routing table to store protocol routes and preferred routes. The router then sends the preferred routes to the FIB table to guide packet forwarding. The router selects routes according to the priorities of protocols and costs stored in the routing table.

- Protocol routing table

  A protocol routing table stores the routing information discovered by the protocol.

  A routing protocol can import and advertise the routes that are discovered by other routing protocols. For example, if a router that runs the Open Shortest Path First (OSPF) protocol needs to use OSPF to advertise direct routes, static routes, or Intermediate System-Intermediate System (IS-IS) routes, the router must import the routes into the OSPF routing table.

Routing Table Contents

You can run the **display ip routing-table** command on a router to view brief information about the routing table of the router. The command output is as follows:

```
<Huawei> display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 14       Routes : 14

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0          RD   10.137.216.1    GigabitEthernet
2/0/0
     10.10.10.0/24  Direct  0    0           D   10.10.10.10     GigabitEthernet
1/0/0
    10.10.10.10/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   10.10.10.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
     10.10.11.0/24  Direct  0    0           D   10.10.11.1      LoopBack0
     10.10.11.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   10.10.11.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
   10.137.216.0/23  Direct  0    0           D   10.137.217.208  GigabitEthernet
2/0/0
 10.137.217.208/32  Direct  0    0           D   127.0.0.1       InLoopBack0
 10.137.217.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

A routing table contains the following key data for each IP packet:

- Destination: identifies the destination IP address or the destination network address of an IP packet.
- Mask: works with the destination address to identify the address of the network segment where the destination host or router resides.

  The network segment address of the destination host or router is obtained through the "AND" operation on the destination address and network mask. For example, if the destination address is 1.1.1.1 and the mask is 255.255.255.0, the address of the network segment where the host or router resides is 1.1.1.0.

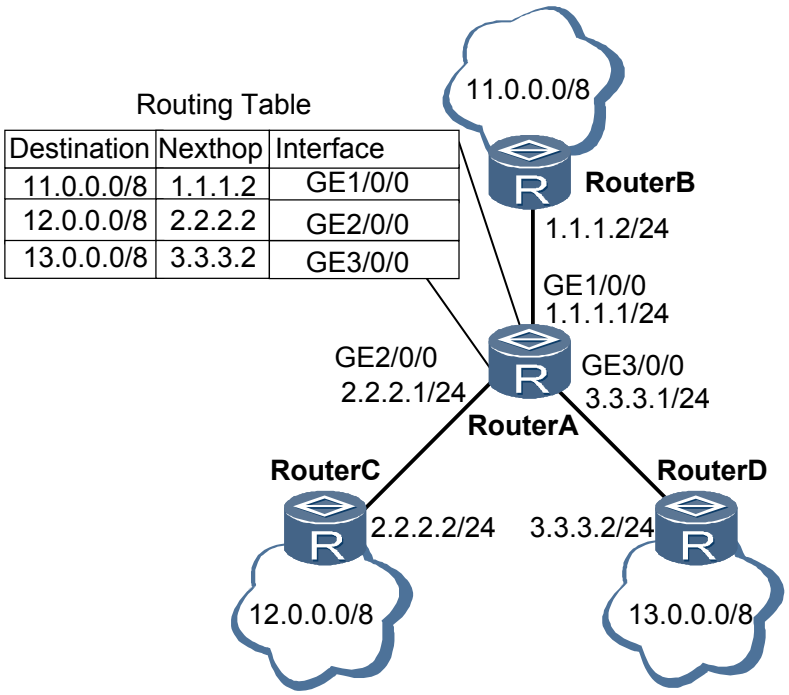
  The network mask is composed of several consecutive 1s. These 1s can be expressed in either the dotted decimal notation or the number of consecutive 1s in the mask. For example, the network mask can be expressed either as 255.255.255.0 or 24.
- Proto: indicates the protocol through which routes are learned.
- Pre: indicates the routing protocol preference of a route. There may multiple routes to the same destination, which have different next hops and outbound interfaces. These routes may be discovered by different routing protocols or manually configured. A router selects the route with the highest preference (the smallest value) as the optimal route. For the routing protocol preference, see Routing Protocol Preference.
- Cost: indicates the route cost. When multiple routes to the same destination have the same preference, the route with the lowest cost is selected as the optimal route.

  NOTE

  The Preference value is used to compare the preferences of different routing protocols, while the Cost value is used to compare the preferences of different routes of the same routing protocol.
- NextHop: indicates the IP address of the next device that an IP packet passes through.
- Interface: indicates the outbound interface through which an IP packet is forwarded.

As shown in **Figure 3-8**, RouterA connects to three networks, so it has three IP addresses and three outbound interfaces. **Figure 3-8** shows the routing table of RouterA.

Figure 3-8 Routing table



Matching with FIB Table

After route selection, routers send active routes in the routing table to the FIB table. When a router receives a packet, the router searches the FIB table for the optimal route to forward the packet.

Each entry in the FIB table contains the physical or logical interface through which a packet is sent to a network segment or host to reach the next router. An entry also indicates whether the packet can be sent to a destination host in a directly connected network.

The router performs the "AND" operation on the destination address in the packet and the network mask of each entry in the FIB table. The router then compares the result of the "AND" operation with the entries in the FIB table to find a match and chooses the optimal route to forward packets according to the longest match.

Assume that a router has the following routing table:

```
Routing Tables:
Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface
 0.0.0.0/0    Static   60   0        D   120.0.0.2      GigabitEthernet1/0/0
 8.0.0.0/8    RIP      100  3        D   120.0.0.2      GigabitEthernet1/0/0
 9.0.0.0/8    OSPF     10   50       D   20.0.0.2       GigabitEthernet3/0/0
 9.1.0.0/16   RIP      100  4        D   120.0.0.2      GigabitEthernet2/0/0
 20.0.0.0/8   Direct   0    0        D   20.0.0.1       GigabitEthernet4/0/0
```

After receiving a packet that carries the destination address 9.1.2.1, the router searches the following FIB table:

```
 FIB Table:
 Total number of Routes : 5
Destination/Mask   Nexthop         Flag TimeStamp     Interface             TunnelID
0.0.0.0/0          120.0.0.2        SU   t[37]         GigabitEthernet1/0/0  0x0
8.0.0.0/8          120.0.0.2        DU   t[37]         GigabitEthernet1/0/0  0x0
9.0.0.0/8          20.0.0.2         DU   t[9992]       GigabitEthernet3/0/0  0x0
9.1.0.0/16         120.0.0.2        DU   t[9992]       GigabitEthernet2/0/0  0x0
20.0.0.0/8         20.0.0.1         U    t[9992]       GigabitEthernet4/0/0  0x0
```

The router performs the "AND" operation on the destination address 9.1.2.1 and the masks 0, 8, and 16 to obtain the network segment addresses: 0.0.0.0/0, 9.0.0.0/8, and 9.1.0.0/16. The three addresses match three entries in the FIB table. The router chooses the entry 9.1.0.0/16 according to the longest match, and forwards the packet through GigabitEthernet2/0/0.

3.3.2.3 Route Metric

A route metric specifies the cost of a route to a specified destination address. The following factors often affect the route metric:

- Path length

  The path length is the most common factor affecting the route metric. Link-state routing protocols allow you to assign a link cost for each link to identify the path length of a link. In this case, the path length is the sum of link costs of all the links that packets pass through. Distance-vector routing protocols use the hop count to identify the path length. The hop count is the number of devices that packets pass through from the source to the destination. For example, the hop count from a router to its directly connected network is 0, and the

hop count from a router to a network that can be reached through another router is 1. The rest can be deduced in the same manner.

- Network bandwidth

  The network bandwidth is the transmission capability of a link. For example, a 10-Gigabit link has a higher transmission capability than a 1-Gigabit link. Although bandwidth defines the maximum transmission rate of a link, routes over high-bandwidth links are not necessarily better than routes over low-bandwidth links. For example, when a high-bandwidth link is congested, forwarding packets over this link will require more time.

- Load

  The load is the degree to which a network resource is busy. You can calculate the load by calculating the CPU usage and packets processed per second. Monitoring the CPU usage and packets processed per second continually helps learn about network usage.

- Communication cost

  The communication cost measures the operating cost of a route over a link. The communication cost is another important indicator, especially if you do not care about network performance but the operating expenditure.

3.3.2.4 Load Balancing and Route Backup

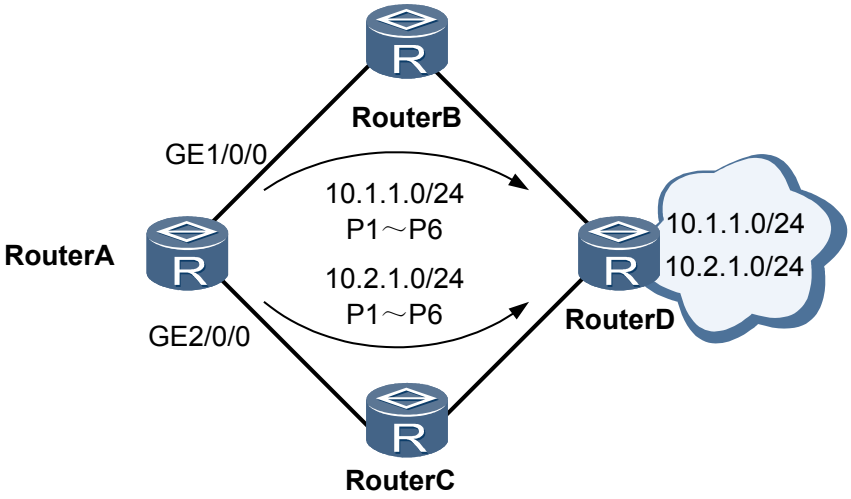
When multiple routes have the same routing protocol preference and metric, these routes are called equal-cost routes, among which load balancing can be implemented. When multiple routes have different routing protocol preferences and metrics, route backup can be implemented among these routes.

Load Balancing

Routers support the multi-route mode, allowing you to configure multiple routes with the same destination and preference. If the destinations and costs of multiple routes discovered by the same routing protocol are the same, load balancing can be performed among the routes.

During load balancing, a router forwards packets based on the 5-tuple (source IP address, destination IP address, source port, destination port, and transport protocol) in the packets. When the 5-tuple information is the same, the router always chooses the next-hop address that is the same as the last one to send packets. When the 5-tuple information is different, the router forwards packets over idle paths.

Figure 3-9 Networking diagram of load balancing



As shown in **Figure 3-9**, RouterA forwards the first packet P1 to 10.1.1.0/24 through GE1/0/0 and needs to forward subsequent packets to 10.1.1.0/24 and 10.2.1.0/24 respectively. The forwarding process is as follows:

- When forwarding the second packet P2 to 10.1.1.0/24, RouterA forwards P2 and subsequent packets destined for 10.1.1.0/24 through GE1/0/0 if it finds that the 5-tuple information of P2 is the same as that of P1 destined for 10.1.1.0/24.
- When forwarding the first packet P1 to 10.2.1.0/24, RouterA forwards this packet and subsequent packets destined for 10.2.1.0/24 through GE2/0/0 if it finds that the 5-tuple information of P1 destined for 10.2.1.0/24 is different from that of P1 destined for 10.1.1.0/24.

Route Backup

Route backup can improve network reliability. You can configure multiple routes to the same destination as required. The route with the highest preference functions as the primary route, and the other routes with lower preferences function as backup routes.

A router generally uses the primary route to forward data. When the primary link fails, the primary route becomes inactive. The router selects a backup route with the highest preference to forward data. In this manner, data is switched from the primary route to a backup route. When the primary link recovers, the router selects the primary route to forward data again because the primary route has the highest preference. Data is then switched back from the backup route to the primary route.

3.3.2.5 Route Convergence

Definition

Route convergence is the action of recalculating routes to replace existing routes in the case of network topology changes. The integration of network services urgently requires differentiated services. Routes for key services, such as Voice over IP (VoIP), video conferences, and multicast services, need to be converged rapidly, while routes for common services can be converged

relatively slowly. In this case, the system needs to converge routes based on their convergence priorities to improve network reliability.

Priority-based convergence is a mechanism that allows the system to converge routes based on the convergence priority. You can set different convergence priorities for routes: critical, high, medium, and low, which are in descending order of priority. The system then converges routes according to the scheduling weight to guide service forwarding.

Principles

Routing protocols first compute and deliver routes of high convergence priorities to the system. You can reconfigure the scheduling weight values as required. **Table 3-6** lists the default convergence priorities of public routes.

Table 3-6 Default convergence priorities of public routes

Routing Protocol or Route Type	Convergence Priority
Direct	high
Static	medium
32-bit host routes of OSPF and IS-IS	medium
OSPF routes (excluding 32-bit host routes)	low
IS-IS routes (excluding 32-bit host routes)	low
RIP	low
BGP	low

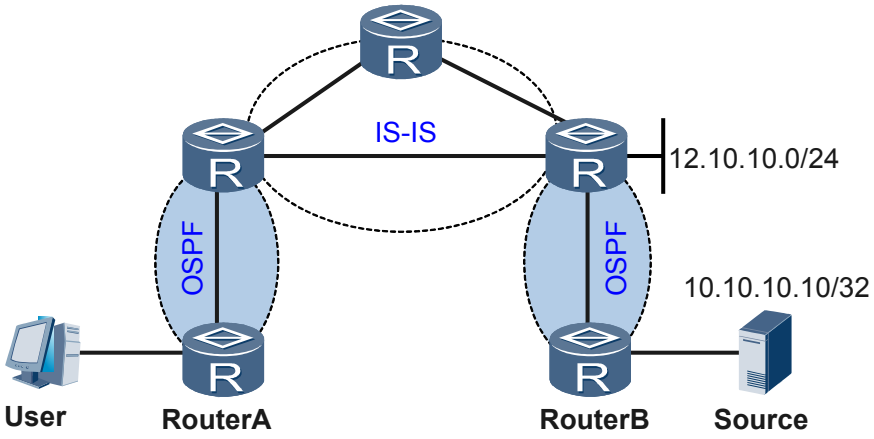
NOTE

For private routes, only the convergence priority of 32-bit host routes of OSPF and IS-IS is identified as medium and the convergence priorities of the other routes are identified as low.

Priority-based Route Convergence

Figure 3-10 shows the networking for multicast services. OSPF and IS-IS run on the network; the receiver connects to RouterA; the multicast source server 10.10.10.10/32 connects to RouterB. The route to the multicast source server must be converged faster than other routes, such as 12.10.10.0/24. You can set the convergence priority of route 10.10.10.10/32 to be higher than that of route 12.10.10.0/24. When routes are converged on the network, the route to the multicast source server 10.10.10.10/32 is converged first. This ensures the transmission of multicast services.

Figure 3-10 Networking diagram of priority-based route convergence



3.3.2.6 Default Routes

Default routes are special routes, which are used only when packets to be forwarded do not match any routing entry in a routing table. If the destination address of a packet does not match any entry in the routing table, the packet is sent through a default route. If no default route exists and the destination address of the packet does not match any entry in the routing table, the packet is discarded. An Internet Control Message Protocol (ICMP) packet is then sent, informing the originating host that the destination host or network is unreachable.

In a routing table, a default route is the route to network 0.0.0.0 (with the mask 0.0.0.0). You can run the **display ip routing-table** command to check whether a default route is configured. Generally, administrators can manually configure default static routes. Default routes can also be generated through dynamic routing protocols such as OSPF and IS-IS.

3.3.3 References

This section lists references of IP Routing.

None

3.4 MAC Address Table Configuration

This chapter provides the basics for MAC address table configuration, configuration procedure, and configuration examples.

3.4.1 Introduction to MAC

This section describes the definition, background, and functions of MAC.

A Media Access Control (MAC) address defines the location of a network device. A MAC address consists of 48 bits and is displayed as a 12-digit hexadecimal number. The 0 to 23 bits are assigned by IETF and other institutions to identify vendors, and the 24 to 47 bits are the unique ID assigned by vendors to identify their network adapters.

MAC addresses are classified into the following types:

- Physical MAC address: identifies a device on a LAN. Each physical MAC address is globally unique.
- Broadcast MAC address: indicates all devices on a LAN. The broadcast address is all 1s (FF-FF-FF-FF-FF-FF).
- Multicast MAC address: indicates a group of stations on a LAN. All the MAC addresses with the eighth bit as 1 are the multicast MAC address, excluding the broadcast MAC address.

3.4.2 Principles

This section describes principles of MAC address table.

3.4.2.1 MAC Address Table

Each device maintains a MAC address table. A MAC address table records the MAC address, VLAN ID and outbound interfaces learned from other devices. When forwarding a data frame, the device searches the MAC table for the outbound interface according to the destination MAC address and VLAN ID in the frame. This helps the device reduce broadcasting.

Packet Forwarding Based on the MAC Address Table

The device forwards packets based on the MAC address table in either of the following modes:

- Unicast mode: If the destination MAC address of a packet can be found in the MAC address table, the device forwards the packet through the outbound interface specified in the matching entry.
- Broadcast mode: If a packet is a broadcast or multicast packet or its destination MAC address cannot be found in the MAC address table, the device broadcasts the packet to all the interfaces in the VLAN except the inbound interface.

Categories of MAC Address Entries

The MAC address entry can be classified into the dynamic entry, the static entry and the blackhole entry.

- The dynamic entry is created by learning the source MAC address. It has aging time.
- The static entry is set by users and is delivered to each SIC. It does not age.
- The blackhole entry is used to discard the frame with the specified source MAC address or destination MAC address. Users manually set the blackhole entries and send them to each SIC. Blackhole entries have no aging time.

The dynamic entry will be lost after the system is reset or the interface board is hot swapped or reset. The static entry and the blackhole entry, however, will not be lost.

Generation of a MAC address entry

MAC address entries are generated automatically or configured manually.

- Automatically Generated MAC Address Entries

  MAC address entries are learned by the system automatically. For example, SwitchA and HostB are connected. When SwitchB sends a frame to SwitchA, SwitchA obtains the source

MAC address (the MAC address of HostB) from the frame and adds the source MAC address and the interface number to the MAC address table. When SwitchA receives a frame sent to HostB again, SwitchA can search the MAC address table to find the correct outbound interface.

The entries in the MAC table will not be valid all the time. Each entry has its own lifetime. If the entry has not been refreshed at the expiration of its lifetime, the device will delete that entry from the MAC table. That lifetime is called aging time. If the entry is refreshed before its lifetime expires, the device resets the aging time for it.

- Manually Configured MAC Address Entries

  When creating MAC address entries by itself, the device cannot identify whether the packets are from the legal users or the hackers. This threatens the network safety.

  Hackers can fake the source MAC address in attack packets. The packet with a forged address enters the device from the other port. Then the device learns a fault MAC table entry. That is why the packets sent to the legal users are forwarded to the hackers.

  For security, the network administrator can add static entries to the MAC table manually to bind the user's device and the port of the device. In this way, the device can stop the illegal users from stealing data.

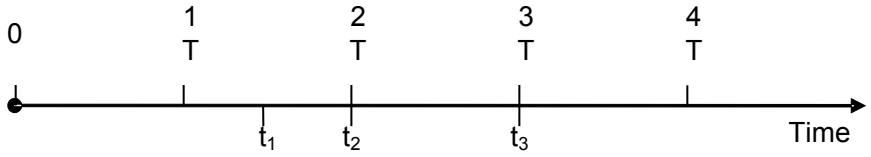
  By configuring blackhole MAC address entries, you can configure the specified user traffic not to pass through a switch to prevent attacks from unauthorized users.

  The priority of MAC entries set up by users is higher than that generated by the device itself.

Aging Time of MAC Addresses

To adapt to the changes of networks, the MAC table needs to be updated constantly. The dynamic entries automatically created in a MAC address table are not always valid. Each entry has a life cycle. The entry that has never been updated till its life cycle ends will be deleted. This life cycle is called aging time. If the entry is updated before its life cycle ends, the aging time of the entry is recalculated.

Figure 3-11 Aging of MAC addresses



As shown in the preceding figure, the aging time of MAC addresses is set to T. At t_1, packets with the source MAC address 00e0-fc00-0001 and VLAN ID 1 reach an interface. Assume that the interface is added to VLAN 1. If no entry with the MAC address as 00e0-fc00-0001 and the VLAN ID as 1 exists in the MAC address table, the MAC address is added to the MAC address table as a dynamic MAC address entry and the flag of the matching entry is set to 1.

The switch checks all learned dynamic MAC address entries at an interval of T. For example, at t_2, if the switch discovers that the flag of the matching dynamic MAC address entry with the MAC address as 00e0-fc00-0001 and the VLAN ID as 1 is 1, the flag of the matching MAC address entry is set to 0 and the MAC address entry is not deleted. If packets with the source MAC address as 00e0-fc00-0001 and the VLAN ID as 1 enter the switch between t_2 and t_3, the flag of the matching MAC address entry is set to 1 again. If no packet with the source MAC

address as 00e0-fc00-0001 and the VLAN ID as 1 enters the switch between t_2 and t_3, the flag of the matching MAC address entry is always 0. At t_3, after discovering that the flag of the matching MAC address entry is 0, the switch assumes that the aging time of the MAC address entry expires and deletes the MAC address entry.

As stated above, the minimum holdtime of a dynamic MAC address entry in the MAC address table ranges from the aging time T to 2 T configured on the switch through automatic aging.

The aging time of MAC addresses is configurable. By setting the aging time of MAC addresses, you can flexibly control the holdtime of learned dynamic MAC address entries in the MAC address table.

3.4.2.2 Disabling MAC Address Learning and Limiting the Number of MAC Addresses

The capacity of a MAC address table is limited. Therefore, when hackers forge a large quantity of packets with different source MAC addresses and send the packets to a device, the MAC address table of the device may reach its full capacity. When the MAC address table is full, the device cannot learn source MAC addresses of valid packets.

A device limits the number of learned MAC addresses in one of the following modes:

- Disabling MAC address learning on an interface or a VLAN
- Limiting the number of MAC addresses on an interface or a VLAN

After MAC address learning is disabled on an interface or a VLAN, no MAC address entry can be learned on the interface or VLAN. The system deletes the previously learned dynamic MAC entries after the aging time expires. You can also manually delete these entries.

You can limit the maximum number of dynamic MAC address entries on a specified VLAN or interface. After the number of MAC address entries learned by the VLAN or interface reaches the limit, no MAC address entry can be learned on the VLAN or interface until the previously learned MAC address entries age out.

In most cases, attack packets sent by a hacker enter a switch through the same interface. Therefore, you can set the limit on the number of MAC address entries or disable MAC address learning on an interface to prevent attack packets from exhausting the MAC address table.

3.4.3 Configuration Task Summary

This chapter describes the configuration task summary of MAC.

Table 3-7 lists the configuration task summary of MAC address table.

Table 3-7 Configuration task summary of MAC address table

Item	Description	Task
Configuring the MAC Address Table	This section describes procedures to configure static, blackhole, and dynamic MAC address entries, prevent an interface from learning MAC addresses, limit the number of learned MAC addresses.	**3.4.5.1 Configuring the MAC Address Table**

3.4.4 Default Configuration

This section describes the default configuration of the MAC address table.

Table 3-8 Default values of a MAC address entry

Parameter	Default Value
Aging time of a dynamic MAC address entry	300 seconds
Whether MAC address learning is enabled	Enable

3.4.5 Configuring the MAC Address Table

This section describes the MAC address table configuration.

3.4.5.1 Configuring the MAC Address Table

This section describes procedures to configure static, blackhole, and dynamic MAC address entries, prevent an interface from learning MAC addresses, limit the number of learned MAC addresses.

3.4.5.1.1 Configuring a Static MAC Address Entry

Context

To ensure communication security, you can configure MAC addresses of trusted upstream devices or users as static MAC address entries.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mac-address static mac-address interface-type interface-number vlan vlan-id
```

A static MAC address entry is configured.

NOTE

A static MAC address entry takes precedence over a dynamic MAC address entry. The system discards packets with configured static MAC addresses that have been learned by other interfaces.

----End

3.4.5.1.2 Configuring a Blackhole MAC Address Entry

Context

To save the MAC address table space, protect user devices or network devices from MAC address attacks, you can configure untrusted MAC addresses as blackhole MAC addresses. Packets with source or destination MAC addresses matching the blackhole MAC address entries are discarded.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mac-address blackhole mac-address [ vlan vlan-id ]
```

A blackhole MAC address entry is configured.

----End

3.4.5.1.3 Setting the Aging Time of Dynamic MAC Address Entries

Context

The network topology changes frequently, and the access point will learn many MAC addresses. After the aging time of dynamic MAC address entries is set, the device can delete unneeded MAC address entries to prevent sharp increase of MAC address entries. A shorter aging time is applicable to networks where network topology changes frequently, and a longer aging time is applicable to stable networks.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mac-address aging-time aging-time
```

The aging time of a dynamic MAC address entry is set.

----End

3.4.5.1.4 Disabling MAC Address Learning

Context

When an access point with MAC address learning enabled receives an Ethernet frame, it records the source MAC address and inbound interface of the Ethernet frame in a MAC address entry. When receiving other Ethernet frames destined for this MAC address, the access point forwards the frames through the outbound interface according to the MAC address entry. The MAC address learning function reduces broadcast packets on a network. After MAC address learning is disabled on an interface, the access point does not learn source MAC addresses of packets received by the interface.

Configuration Process

- Disabling MAC address learning in the interface view
  1. Run:
     system-view
     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*
     The interface view is displayed.
  3. Run:
     mac-address learning disable [**action** { **discard** | **forward** }]
     MAC address learning is disabled on the interface.
     By default, MAC address learning is enabled on an interface.
     By default, the access point performs the forward action after MAC address learning is disabled. That is, the access point forwards packets according to the MAC address table. When the action is configured to discard, the access point matches the source MAC addresses of packets with the MAC address entries. If the inbound interface and source MAC address of a packet matches a MAC address entry, the access point forwards the packet. Otherwise, the access point discards the packet.
- Disabling MAC address learning in the VLAN view
  1. Run:
     system-view
     The system view is displayed.
  2. Run:
     vlan *vlan-id*
     The VLAN view is displayed.
  3. Run:
     mac-address learning disable
     MAC address learning is disabled in the VLAN.
     By default, MAC address learning is enabled in a VLAN.

3.4.5.1.5 Limiting the Number of Learned MAC Addresses

Context

The network with low security may be attacked by MAC address attacks. The capacity of a MAC address table is limited. Therefore, when hackers forge a large quantity of packets with different source MAC addresses and send the packets to the access point, the MAC address table of the access point may reach its full capacity. When the MAC address table is full, the access point cannot learn source MAC addresses of valid packets.

You can limit the number of MAC addresses learned on the access point. When the number of learned MAC address entries reaches the limit, the access point does not learn new MAC addresses. You can also configure the action and enable the device to send traps to the NMS when the number of MAC addresses reaches the limit.. This prevents MAC address attacks and improves network security.

Procedure

- Limiting the number of MAC addresses learned by an interface
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     mac-limit maximum *max-num*

     The maximum number of MAC addresses learned on the interface is set.

     By default, the number of MAC addresses learned on an interface is not limited.
  4. Run:
     mac-limit action { **discard** | **forward** }

     The action to be taken on packets with unknown source MAC addresses when the number of learned MAC addresses reaches the limit is configured.

     By default, packets with unknown source MAC addresses are discarded after the number of learned MAC addresses reaches the limit.
  5. Run:
     mac-limit alarm { **disable** | **enable** }

     The access point is configured to (or not to) send a trap to the NMS when the number of learned MAC addresses reaches the limit.

     By default, the access point sends a trap to the NMS when the number of learned MAC addresses reaches the limit.
- Limiting the number of MAC addresses learned in a VLAN
  1. Run:
     system-view

The system view is displayed.

2. Run:
   vlan *vlan-id*

   The VLAN view is displayed.

3. Run:
   mac-limit maximum *max-num*

   The maximum number of MAC addresses learned in the VLAN is set.

   By default, the number of MAC addresses learned in a VLAN is not limited.

4. Run:
   mac-limit alarm { **disable** | **enable** }

   The access point is configured to (or not to) send a trap to the NMS when the number of learned MAC addresses reaches the limit.

   By default, the access point sends a trap to the NMS when the number of learned MAC addresses reaches the limit.

----End

3.4.5.1.6 Checking the Configuration

Procedure

- Run the **display mac-address** command to view all MAC address entries.
- Run the **display mac-address static** command to view static MAC address entries.
- Run the **display mac-address dynamic** command to view dynamic MAC address entries.
- Run the **display mac-address blackhole** command to view blackhole MAC address entries.
- Run the **display mac-address aging-time** command to view the aging time of dynamic MAC address entries.
- Run the **display mac-address summary** command to view statistics on all the MAC address entries.
- Run the **display mac-address total-number** command to view the number of MAC address entries.
- Run the **display mac-limit** command to view the limit of the number of learned MAC addresses.

----End

3.4.6 Configuration Examples

This section provides several configuration examples of MAC address.

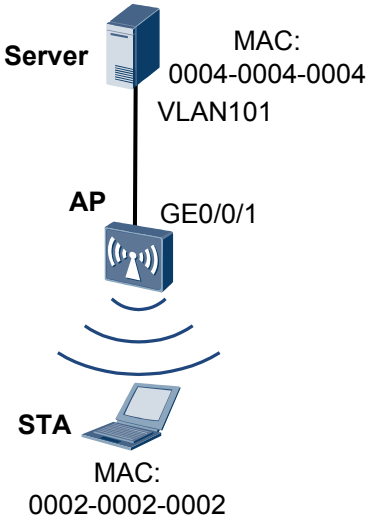
3.4.6.1 Example for Configuring the MAC Address Table

Networking Requirements

As shown in **Figure 3-12**, The MAC address of the server is 0004-0004-0004. The server is connected to GE0/0/1 of the AP, which belongs to VLAN 101. The network requires the following configurations:

- To prevent hackers from stealing user information by forging the MAC address of the server, configure a static MAC address entry on the AP for the server.

Figure 3-12 Network diagram



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on the AP and add the interfaces to the VLANs.
2. Configure static MAC address entries.
3. Set the aging time for the dynamic MAC address entries.

Procedure

Step 1 Add static MAC address entries.

Create VLAN 101 and add GigabitEthernet0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] vlan 101
[Huawei-vlan101] quit
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] port hybrid pvid vlan 101
[Huawei-GigabitEthernet0/0/1] port hybrid untagged vlan 101
[Huawei-GigabitEthernet0/0/1] quit
```

Configure static MAC address entries.

```
[Huawei] mac-address static 0004-0004-0004 gigabitethernet 0/0/1 vlan 101
```

Step 2 Set the aging time for the dynamic MAC address entries.

```
[Huawei] mac-address aging-time 500
```

Step 3 Verify the configuration.

Run the **display mac-address** command in any view to check whether the static MAC address entries are successfully added to the MAC address table.

```
[Huawei] display mac-address static vlan 101
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI                        Learned-From        Type
--------------------------------------------------------------------------------
0004-0004-0004    101/-                   GE0/0/1                 static

--------------------------------------------------------------------------------
Total items displayed = 1
```

Run the **display mac-address aging-time** command to check whether the aging time for dynamic entries is set successfully.

```
[Huawei] display mac-address aging-time
  Aging time: 500 second(s)
```

----End

Configuration Files

Configuration file of the AP

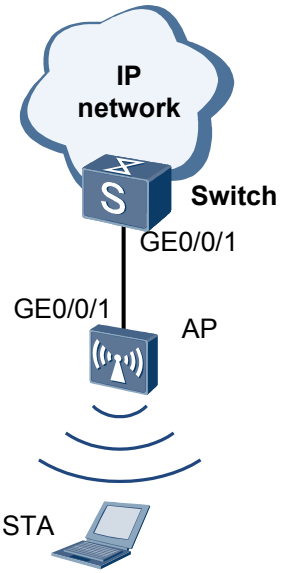
```
#
vlan batch 101
#
 mac-address aging-time 500
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
 mac-address static 0004-0004-0004 GigabitEthernet0/0/1 vlan 101
#
return
```

3.4.6.2 Example for Configuring MAC Address Limiting Rules on Interfaces

Networking Requirements

As shown in **Figure 3-13**, GE0/0/1 of the AP is connected to switch. To prevent MAC address attacks on the AP, configure MAC address limiting rules on GE0/0/1.

Figure 3-13 Network diagram for MAC address limiting on interfaces



Configuration Roadmap

The configuration roadmap is as follows:

1. Set the limit on the number of MAC addresses learned by the interfaces.
2. Set the action performed when the limit is reached.

Procedure

Step 1 Configure MAC address limiting rules on the interfaces.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] mac-limit maximum 100 action discard alarm enable
[Huawei-GigabitEthernet0/0/1] quit
```

Step 2 Verify the configuration.

Run the **display mac-limit** command in any view to check whether the MAC address limiting rule is successfully configured.

```
[Huawei] display mac-limit
MAC limit is enabled
Total MAC limit rule count : 1

PORT                VLAN/VSI         SLOT Maximum Rate(ms) Action  Alarm
------------------------------------------------------------------------------
GE0/0/1             -                -    100     -        discard enable
```

----End

Configuration Files

Configuration file of the AP

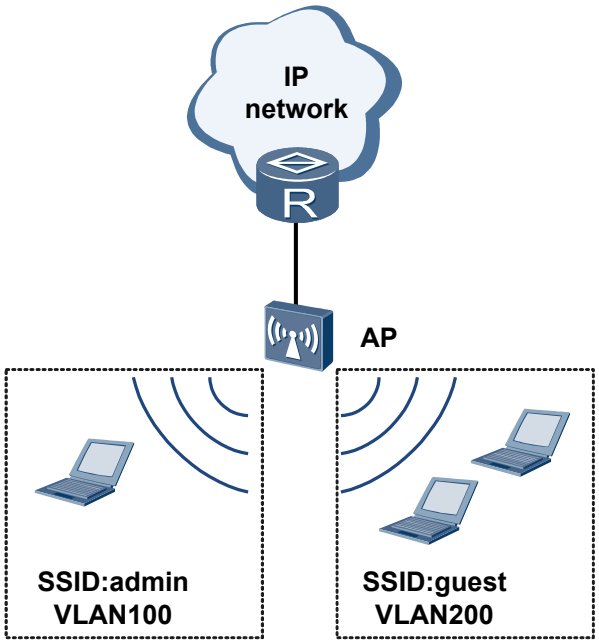
```
#
interface GigabitEthernet0/0/1
 mac-limit maximum 100
#
return
```

3.4.6.3 Example for Configuring a MAC Address Learning Rule in a VLAN

Networking Requirements

As shown in **Figure 3-14**, the AP provides wireless networks with SSIDs **admin** and **guest**. A few STAs connect to the wireless network with SSID **admin**. The service VLAN of these STAs is VLAN 100. Many STAs connect to the wireless network with SSID **guest**. The service VLAN of these STAs is VLAN 200. To prevent MAC address attacks and save MAC address table space, limit the number of MAC addresses learned in VLAN 200.

Figure 3-14 Networking diagram for MAC address limiting in a VLAN



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on the AP and add the interfaces to the VLANs.
2. Set the limit on the number of MAC addresses learned in the VLAN 200.

Procedure

Step 1 Configure WLAN services for the AP.

Configure VAP1 with SSID **admin** and VAP2 with SSID **guest** on the AP, and configure VLAN 100 and VLAN 200 respectively as the service VLANs for VAP1 and VAP2. After the

configurations are complete, the AP can provide two wireless networks and STAs can associate with the APs through the wireless networks. For details, refer to **4.8.1 Example for Configuring the WLAN Service on a Small-Scale Network**.

Step 2 Configure a MAC address limiting rule in the VLAN 200.

Configure the following MAC address limiting rule in VLAN 200:

- A maximum of 100 MAC addresses can be learned.
- When the number of learned MAC address entries reaches the limit, the AP forwards packets with new source MAC addresses and generates an alarm, but does not add the new MAC addresses to the MAC address table.

```
<Huawei> system-view
[Huawei] vlan 200
[Huawei-vlan200] mac-limit maximum 100 alarm enable
[Huawei-vlan200] quit
```

Step 3 Verify the configuration.

Run the **display mac-limit** command in any view to check whether the MAC address limiting rule is successfully configured.

```
[Huawei] display mac-limit
MAC limit is enabled
Total MAC limit rule count : 1

PORT                VLAN/VSI         SLOT Maximum Rate(ms) Action  Alarm
------------------------------------------------------------------------------
-                   200              -    100     -        forward enable
```

----End

Configuration Files

Configuration file of the AP

```
#
vlan batch 100 200
#
vlan 200
 mac-limit maximum 100
#
return
```

3.4.7 Common Configuration Errors

This section describes how to process common configuration errors in MAC address entries.

3.4.7.1 Correct MAC Address Entry Cannot Be Learned on the Device

Fault Description

MAC address entries cannot be learned on the device, so Layer 2 forwarding fails.

Procedure

Step 1 Check that the configurations on the interface are correct.

Run the **display mac-address** command in any view to check whether the binding relationships between the MAC address, VLAN, and interface are correct.

```
<Huawei> display mac-address
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI                          Learned-From        Type
--------------------------------------------------------------------------------
0025-9e80-2494 1/-                               GE0/0/1            dynamic

--------------------------------------------------------------------------------
Total items displayed = 1
```

If not, re-configure the binding relationships between the MAC address, VLAN, and interface.

If yes, go to step 2.

Step 2 Check whether a loop on the network causes MAC address flapping.

- Remove the loop from the network.

If no loop exists, go to step 3.

Step 3 Check that MAC address learning is disable.

Check whether MAC address learning is disable in the interface view and the VLAN view.

```
[Huawei-GigabitEthernet0/0/1] display this
#
interface GigabitEthernet0/0/1
 mac-address learning disable
#
return
[Huawei-vlan10] display this
 #
vlan 10
 mac-address learning disable
#
return
```

If the command output contains **mac-address learning disable**, MAC address learning is disabled on the interface or VLAN.

- If MAC address learning is disabled, run the **undo mac-address learning disable** command in the interface view or VLAN view to enable MAC address learning.
- If MAC address learning is enabled on the interface, go to step 4.

Step 4 Check whether any blackhole MAC address entry or MAC address limiting is configured.

If a blackhole MAC address entry or MAC address limiting is configured, the interface discards packets.

- Blackhole MAC address entry

  Run the **display mac-address blackhole** command to check whether any blackhole MAC address entry is configured.

  ```
  [Huawei] display mac-address blackhole
  --------------------------------------------------------------------------------
  -
  MAC Address    VLAN/VSI                          Learned-From        Type
  --------------------------------------------------------------------------------
  -
  0001-0001-0001 3333/-                            -                   blackhole
  ```

```
--------------------------------------------------------------------------
-
Total items displayed = 1
```

If a blackhole MAC address entry is displayed, run the **undo mac-address blackhole** command to delete it.

- MAC address limiting on the interface or VLAN
  - Run the **display this** command in the interface view or VLAN view. If the command output contains **mac-limit maximum**, the number of learned MAC addresses is limited. Run either of the following commands:
    - Run the **undo mac-limit** command in the interface view or VLAN view to disable MAC address limiting.
    - Run the **mac-limit** command in the interface view or VLAN view to increase the maximum number of learned MAC addresses.

If the fault persists, go to step 5.

Step 5 Check whether the number of learned MAC addresses has reached the maximum supported by the access point.

Run the **display mac-address summary** command to check the number of MAC addresses in the MAC address table.

- If the number of learned MAC addresses has reached the maximum supported by the access point, no MAC address entry can be created. Run the **display mac-address** command to view all MAC address entries.
  - If the number of MAC addresses learned on an interface is much greater than the number of devices on the network connected to the interface, a user on the network may maliciously update the MAC address table. Check the device connected to the interface:
    - If the interface is connected to a device, run the **display mac-address** command on the device to view its MAC address table. Locate the interface connected to the malicious user according to the displayed MAC address entries. If the interface that you find is connected to another device, repeat this step until you find the user of the malicious user.
    - If the interface is connected to a computer, perform either of the following operations after obtaining permission of the administrator:
      - Disconnect the computer. When the attack stops, connect the computer to the network again.
      - Run the **mac-limit** command to set the maximum number of MAC addresses that the interface can learn to 1.
    - If the interface is connected to a hub, perform either of the following operations:
      - Configure port mirroring or other tools to observe packets received by the interface. Analyze the packet types to locate the attacking computer. Disconnect the computer after obtaining permission of the administrator. When the attack stops, connect the computer to the hub again.
      - Disconnect computers connected to the hub one by one after obtaining permission of the administrator. If the fault is rectified after a computer is disconnected, the computer is the attacker. After it stops the attack, connect it to the hub again.

- If the number of MAC addresses on the interface is equal to or smaller than the number of devices connected to the interface, the number of devices connected to the access point has exceeded the maximum supported by the access point. Adjust network deployment.

----End

3.4.8 Reference

This section describes references of MAC address table.

The following table lists the references of this document.

Document	Description	Remarks
IEEE 802.1D	Standard for Information technology--Telecommunications and information exchange between systems--IEEE standard for local and metropolitan area networks--Common specifications--Media access control (MAC) Bridges	-
IEEE 802.1Q	IEEE standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	-

3.5 VLAN Configuration

VLANs have advantages of broadcast domain isolation, security hardening, flexible networking, and good extensibility.

3.5.1 Introduction to VLAN

This section describes definition, purpose and benefits of VLAN.

Definition

The Virtual Local Area Network (VLAN) technology divides a physical LAN into multiple broadcast domains, each of which is called a VLAN. Hosts within a VLAN can communicate with each other, while hosts in different VLANs cannot directly communicate with each other. Therefore, the broadcast packets are limited in each VLAN.

Purpose

The Ethernet technology is used to share communication media and data based on the Carrier Sense Multiple Access/Collision Detection (CSMA/CD). If there are a large number of hosts on an Ethernet network, collision becomes a serious problem and can lead to broadcast storms. As a result, network performance deteriorates. Switches can be used to connect LANs, preventing collision. However, broadcast packets cannot be isolated and network quality cannot be improved.

The VLAN technology divides a physical LAN into multiple broadcast domains, each of which is called a VLAN. Hosts within a VLAN can communicate with each other, while hosts in different VLANs cannot communicate with each other directly. Therefore, the broadcast packets are limited in each VLAN.

NOTE

In this document, the Layer 2 switch is referred to as the switch for short.

Figure 3-15 Networking diagram for a typical VLAN application

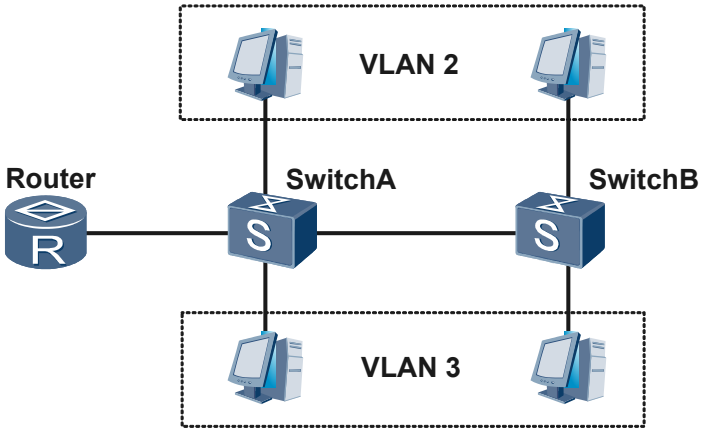


Figure 3-15 shows the networking diagram for a typical VLAN application. Two switches are placed in different locations (for example, in different floors of a building). Each switch is connected to two PCs that respectively belong to different VLANs (for example, different companies).

Benefits

The VLAN technology brings the following benefits to customers:

- Limits broadcast domains. A broadcast domain is limited in a VLAN. This saves bandwidth and improves network processing capabilities.
- Enhances network security. Packets from different VLANs are separately transmitted. Hosts in a VLAN cannot directly communicate with hosts in another VLAN.
- Improves network robustness. A fault in a VLAN does not affect hosts in other VLANs.
- Flexibly sets up virtual groups. With the VLAN technology, hosts in different geographical areas can be grouped together. This facilitates network construction and maintenance.

3.5.2 Principles

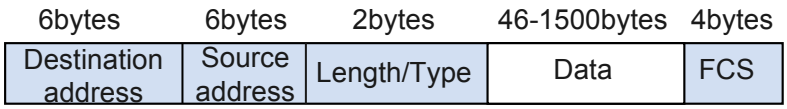
This section describes principles of VLAN.

3.5.2.1 Basic Concepts of VLAN

VLAN frame format

A conventional Ethernet frame is encapsulated with the Length/Type field for an upper-layer protocol following the Destination address and Source address fields, as shown in **Figure 3-16**.

Figure 3-16 Conventional Ethernet frame format



IEEE 802.1Q is an Ethernet networking standard for a specified Ethernet frame format. It adds a 4-byte field between the Source address and the Length/Type fields of the original frame, as shown in **Figure 3-17**.

Figure 3-17 802.1Q frame format

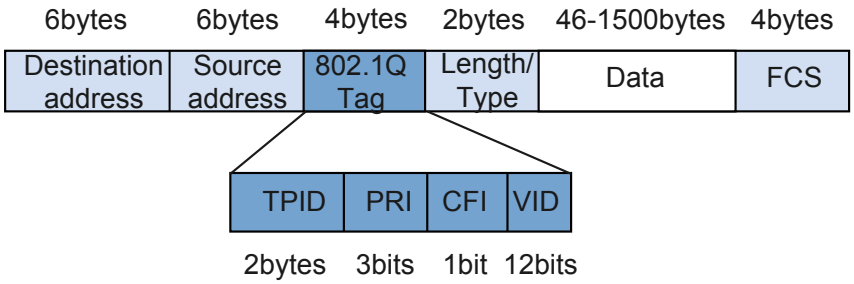


Table 3-9 describes the fields contained in an 802.1Q tag.

Table 3-9 Fields contained in an 802.1Q tag

Field	Length	Name	Description
TPID	2 bytes	Tag Protocol Identifier (TPID), indicating the frame type.	The value 0x8100 indicates an 802.1Q-tagged frame. If an 802.1Q-incapable device receives an 802.1Q frame, it will discard the frame.
PRI	3 bits	Priority (PRI), indicating the frame priority.	The value ranges from 0 to 7. The greater the value, the higher the priority. These values can be used to prioritize different classes of traffic to ensure that frames with high priorities are transmitted first when traffic is heavy.

Field	Length	Name	Description
CFI	1 bit	Canonical Format Indicator (CFI), indicating whether the MAC address is in canonical format.	If the value is 0, the MAC address is in the canonical format. CFI is used to ensure compatibility between Ethernet networks and Token Ring networks. It is always set to zero for Ethernet switches.
VID	12 bits	VLAN ID (VID), indicating the VLAN to which the frame belongs.	VLAN IDs range from 0 to 4095. The values 0 and 4095 are reserved, and therefore VLAN IDs range from 1 to 4094.

Each frame sent by an 802.1Q-capable switch carries a VLAN ID. In a VLAN, Ethernet frames are classified into the following types:

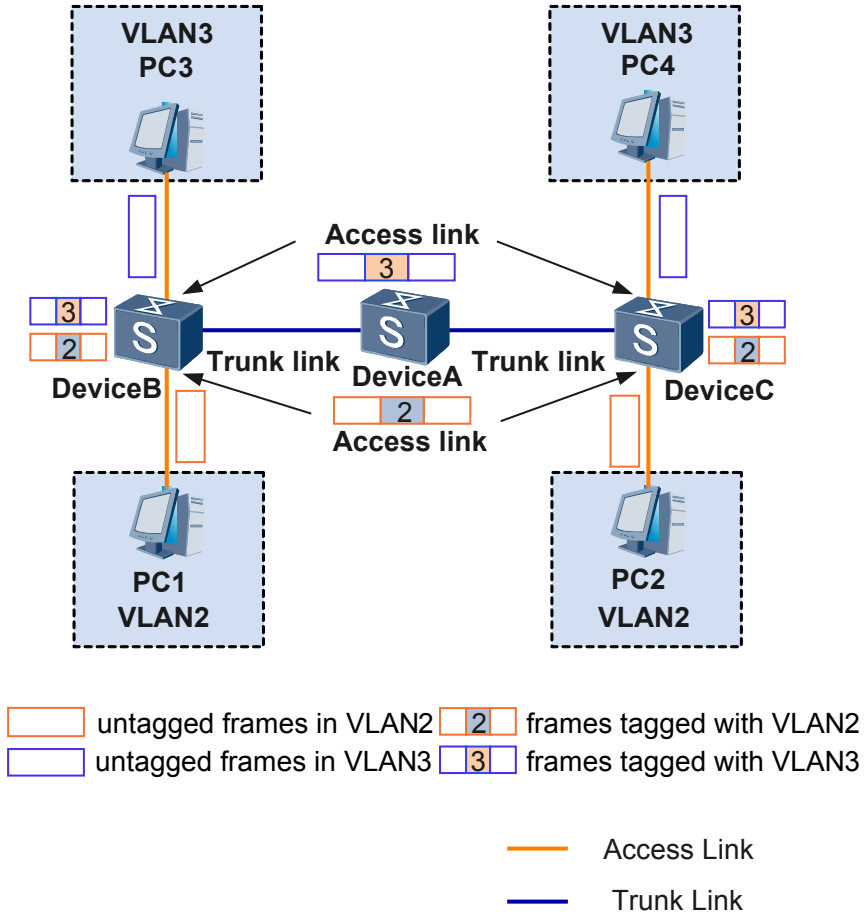
- Tagged frames: frames with 4-byte 802.1Q tags.
- Untagged frames: frames without 4-byte 802.1Q tags.

Link Types

As shown in **Figure 3-18**, there are the following types of VLAN links:

- Access link: connects a host to a switch. Generally, a host does not know which VLAN it belongs to, and host hardware cannot distinguish frames with VLAN tags. Therefore, hosts send and receive only untagged frames.
- Trunk link: connects a switch to another switch or to a router. Data of different VLANs are transmitted along a trunk link. The two ends of a trunk link must be able to distinguish frames with VLAN tags. Therefore, only tagged frames are transmitted along trunk links.

Figure 3-18 Link types



NOTE

- A host does not need to know the VLAN to which it belongs. It sends only untagged frames.
- After receiving an untagged frame from a host, a switching device determines the VLAN to which the frame belongs. The determination is based on the configured VLAN assignment method such as port information, and then the switching device processes the frame accordingly.
- If the frame needs to be forwarded to another switching device, the frame must be transparently transmitted along a trunk link. Frames transmitted along trunk links must carry VLAN tags to allow other switching devices to properly forward the frame based on the VLAN information.
- Before sending the frame to the destination host, the switching device connected to the destination host removes the VLAN tag from the frame to ensure that the host receives an untagged frame.

Generally, only tagged frames are transmitted on trunk links; only untagged frames are transmitted on access links. In this manner, switching devices on the network can properly process VLAN information and hosts are not concerned about VLAN information.

Port Types

After the 802.1Q defines VLAN frames, some ports on the device can identify VLAN frames, while others cannot. According to whether VLAN frames can be identified, ports can be classified into three types:

- Access port

As shown in **Figure 3-18**, the access port on a switch connects to the port on a host. The access port can only connect to an access link. Only the VLAN whose ID is the same as the default VLAN ID is allowed on the access port. Ethernet frames sent from the access port are untagged frames.

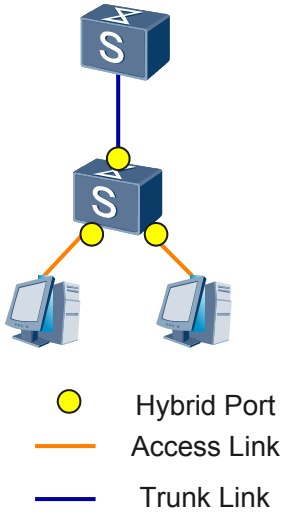
- Trunk port

  As shown in **Figure 3-18**, a trunk port on a switch connects to another switch. It can only connect to a trunk link. Multiple tagged VLAN frames are allowed on the trunk port.

- Hybrid port

  As shown in **Figure 3-19**, a hybrid port on a switch can connect either to a host or to another switch. A hybrid port can connect either to an access link or to a trunk link. The hybrid port allows multiple VLAN frames and removes tags from some VLAN frames on the outbound port.

Figure 3-19 Port types



Default VLAN

Each port can be configured with a default VLAN with a port default VLAN ID (PVID). The meaning of the default VLAN varies according to the port type.

For details on different PVIDs and methods of processing Ethernet frames, see **Frame processing based on the port type**.

3.5.2.2 VLAN Assignment

VLAN assignment can be based on interface numbers, and VLAN frames are processed depending on the interface type.

The network administrator configures a port default VLAN ID (PVID), that is, the default VLAN ID, for each port on the switching device. That is, a port belongs to a VLAN by default.

- When a data frame reaches a port, it is marked with the PVID if the data frame carries no VLAN tag and the port is configured with a PVID.

- If the data frame carries a VLAN tag, the switching device will not add a VLAN tag to the data frame even if the port is configured with a PVID.

3.5.2.3 Principle of VLAN Communication

Basic Principle of VLAN Communication

To improve the efficiency in processing frames, frames within a switch all carry VLAN tags for uniform processing. When a data frame reaches a port of the switch, if the frame carries no VLAN tag and the port is configured with a PVID, the frame is marked with the port's PVID. If the frame has a VLAN tag, the switch will not mark a VLAN tag for the frame regardless of whether the port is configured with a PVID.

The switch processes frames differently according to the type of port receiving the frames. The following describes the frame processing according to the port type.

Table 3-10 Frame processing based on the port type

Port Type	Untagged Frame Processing	Tagged Frame Processing	Frame Transmission
Access port	Accepts an untagged frame and adds a tag with the default VLAN ID to the frame.	• Accepts the tagged frame if the frame's VLAN ID matches the default VLAN ID. • Discards the tagged frame if the frame's VLAN ID differs from the default VLAN ID.	After the PVID tag is stripped, the frame is transmitted.
Trunk port	• Adds a tag with the default VLAN ID to the untagged frame and then transmits it if the default VLAN ID is permitted by the port • Adds a tag with the default VLAN ID to the untagged frame and then discards it if the default VLAN ID is denied by the port.	• Accepts the tagged frame if the frame's VLAN ID is permitted by the port. • Discards the tagged frame if the frame's VLAN ID is denied by the port.	• If the frame's VLAN ID matches the default VLAN ID and the VLAN ID is permitted by the port, the switch removes the tag and transmits the frame. • If the frame's VLAN ID differs from the default VLAN ID, but the VLAN ID is still permitted by the port, the switch will directly transmit the frame.

Port Type	Untagged Frame Processing	Tagged Frame Processing	Frame Transmission
Hybrid port	● Adds a tag with the default VLAN ID to an untagged frame and accepts the frame if the port permits the default VLAN ID. ● Adds a tag with the default VLAN ID to an untagged frame and discards the frame if the port denies the default VLAN ID.	● Accepts a tagged frame if the VLAN ID carried in the frame is permitted by the port. ● Discards a tagged frame if the VLAN ID carried in the frame is denied by the port.	If the frame's VLAN ID is permitted by the port, the frame is transmitted. The port can be configured whether to transmit frames with tags.

NOTE

Because all interfaces join VLAN 1 by default, broadcast storms may occur if unknown unicast, multicast, or broadcast packets exist in VLAN 1. To prevent loops, delete interfaces that do not need to be added to VLAN 1 from VLAN 1.

Intra-VLAN Communication

Sometimes VLAN hosts are connected to different switches, in which case the VLAN spans multiple switches. Since ports between these switches must recognize and send packets belonging to the VLAN, the trunk link technology becomes helpful in simplifying this solution.

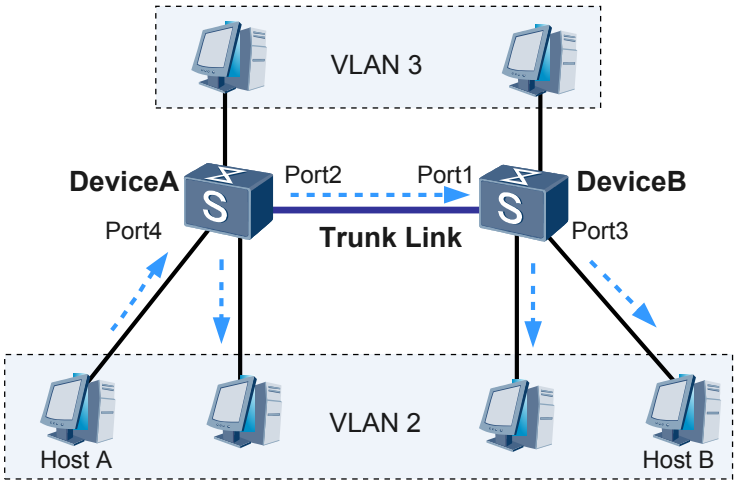
The trunk link plays the following two roles:

- Trunk line

  The trunk link transparently transmits VLAN packets between switches.
- Backbone line

  The trunk link transmits packets belonging to multiple VLANs.

Figure 3-20 Trunk link communication



As shown in **Figure 3-20**, the trunk link between DeviceA and DeviceB must both support the intra-communication of VLAN 2 and the intra-communication of VLAN 3. Therefore, the ports at both ends of the trunk link must be configured to belong to both VLANs. That is, Port2 on DeviceA and Port1 on DeviceB must belong to both VLAN 2 and VLAN 3.

Host A sends a frame to Host B in the following process:

1. The frame is first sent to Port4 on DeviceA.
2. A tag is added to the frame on Port4. The VID field of the tag is set to 2, that is, the ID of the VLAN to which Port4 belongs.
3. DeviceA queries its MAC address table for the MAC forwarding entry with the destination MAC address of Host B.
   - If this entry exists, DeviceA sends the frame to the outbound interface Port2.
   - If this entry does not exist, DeviceA sends the frame to all interfaces bound to VLAN 2 except for Port4.
4. Port2 sends the frame to DeviceB.
5. After receiving the frame, DeviceB queries its MAC address table for the MAC forwarding entry with the destination MAC address of Host B.
   - If this entry exists, DeviceB sends the frame to the outbound interface Port3.
   - If this entry does not exist, DeviceB sends the frame to all interfaces bound to VLAN 2 except for Port1.
6. Port3 sends the frame to Host B.

Inter-VLAN Communication

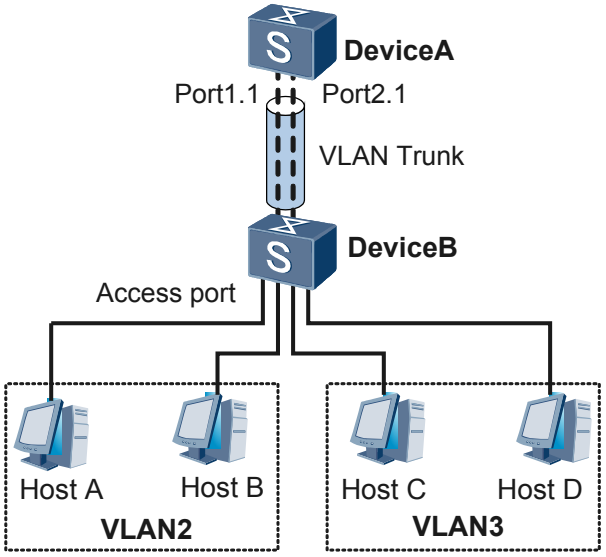
After VLANs are configured, hosts in different VLANs cannot directly communicate with each other. To implement communication between VLANs, use either of the following methods:

- Sub-interface

  As shown in **Figure 3-21**, DeviceA is a Layer 3 switch supporting sub-interface, and DeviceB is a Layer 2 switch. LANs are connected using the switched Ethernet interface on DeviceB and the routed Ethernet interface on DeviceA. User hosts are assigned to VLAN2 and VLAN3. To implement inter-VLAN communication, configure as follows:

  - On DeviceA, create two sub-interfaces Port1.1 and Port2.1 on the Ethernet interface connecting to DeviceB, and configure 802.1Q encapsulation on sub-interfaces corresponding to VLAN2 and VLAN3.
  - Configure IP addresses for sub-interfaces.
  - Set types of Ethernet interfaces connecting DeviceB and DeviceA to **Trunk** or **Hybrid**, to allow VLAN2 and VLAN3 frames.
  - Set the default gateway address to the IP address of the sub-interface mapping the VLAN to which the user host belongs.

Figure 3-21 Inter-VLAN communication using sub-interfaces



Host A communicates with host C as follows:

1. Host A checks the IP address of host C and determines that host C is in another VLAN.
2. Host A sends an ARP request packet to DeviceA to request DeviceA's MAC address.
3. After receiving the ARP request packet, DeviceA returns an ARP reply packet in which the source MAC address is the MAC address of the sub-interface mapping VLAN2.
4. Host A obtains DeviceA's MAC address.
5. Host A sends a packet whose destination MAC address is the MAC address of the sub-interface and destination IP address is host C's IP address to DeviceA.
6. After receiving the packet, DeviceA forwards the packet and detects that the route to host C is a direct route. The packet is forwarded by the sub-interface mapping VLAN3.
7. Functioning as the gateway of hosts in VLAN3, DeviceA broadcasts an ARP packet requesting host C's MAC address.
8. After receiving the packet, host C returns an ARP reply packet.
9. After receiving the reply packet, DeviceA sends the packet from host A to host C. All packets sent from host A to host C are sent to DeviceA first to implement Layer 3 forwarding.

- VLANIF interface

  Layer 3 switching combines routing and switching techniques to implement routing on a switch, improving the overall performance of the network. After sending the first data flow, a Layer 3 switch generates a mapping table on which it records the mapping between the MAC address and the IP address for the data flow. If the switch needs to send the same data flow again, it directly sends the data flow at Layer 2 based on the mapping table. In this manner, network delays caused by route selection are eliminated, and data forwarding efficiency is improved.

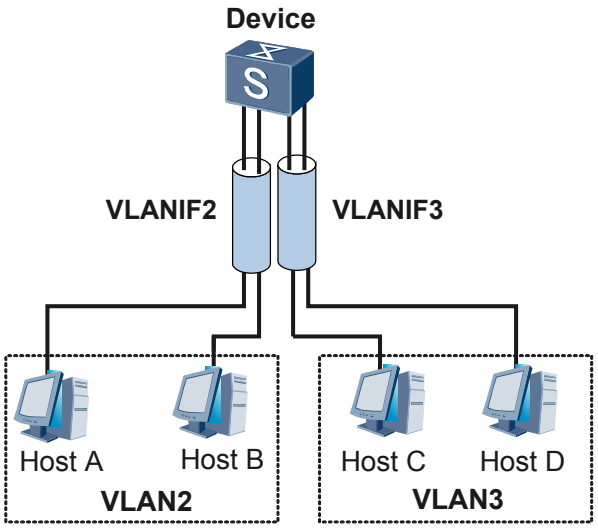
  In order for new data flows to be correctly forwarded, the routing table must have the correct routing entries. Therefore, VLANIF interfaces are used to configure routing protocols on Layer 3 switches to reach Layer 3 routes.

A VLANIF interface is a Layer 3 logical interface, which can be configured on either a Layer 3 switch or a router.

As shown in **Figure 3-22**, hosts connected to the switch are assigned to VLAN 2 and VLAN 3. To implement inter-VLAN communication, configure as follows:

- Create two VLANIF interfaces on the device, and configure IP addresses for them.
- Set the default gateway address to the IP address of the VLANIF interface mapping the VLAN to which the user host belongs.

Figure 3-22 Inter-VLAN communication through VLANIF interfaces



Host A communicates with host C as follows:

1. Host A checks the IP address of host C and determines that host C is in another subnet.
2. Host A sends an ARP request packet to Device to request Device's MAC address.
3. After receiving the ARP request packet, Device returns an ARP reply packet in which the source MAC address is the MAC address of VLANIF2.
4. Host A obtains Device's MAC address.
5. Host A sends a packet whose destination MAC address is the MAC address of the VLANIF interface and destination IP address is host C's IP address to Device.
6. After receiving the packet, Device forwards the packet and detects that the route to host C is a direct route. The packet is forwarded by VLANIF3.
7. Functioning as the gateway of hosts in VLAN3, Device broadcasts an ARP packet requesting host C's MAC address.
8. After receiving the packet, host C returns an ARP reply packet.
9. After receiving the reply packet, DeviceA sends the packet from host A to host C. All packets sent from host A to host C are sent to Device first to implement Layer 3 forwarding.

3.5.2.4 VLAN Damping

Assume that a specific VLAN has been configured with a VLANIF interface. When the VLAN goes Down after all interfaces in the VLAN goes Down, the VLAN reports the Down event to

the VLANIF interface. The status of the VLANIF interface changes. To avoid network flapping due to the status change of the VLANIF interface, you can enable VLAN damping on the VLANIF interface and set a delay after which the VLANIF interface goes Down.

With VLAN damping enabled, when the last Up interface in the VLAN goes Down, the Down event will be reported to the VLANIF interface after a delay (the delay can be set as required). If an interface in the VLAN goes Up during the delay, the status of the VLANIF interface keeps unchanged. That is, the VLAN damping function postpones the time at which the VLAN reports a Down event to the VLANIF interface, avoiding unnecessary route flapping.

3.5.2.5 VLAN Management

To use a network management system to manage multiple devices, create a VLANIF interface on each device and configure a management IP address for the VLANIF interface. You can then log in to a device and manage it using its management IP address. If a user-side interface is added to the VLAN, users connected to the interface can also log in to the device. This brings security risks to the device.

After a VLAN is configured as a management VLAN, no access interface or dot1q-tunnel interface can be added to the VLAN. An access interface or a dot1q-tunnel interface is connected to users. The management VLAN forbids users connected to access and dot1q-tunnel interfaces to log in to the device, improving device performance.

3.5.3 Configuration Task Summary

This chapter describes the configuration task summary of VLAN.

Table 3-11 lists the configuration task summary of VLAN.

Table 3-11 Configuration task summary of VLAN

Item	Description	Task
Assigning a LAN to VLANs	VLANs can isolate the hosts that require no communication with each other, which improves network security, reduces broadcast traffic, and suppresses broadcast storms.	**3.5.5.1 Assigning a LAN to VLANs**
Configuring VLANIF Interfaces for Inter-VLAN Communication	After VLANs are configured, users in the same VLAN can communication with each other while users in different VLANs cannot. To implement inter-VLAN communication, configure the VLANIF interfaces which are Layer 3 logical interfaces.	**3.5.5.2 Configuring VLANIF Interfaces for Inter-VLAN Communication**

Item	Description	Task
Configuring VLAN Aggregation to Save IP Addresses	VLAN aggregation prevents the waste of IP addresses and implements inter-VLAN communication.	Configuring VLAN Aggregation to Save IP Addresses
Configuring an mVLAN to Implement Integrated Management	Management VLAN (mVLAN) configuration allows users to use the VLANIF interface of the mVLAN to log in to the management access point to manage devices in a centralized manner.	**3.5.5.4 Configuring an mVLAN to Implement Integrated Management**

3.5.4 Default Configuration

This section describes the default configuration of VLAN.

Table 3-12 Default configuration of VLAN

Parameter	Default Setting
Port connection mode	Hybrid
Default VLAN ID	1
Damping time	0s
Traffic statistics function of VLAN	Disabled
Traffic statistics function of the VLANIF interface	Disabled

3.5.5 Configuring VLAN

This section describes the VLAN configuration.

3.5.5.1 Assigning a LAN to VLANs

VLANs can isolate the hosts that require no communication with each other, which improves network security, reduces broadcast traffic, and suppresses broadcast storms.

Context

Ports on a Layer 2 switching device can be bound to a specific VLAN. After a port is added to a VLAN, packets of the user that is connected to the port can only be forwarded within the

VLAN, but not forwarded to another VLAN. This implementation ensures that broadcast packets are forwarded only within a single VLAN.

You must create VLANs, configure the port type, and associate ports with VLANs.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

A VLAN is created, and the VLAN view is displayed. If the specified VLAN has been created, the VLAN view is directly displayed.

The VLAN ID ranges from 1 to 4094. If VLANs need to be created in batches, run the **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command to create VLANs in batches, and then run the **vlan** *vlan-id* command to enter the view of a specified VLAN.

NOTE

If a device is configured with multiple VLANs, configuring names for these VLANs is recommended:

Run the **name** *vlan-name* command in the VLAN view. After a VLAN name is configured, you can run the **vlan vlan-name** *vlan-name* command in the system view to enter the corresponding VLAN view.

Step 3 Run:

```
quit
```

The system view is displayed.

Step 4 Configure the port type and features.

1. Run the **interface** *interface-type interface-number* command to enter the view of an Ethernet port to be added to the VLAN.
2. Run the **port link-type** { **access** | **hybrid** | **trunk** } command to configure the port type.

   By default, the port type is Hybrid.

   - If an Ethernet port is directly connected to a terminal, set the port type to access or hybrid.
   - If an Ethernet port is connected to another access point, set the port type to trunk or hybrid.

Step 5 Add ports to the VLAN.

Run either of the following commands as needed:

- For access ports:

  Run the **port default vlan** *vlan-id* command to add a port to a specified VLAN.

  To add ports to a VLAN in batches, run the **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10> command in the VLAN view.
- For trunk ports:

- Run the **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** } command to add the port to specified VLANs.
- (Optional) Run the **port trunk pvid vlan** *vlan-id* command to specify the default VLAN for a trunk interface.

- For hybrid ports:
  - Run either of the following commands to add a port to VLANs in untagged or tagged mode:
    - Run the **port hybrid untagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** } command to add a port to VLANs in untagged mode.

      In untagged mode, a port removes tags from frames and then forwards the frames. This is applicable to scenarios in which Ethernet ports are connected to terminals.
    - Run the **port hybrid tagged vlan** { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** } command to add a port to VLANs in tagged mode.

      In tagged mode, a port forwards frames without removing their tags. This is applicable to scenarios in which Ethernet ports are connected to access pointes.
  - (Optional) Run the **port hybrid pvid vlan** *vlan-id* command to specify the default VLAN of a hybrid interface.

  By default, all ports are added to VLAN 1.

----End

Checking the Configuration

- Run the **display vlan** [*vlan-id* [**verbose**]] command to view information about all VLANs or a specified VLAN.

3.5.5.2 Configuring VLANIF Interfaces for Inter-VLAN Communication

A VLANIF interface is a Layer 3 logical interface. After VLANIF interfaces are created on the device, communication between VLANs is allowed.

Context

After VLANs are configured, users in the same VLAN can communication with each other while users in different VLANs cannot. To implement inter-VLAN communication, configure VLANIF interfaces which are Layer 3 logical interfaces.

If a VLAN goes Down because all ports in the VLAN go Down, the system immediately reports the VLAN Down event to the corresponding VLANIF interface, instructing the VLANIF interface to go Down. To prevent network flapping caused by changes of VLANIF interface status, enable VLAN damping on the VLANIF interface. After the last Up port in a VLAN goes Down, the system starts a delay timer and informs the corresponding VLANIF interface of the VLAN Down event after the timer expires. If a port in the VLAN goes Up during the delay period, the VLANIF interface remains Up.

MTU is short for maximum transmission unit. An MTU value determines the maximum number of bytes each time a sender can send. If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, aggravating the network transmission load. To avoid this problem, set the MTU value of the VLANIF interface.

NOTE

To implement communication between VLANs, hosts in each VLAN must use the IP address of the corresponding VLANIF interface as the gateway address.

Pre-configuration Tasks

Before creating a VLANIF interface, complete the following tasks:

- Create a VLAN.
- Associate the VLAN with the physical interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface vlanif vlan-id
```

A VLANIF interface is created and the VLAIF interface view is displayed.

The VLAN ID specified in this command must be the ID of an existing VLAN.

A VLANIF interface is Up only when at least one physical port added to the corresponding VLAN is Up.

Step 3 Run:

```
ip address ip-address { mask | mask-length } [ sub ]
```

An IP address is assigned to the VLANIF interface for communication at the network layer.

If IP addresses assigned to VLANIF interfaces belong to different network segments, a routing protocol must be configured on the switch to provide reachable routes. Otherwise, VLANIF interfaces cannot communicate with each other at the network layer.

Step 4 (Optional) Run:

```
damping time delay-time
```

The delay period of VLAN damping is configured.

The *delay-time* value ranges from 0 to 20, in seconds. By default, the delay is 0 second, indicating that VLAN damping is disabled.

Step 5 (Optional) Run:

```
mtu mtu
```

The MTU value of the VLANIF interface is configured.

The *mtu* value ranges from 128 to 9216. By default, the value is 1500.

NOTE

- After changing the maximum transmission unit (MTU) using the **mtu** command on a VLANIF interface, you need to restart the VLANIF interface to make the new MTU take effect. To restart the VLANIF interface, run the **shutdown** command and then the **undo shutdown** command, or run the **restart** command in the VLANIF interface view.

----End

Checking the Configuration

- Run the **display interface vlanif** [*vlan-id*] command to verify that the VLANIF interface and protocol are enabled and view the interface description and IP address.

3.5.5.3 Configuring Inter-VLAN Communication

This section describes how to configure VLANIF interfaces to implement inter-VLAN communication.

Pre-configuration Tasks

Before creating a VLANIF interface, complete the following tasks:

- Create a VLAN.
- Associate the VLAN with the physical interface.

3.5.5.3.1 Configuring VLANIF Interfaces for Inter-VLAN Communication

Context

After VLANs are configured, users in the same VLAN can communication with each other while users in different VLANs cannot. To implement inter-VLAN communication, configure VLANIF interfaces which are Layer 3 logical interfaces.

If a VLAN goes Down because all ports in the VLAN go Down, the system immediately reports the VLAN Down event to the corresponding VLANIF interface, instructing the VLANIF interface to go Down. To prevent network flapping caused by changes of VLANIF interface status, enable VLAN damping on the VLANIF interface. After the last Up port in a VLAN goes Down, the system starts a delay timer and informs the corresponding VLANIF interface of the VLAN Down event after the timer expires. If a port in the VLAN goes Up during the delay period, the VLANIF interface remains Up.

MTU is short for maximum transmission unit. An MTU value determines the maximum number of bytes each time a sender can send. If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, aggravating the network transmission load. To avoid this problem, set the MTU value of the VLANIF interface.

After configuring bandwidth for VLANIF interfaces, you can use the NMS to query the bandwidth. This facilitates traffic monitoring.

NOTE

To implement communication between VLANs, hosts in each VLAN must use the IP address of the corresponding VLANIF interface as the gateway address.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface vlanif vlan-id
```

A VLANIF interface is created and the VLANIF interface view is displayed.

The VLAN ID specified in this command must be the ID of an existing VLAN.

A VLANIF interface is Up only when at least one physical port added to the corresponding VLAN is Up.

Step 3 Run:

```
ip address ip-address { mask | mask-length } [ sub ]
```

An IP address is assigned to the VLANIF interface for communication at the network layer.

If IP addresses assigned to VLANIF interfaces belong to different network segments, a routing protocol must be configured on the device to provide reachable routes. Otherwise, VLANIF interfaces cannot communicate with each other at the network layer.

Step 4 (Optional) Run:

```
damping time delay-time
```

The delay period of VLAN damping is configured.

The *delay-time* value ranges from 0 to 20, in seconds. By default, the delay is 0 second, indicating that VLAN damping is disabled.

Step 5 (Optional) Run:

```
mtu mtu
```

The MTU value of the VLANIF interface is configured.

By default, the value is 1500.

NOTE

- After changing the maximum transmission unit (MTU) using the **mtu** command on a specified interface, you need to restart the interface to make the new MTU take effect. To restart the interface, run the **shutdown** command and then the **undo shutdown** command, or run the **restart (interface view)** command in the interface view.

----End

3.5.5.3.2 Checking the Configuration

Prerequisites

The configurations of inter-VLAN communication are complete.

Procedure

- Run the **display vlan** [*vlan-id* [**verbose**]] command to check information about all VLANs or a specified VLAN.
- Run the **display interface vlanif** [*vlan-id*] command to check information about VLANIF interfaces.

  Before running this command, ensure that VLANIF interfaces have been configured.

----End

3.5.5.4 Configuring an mVLAN to Implement Integrated Management

Management VLAN (mVLAN) configuration allows users to use the VLANIF interface of the mVLAN to log in to the management access point to manage devices in a centralized manner.

Context

To use a network management system to manage multiple devices, create a VLANIF interface on each device and configure a management IP address for the VLANIF interface. You can then log in to a device and manage it using its management IP address. If a user-side interface is added to the VLAN, users connected to the interface can also log in to the device. This brings security risks to the device.

After a VLAN is configured as a management VLAN, no access interface or dot1q-tunnel interface can be added to the VLAN. An access interface or a dot1q-tunnel interface is connected to users. The management VLAN forbids users connected to access and dot1q-tunnel interfaces to log in to the device, improving device performance.

Pre-configuration Tasks

Before creating a VLANIF interface, complete the following tasks:

- Create a VLAN.
- Associate the VLAN with the physical interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
vlan vlan-id
```

The VLAN view is displayed.

NOTE

If a device is configured with multiple VLANs, configuring names for these VLANs is recommended:

Run the **name** *vlan-name* command in the VLAN view. After a VLAN name is configured, you can run the **vlan vlan-name** *vlan-name* command in the system view to enter the corresponding VLAN view.

Step 3 Run:

management-vlan

An mVLAN is configured.

After an mVLAN is configured, an interface added to the mVLAN must be a trunk or hybrid interface.

VLAN 1 cannot be configured as an mVLAN.

Step 4 Run:

quit

The VLAN view is quit.

Step 5 Run:

interface vlanif *vlan-id*

A VLANIF interface is created and the VLANIF interface view is displayed.

Step 6 Run:

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

The IP address of the VLANIF interface is configured.

After assigning an IP address to the VLANIF interface, you can run the stelnet command to log in to a management access point to manage attached devices.

----End

Checking the Configuration

- Run the **display vlan** command to check information about the mVLAN. The command output shows information about the mVLAN in the line started with an asterisk sign (*).

3.5.6 Configuration Examples

This section provides several configuration examples of VLANs including networking requirements, configuration roadmap, and configuration procedure.

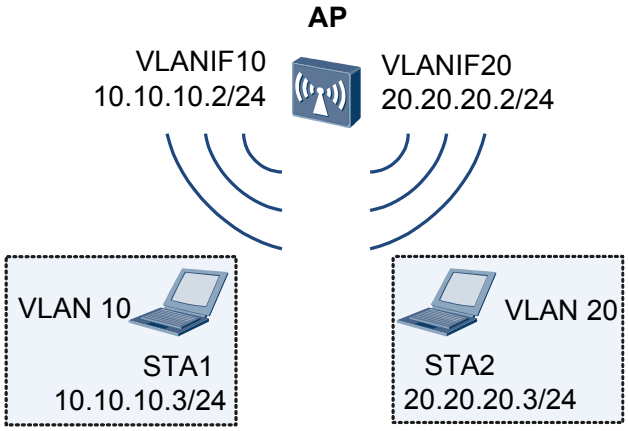
3.5.6.1 Example for Implementing Inter-VLAN Communication Using VLANIF Interfaces

Networking Requirements

Users in an enterprise use different services and locate at different network segments. Users who use the same service belong to different VLANs and they want to communicate with each other.

As shown in **Figure 3-23**, STA 1 and STA 2 use the same service but belong to different VLANs and locate at different network segments. STA 1 wants to communicate with STA 2.

Figure 3-23 Networking diagram for implementing inter-VLAN communication using VLANIF interfaces



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs on the switches for different users.
2. Create VLANIF interfaces and configure IP addresses for the VLANIF interfaces to implement Layer 3 communication.

NOTE

To implement communication between VLANs, hosts in each VLAN must use the IP address of the corresponding VLANIF interface as the gateway address.

Procedure

Step 1 Configure STAs to go online on the APs.

Configure STA1 and STA2 to go online on the APs. The service VLANs of STA1 and STA2 are configured respectively as VLAN 10 and VLAN 20. For details, see **4.8.1 Example for Configuring the WLAN Service on a Small-Scale Network**.

Step 2 Configure the AP.

Create VLANs.

```
<Huawei> system-view
[Huawei] vlan batch 10 20
```

Assign IP addresses to the VLANIF interfaces.

```
[Huawei] interface vlanif 10
[Huawei-Vlanif10] ip address 10.10.10.2 24
[Huawei-Vlanif10] quit
[Huawei] interface vlanif 20
[Huawei-Vlanif20] ip address 20.20.20.2 24
[Huawei-Vlanif20] quit
```

Step 3 Verify the configuration.

Configure the IP address 10.10.10.3/24 on STA 1's host, configure the VLANIF 10 interface IP address 10.10.10.2/24 as the gateway address.

Configure the IP address 20.20.20.3/24 on STA 2's host, configure the VLANIF 20 interface IP address 20.20.20.2/24 as the gateway address.

After the preceding configurations are complete, STA 1 in VLAN 10 and STA 2 in VLAN 20 can communicate.

----End

Configuration Files

Configuration file of the AP

```
#
 vlan batch 10 20
#
interface Vlanif10
 ip address 10.10.10.2 255.255.255.0
#
interface Vlanif20
 ip address 20.20.20.2 255.255.255.0
#
return
```

3.5.7 Common Configuration Errors

This section describes common VLAN configuration errors.

3.5.7.1 User Terminals in the Same VLAN Cannot Ping Each Other

Fault Description

User terminals in the same VLAN cannot ping each other.

Procedure

Step 1 Check that the interfaces connected to the user terminals are in Up state.

Run the **display interface** *interface-type interface-number* command in any view to check the status of the interfaces.

- If the interface is Down, rectify the interface fault.
- If the interface is Up, go to **Step 2**.

Step 2 Check whether the IP addresses of user terminals are in the same network segment.

- If they are in different network segments, change the IP addresses of the user terminals.
- If they are in the same network segment, go to **Step 3**

Step 3 Check that the MAC address entries on the AP are correct.

Run the **display mac-address** command on the AP to check whether the MAC addresses, interfaces, and VLANs in the learned MAC address entries are correct. If the learned MAC address entries are incorrect, run the **undo mac-address** *mac-address* **vlan** *vlan-id* command

on the system view to delete the current entries so that the AP can learn MAC address entries again.

After the MAC address table is updated, check the MAC address entries again.

- If the MAC address entries are incorrect, go to **Step 4**.

Step 4 Check that the VLAN is properly configured.

- Check the VLAN configuration according to the following table.

Check Item	Method
Whether the VLAN has been created	Run the **display vlan** *vlan-id* command in any view to check whether the VLAN has been created. If not, run the **vlan** command in system view to create the VLAN.
Whether the interfaces are added to the VLAN	Run the **display vlan** *vlan-id* command in any view to check whether the VLAN contains the interfaces. If not, add the interfaces to the VLAN. **NOTE** If the interfaces are located on different devices, add the interfaces connecting the devices to the VLAN. The default type of an AP interface is Hybrid. You can run the **port link-type** command to change the interface type. ● Add an access interface to the VLAN using either of the following methods: 1. Run the **port default vlan** command in the interface view. 2. Run the **port** command in the VLAN view. ● Add a trunk interface to the VLAN. Run the **port trunk allow-pass vlan** command in the interface view. ● Add a hybrid interface to the VLAN using either of the following methods: 1. Run the **port hybrid tagged vlan** command in the interface view. 2. Run the **port hybrid untagged vlan** command in the interface view.
Whether connections between interfaces and user terminals are correct	Check the connections between interfaces and user terminals according to the network plan. If any user terminal is connected to an incorrect interface, connect it to the correct interface.

After the preceding operations, if the MAC address entries are correct, go to **Step 5**.

Step 5 Check whether correct static Address Resolution Protocol (ARP) entries are configured on the user terminals. If the static ARP entries are incorrect, modify them.

----End

3.5.7.2 VLANIF Interface Goes Down

Fault Symptom

A VLANIF interface is in Down state.

Common causes and solutions

Table 3-13 lists the common causes and solutions.

Table 3-13 Common causes and solutions

Common Cause	Solution
No interface is added to the corresponding VLAN.	Add interfaces to the corresponding VLAN.
All interfaces added to the VLAN are physically Down.	Rectify the fault. A VLANIF interface is Up as long as an interface in the corresponding VLAN is Up.
No IP address is assigned to the VLANIF interface.	Run the **ip address** command in the view of the VLANIF interface to assign an IP address to the VLANIF interface.
The VLANIF interface is shut down.	Run the **undo shutdown (interface view)** command in the view of the VLANIF interface to enable the VLANIF interface.

3.5.8 References

This section describes references of VLAN.

The following table lists the references of this document.

Document	Description	Remarks
RFC 3069	VLAN Aggregation for Efficient IP Address Allocation	-
IEEE 802.1Q	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks	-
IEEE 802.1ad	IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks- Amendment 4	-
IEEE 802.10	IEEE Standards for Local and Metropolitan Area Networks: Standard for Interoperable LAN/MAN Security	-

Document	Description	Remarks
YD/T 1260-2003	Technical and Testing Specification of Virtual LAN Based on Port	-

3.6 IP Address Configuration

Network devices can communicate at the network layer only after they are configured with IP addresses.

3.6.1 IPv4 Overview

This section describes basic definition of the IPv4 protocol suite.

Definition

Internet Protocol Version 4 (IPv4) is the core protocol in the TCP/IP protocol suite. IPv4 works at the network layer in the TCP/IP model. This layer corresponds to the network layer in the Open System Interconnection Reference Model (OSI RM). The network layer provides connectionless data transmission. Each IP datagram is transmitted independently.

Purpose

IPv4 is used on the network layer between the data link layer and the transport layer. IPv4 shields the differences at the link layer and provides a uniform format for the data packets transmitted at the transport layer.

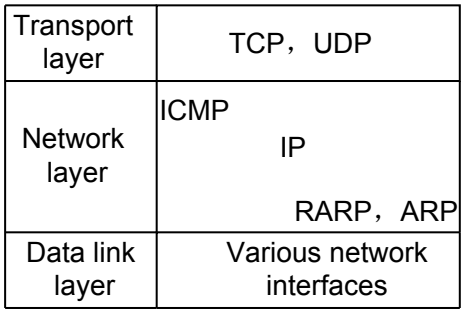
3.6.2 Principles

This section describes members of the IPv4 protocol suite, definition of IPv4 addresses, and IPv4 packet format.

3.6.2.1 IPv4 Protocol Suite

Internet Protocol Version 4 (IPv4) is the core protocol in the TCP/IP protocol suite. IPv4 protocol suite includes Address Resolution Protocol (ARP), Reverse Address Resolution Protocol (RARP), Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), and User Datagram Protocol (UDP).

Figure 3-24 IPv4 protocol suite



As shown in **Figure 3-24**, ARP and RARP work between the data link layer and the network layer for address resolution. ICMP works between the network layer and the transport layer to ensure correct forwarding of IP datagrams.

ARP

ARP maps an IP address to a MAC address. ARP can be implemented in dynamic or static mode. ARP provides some extended functions, such as proxy ARP, gratuitous ARP, ARP security, and ARP-Ping.

RARP

RARP maps a MAC address to an IP address.

ICMP

ICMP works at the network layer to ensure correct forwarding of IP datagrams. ICMP allows hosts and devices to report errors during packet transmission. An ICMP message is encapsulated in an IP datagram as the data, and a header is added to the ICMP message to form an IP datagram.

3.6.2.2 IPv4 Address

To connect a PC to the Internet, you need to apply an IP address from the Internet Service Provider (ISP).

An IP address is a numerical label assigned to each device on a computer network. An IPv4 address is a 32-bit binary number. IPv4 addresses are expressed in dotted decimal notation, which helps you memorize and identify them. In dotted decimal notation, an IPv4 address is written as four decimal numbers, one for each byte of the address. For example, the binary IPv4 address 00001010 00000001 00000001 00000010 is written as 10.1.1.2 in dotted decimal notation.

An IPv4 address consists of two parts:

- Network ID (Net-id).The network ID identifies a network. The leftmost several bits of the network ID identify the class of IP addresses.
- Host ID (Host-id).The host ID identifies different hosts on a network. Network devices with the same network ID are located on the same network, regardless of their physical locations.

Characteristics of IPv4 Addresses

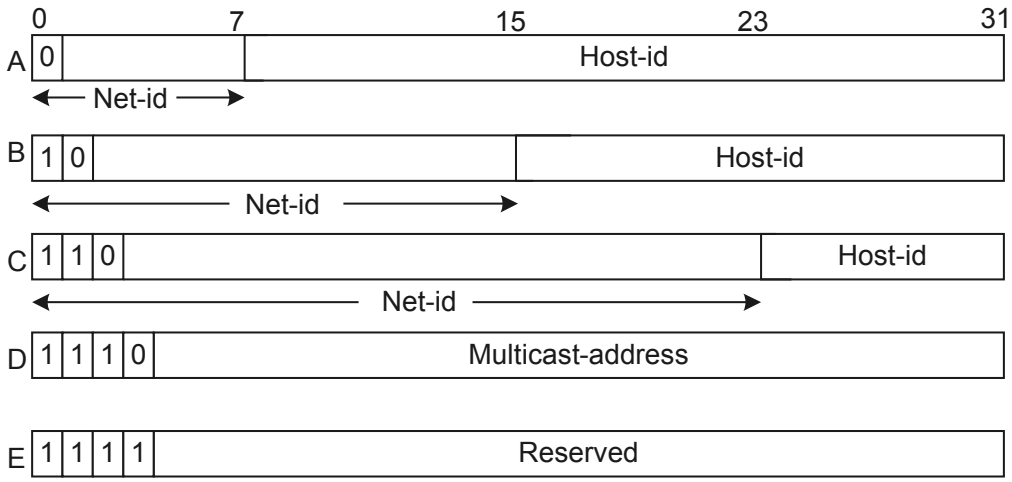
IPv4 addresses have the following characteristics:

- IP addresses do not show any geographical information. The network ID represents the network to which a host belongs.
- When a host connects to two networks simultaneously, it must have two IP addresses with different network IDs. In this case, the host is called a multihomed host.
- Networks allocated with the network ID are in the same class.

IPv4 Address Classification

As shown in **Figure 3-25**, IP addresses are classified into five classes to facilitate IP address management and networking.

Figure 3-25 Five classes of IP addresses



At present, most IP addresses in use belong to Class A, Class B, or Class C. Class D addresses are multicast addresses and Class E addresses are reserved. The easiest way to determine the class of an IP address is to check the first bits in its network ID. The class fields of Class A, Class B, Class C, Class D, and Class E are binary digits 0, 10, 110, 1110, and 1111 respectively. For details about IP address classification, see RFC 1166 (Internet Numbers).

Certain IP addresses are reserved, and they cannot be allocated to users. **Table 3-14** lists the ranges of IP addresses for the five classes.

Table 3-14 IP address classes and ranges

Class	Range	Description
A	0.0.0.0 to 127.255.255.255	IP addresses with all-0 host IDs are network addresses and are used for network routing. IP addresses with all-1 host IDs are broadcast addresses and are used for broadcasting packets to all hosts on the network.
B	128.0.0.0 to 191.255.255.255	IP addresses with all-0 host IDs are network addresses and are used for network routing. IP addresses with all-1 host IDs are broadcast addresses and are used for broadcasting packets to all hosts on the network.
C	192.0.0.0 to 223.255.255.255	IP addresses with all-0 host IDs are network addresses and are used for network routing. IP addresses with all-1 host IDs are broadcast addresses and are used for broadcasting packets to all hosts on the network.

Class	Range	Description
D	224.0.0.0 to 239.255.255.255	Class D addresses are multicast addresses.
E	240.0.0.0 to 255.255.255.255	Reserved. The IP address 255.255.255.255 is used as a Local Area Network (LAN) broadcast address.

Special IPv4 Addresses

Table 3-15 Special IP addresses

Network ID	Host ID	Used as a Source Address	Used as a Destination Address	Description
All 0s	All 0s	Yes	No	Used by local hosts on a local network.
All 0s	Host ID	Yes	No	Used by specified hosts on a network.
127	Any value except all 0s or all 1s	Yes	Yes	Used as loopback addresses.
All 1s	All 1s	No	Yes	Limited broadcast address (packets with this IP address will never be forwarded).
Net-id	All 1s	No	Yes	Directed broadcast address (packets with this IP address is broadcast on the specified network).

NOTE

Net-id is neither all 0s nor all 1s.

Private IPv4 Addresses

Private IP addresses are used to solve the problem of IP address shortage. Private addresses are used on internal networks or hosts, and cannot be used on the public network. RFC 1918 describes three IP address segments reserved for private networks.

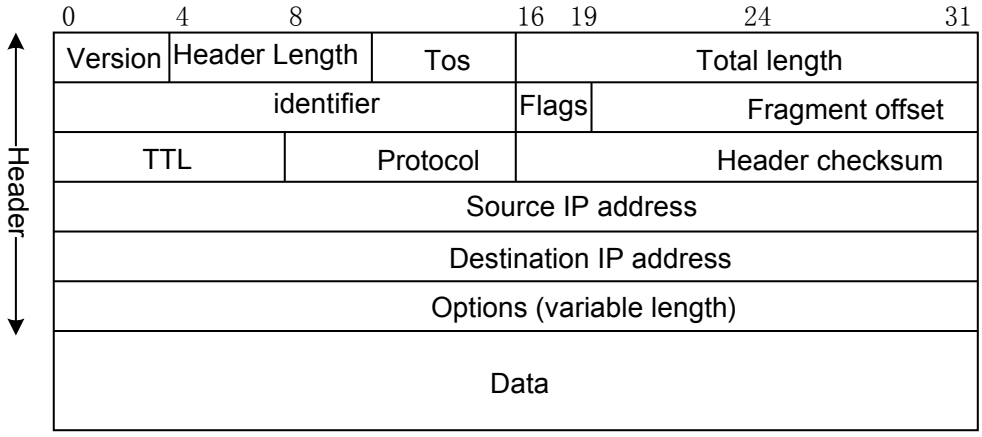
Table 3-16 Private IP addresses

Class	Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

3.6.2.3 IPv4 Packet Format

Figure 3-26 shows the IPv4 packet format.

Figure 3-26 IPv4 packet format



An IPv4 datagram consists of a header and a data field. The first 20 bytes in the header are mandatory for all IPv4 datagrams. The Options field following the 20 bytes has a variable length.

Table 3-17 describes the meaning of each field in an IPv4 packet.

Table 3-17 Description of each field in an IPv4 packet

Field	Length	Description
Version	4 bits	Specifies the IP protocol version, IPv4 or IPv6.
Header Length	4 bits	Specifies the length of the IPv4 header.
Type of Service (ToS)	8 bits	Specifies the type of service. This field takes effect only in the differentiated service model.
Total Length	16 bits	Specifies the length of the header and data.

Field	Length	Description
Identification	16 bits	IPv4 software maintains a counter in the storage device to record the number of IP datagrams. The counter value increases by 1 every time a datagram is sent, and is filled in the identification field.
Flags	3 bits	Only the rightmost two bits are valid. The rightmost bit indicates whether the datagram is not the last data fragment. The value 1 indicates the last fragment, and the value 0 indicates non-last fragment. The middle bit is the fragmentation flag. The value 1 indicates that the datagram cannot be fragmented, and the value 0 indicates that the datagram can be fragmented.
Fragment Offset	13 bits	Specifies the location of a fragment in a packet.
Time to Live (TTL)	8 bits	Specifies the life span of a datagram on a network. TTL is measured by the number of hops.
Protocol	8 bits	Specifies the type of the protocol carried in the datagram.
Header Checksum	16 bits	A device calculates the header checksum for each datagram received. If the checksum is 0, the device knows that the header remains unchanged and retains the datagram. This field checks only the header but not the data.
Source IP Address	32 bits	Specifies the IPv4 address of a sender.
Destination IP Address	32 bits	Specifies the IPv4 address of a receiver.
Options (variable length)	0-40 bytes	Allows IPv4 to support various options such as fault handling, measurement, and security. Pad bytes with a value of 0 are added if necessary.
Data	Variable	Pads an IP datagram .

3.6.2.4 Subnetting

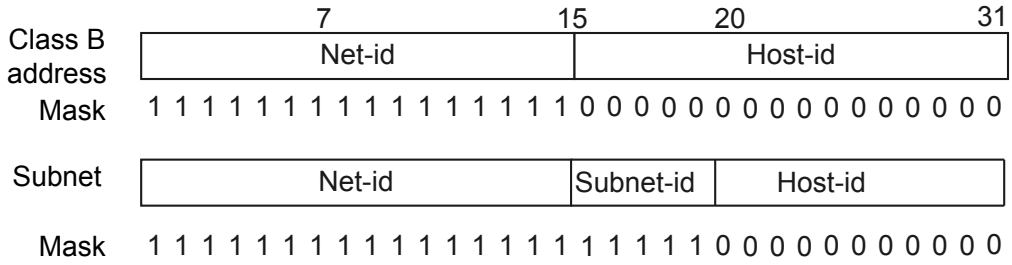
A network can be divided into multiple subnets to conserve IP address space and support flexible IP addressing.

When many hosts are distributed on an internal network, the internal host IDs can be divided into multiple subnet IDs to facilitate management. Then the entire network contains multiple small networks.

Subnetting is implemented within the internal network. The internal network has only one network ID for the external network. When packets are transmitted from the external network to the internal network, the device on the internal network selects a route for the packets based on the subnet ID and finds the destination host.

Figure 3-27 shows subnetting of a Class B IP address. The subnet mask consists of a string of continuous 1s and 0s. 1s indicate the network ID and the subnet ID field, and 0s indicate the host ID.

Figure 3-27 Subnetting of IP addresses



As shown in Figure 3-27, the first 5 bits of the host ID is used as the subnet ID. The subnet ID ranges from 00000 to 11111, allowing a maximum of 32 (2^5) subnets. Each subnet ID has a subnet mask. For example, the subnet mask of the subnet ID 11111 is 255.255.248.0. After performing an AND operation on the IP address and the subnet mask, you can obtain the network address.

Subnetting reduces the available IP addresses. For example, a Class B IP address contains 65534 host IDs. After 5 bits in the host ID are used as the subnet ID, there can be a maximum of 32 subnets, each having an 11-bit host ID. Each subnet has a maximum of 2046 host IDs (2^{11} - 2, excluding the host IDs with all 1s and all 0s). Therefore, the IP address has a maximum of 65472 (32 x 2046) host IDs, 62 less than the maximum number of host IDs before subnetting.

To implement efficient network planning, subnetting and IP addressing should abide by the following rules.

Hierarchy

To divide a network into multiple layers, you need to consider geographic and service factors. Use a top-down subnetting mode to facilitate network management and simplify routing tables. In most cases:

- A network consisting of a backbone network and a MAN is divided into hierarchical subnets.
- An administrative network is divided into subnets based on administrative levels.

Consecutiveness

Consecutive addresses facilitate route summarization on a hierarchical network, which greatly reduces the number of routing entries and improves route search efficiency.

- Allocate consecutive IP addresses to each area.
- Allocate consecutive IP addresses to devices that have the same services and functions.

Scalability

When allocating addresses, reserve certain addresses on each layer to ensure consecutive address allocation in future network expansion.

A backbone network must have enough consecutive addresses for independent autonomous systems (ASs) and further network expansion.

Efficiency

When planning subnets, fully utilize address resources to ensure that the subnets are sufficient for hosts.

- Allocate IP addresses by using variable-length subnet masking (VLSM) to fully use address resources.
- Consider the routing mechanisms in IP address planning to improve address utilization efficiency in the allocated address spaces.

3.6.2.5 IP Address Resolution

A device that connects to multiple networks has the IP addresses of the connected networks. To ensure that users can use the IP address normally, ensure that:

- An IP address is a network layer address of a host. To transmit data packets to a destination host, the device must obtain the physical address of the host. Therefore, the IP address must be resolved to a physical address.
- A host name is easier to remember than an IP address. Therefore, the host name needs to be resolved to the IP address.

On Ethernet, the physical address of a host is the MAC address. The DNS server resolves a host name to an IP address. ARP resolves an IP address to a MAC address. For details, see **3.9 DNS Configuration** and **3.7 ARP Configuration**.

3.6.3 Configuring IP Address

This section describes how to configure an IPv4 address for an interface.

3.6.3.1 Configuring IP Addresses for Interfaces

To enable network devices to communicate at the network layer, configure interface IP addresses on the network devices.

Pre-configuration Tasks

Before configuring IP addresses for interfaces, complete the following tasks:

- Setting link layer parameters for the interfaces to ensure that the link layer protocol status of the interfaces is Up

3.6.3.1.1 Configuring a Primary IP Address for an Interface

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed. The interface can be a VLANIF or loopback interface.

Step 3 Run:

```
ip address ip-address { mask | mask-length }
```

A primary IP address is configured for the interface.

Each interface has only one primary IP address. If you configure multiple primary IP addresses for an interface, the last configured IP address becomes the primary IP address of the interface.

----End

3.6.3.1.2 (Optional) Configuring a Secondary IP Address for an Interface

Context

Generally, an interface needs only a primary IP address. In some special scenarios, you need to configure secondary IP addresses for an interface. For example, a access point connects to a physical network through an interface, and hosts on this network belong to two network segments. To enable the access point to communicate with all hosts on the physical network, configure a primary IP address and a secondary IP address for this interface. You can configure multiple IP address for a Layer 3 interface on a access point, one as the primary IP address, and the others as secondary IP addresses. Each Layer 3 interface can have a maximum of 31 secondary IP addresses.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed. The interface can be a VLANIF or loopback interface.

Step 3 Run:

```
ip address ip-address { mask | mask-length } sub
```

A secondary IP address is configured for the interface.

----End

3.6.3.1.3 Checking the Configuration

Procedure

- Run the **display ip interface** [*interface-type interface-number*] command to check the IP address configuration of an interface.
- Run the **display ip interface brief** [*interface-type* [*interface-number*]] command to check brief information about interface IP addresses.

----End

3.6.4 Configuration Examples

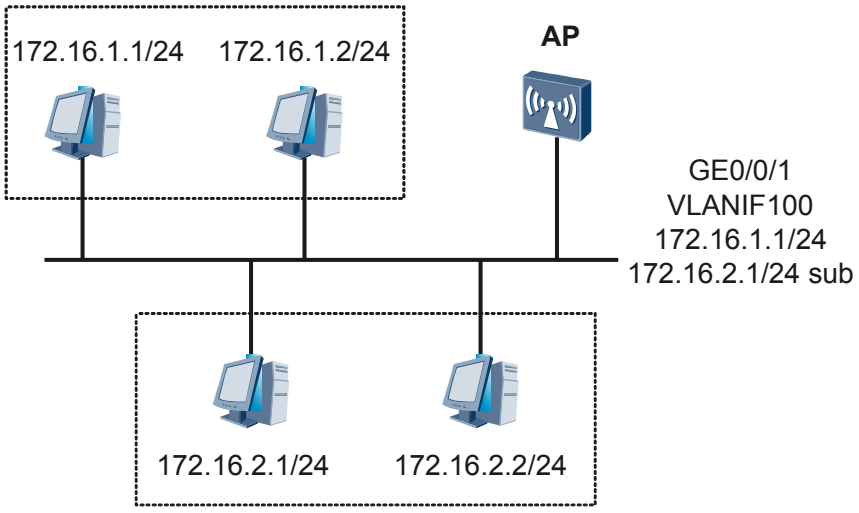
This section provides examples to explain how to configure the primary IP address, secondary IP addresses.

3.6.4.1 Example for Setting IP Addresses

Networking Requirements

As shown in **Figure 3-28**, GigabitEthernet 0/0/1 of the AP is connected to a LAN, in which hosts belong to two different network segments, that is 172.16.1.0/24 and 172.16.2.0/24. It is required that the AP can access the two network segments but the host in 172.16.1.0/24 cannot interconnect with the host in 172.16.2.0/24.

Figure 3-28 Networking diagram for setting IP addresses



Configuration Roadmap

The configuration roadmap is as follows:

1. Analyze the address of the network segment to which each interface is connected.
2. Set the secondary IP addresses for an interface.

Procedure

Step 1 Set the IP address for VLANIF 100 where GE0/0/1 of the AP belongs.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] port hybrid pvid vlan 100
[Huawei-GigabitEthernet0/0/1] port hybrid untagged vlan 100
[Huawei-GigabitEthernet0/0/1] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 172.16.1.1 24
[Huawei-Vlanif100] ip address 172.16.2.1 24 sub
```

Step 2 Verify the configuration.

Ping a host on network segment 172.16.1.0 from AP. The ping succeeds.

```
<Huawei> ping 172.16.1.2
PING 172.16.1.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.1.2: bytes=56 Sequence=1 ttl=128 time=25 ms
    Reply from 172.16.1.2: bytes=56 Sequence=2 ttl=128 time=27 ms
    Reply from 172.16.1.2: bytes=56 Sequence=3 ttl=128 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=4 ttl=128 time=26 ms
    Reply from 172.16.1.2: bytes=56 Sequence=5 ttl=128 time=26 ms
  --- 172.16.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/26/27 ms
```

Ping a host on network segment 172.16.2.0 from the AP. The ping succeeds.

```
<Huawei> ping 172.16.2.2
  PING 172.16.2.2: 56  data bytes, press CTRL_C to break
    Reply from 172.16.2.2: bytes=56 Sequence=1 ttl=128 time=25 ms
    Reply from 172.16.2.2: bytes=56 Sequence=2 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=3 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=4 ttl=128 time=26 ms
    Reply from 172.16.2.2: bytes=56 Sequence=5 ttl=128 time=26 ms
  --- 172.16.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 25/25/26 ms
```

----End

Configuration Files

Configuration file of the AP

```
#
 vlan batch 100
#
interface Vlanif100
 ip address 172.16.1.1 255.255.255.0
 ip address 172.16.2.1 255.255.255.0 sub
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
return
```

3.6.5 Common Configuration Errors

This section describes common errors that may occur in IP address configuration. Learning this section helps you avoid faults caused incorrect IP address configuration.

3.6.5.1 IP Address Configuration Fails on an Interface

Fault Analysis

An error occurs in IP address configuration, so the configuration fails.

Procedure

Step 1 Check the error message and rectify the fault according to **Table 3-18**.

Table 3-18 Error messages and ways to rectify faults

Error Message	Description	Troubleshooting Method
Error: The specified IP address is invalid.	The IP address or subnet mask is incorrect.	Configure the IP address or subnet mask correctly. ● The IP address must be a Class A, Class B, or Class C IP address. ● The subnet mask must match the IP address.
Error: The specified address conflicts with another address.	The specified IP address is on the same network segment as the IP address of another interface on the local device.	Configure another IP address for the interface.
Error: The specified primary address does not exist.	The primary IP address to be deleted does not exist. **NOTE** Each interface has only one primary IP address. If you configure multiple primary IP addresses for an interface, the last configured IP address becomes the primary IP address of the interface.	You do not need to delete the IP address.
Error: Please configure the primary address in the interface view first.	The secondary IP address cannot be configured because the primary IP address has not been configured for the interface.	Configure a primary IP address for the interface first.

Error Message	Description	Troubleshooting Method
Error: The number of addresses of the specified interface reached the upper limit (32).	The number of secondary IP addresses on the interface exceeds the maximum; therefore, no more secondary IP address can be configured. **NOTE** Each interface can have a maximum of 32 IP addresses, including one primary IP address and 31 secondary IP addresses.	-
Error: Please delete the sub address in the interface view first.	The primary IP address cannot be deleted because the interface has secondary IP addresses.	Delete all the secondary IP addresses from the interface, and then delete the primary IP address.
Error: The specified address cannot be deleted because it is not the primary address of this interface.	The command used to delete a primary IP address cannot delete a secondary IP address.	Run the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to delete the secondary IP address.
Error: The specified sub address does not exist.	The secondary IP address to be deleted does not exist.	You do not need to delete the IP address.
Error: The address already exists.	The interface has been configured with the same IP address.	Configure a different IP address for the interface.

----End

3.6.6 References

This section lists references of IPv4.

The following table lists the references of the IPv4 feature.

Document	Description	Remarks
RFC1166	Internet Numbers	-
RFC1918	Address Allocation for Private Internets	-

3.7 ARP Configuration

The Address Resolution Protocol (ARP) maps IP addresses to MAC addresses so that Ethernet frames can be transmitted on a physical network.

3.7.1 ARP Overview

This section describes definition and purpose of Address Resolution Protocol (ARP).

Definition

ARP maps IP addresses into MAC addresses.

Purpose

On a local area network (LAN), a host or a network device must learn the IP address of the destination host or device before sending data to it. Additionally, the host or network device must learn the physical address of the destination host or device because IP packets must be encapsulated into frames for transmission over a physical network. Therefore, the mapping from an IP address into a physical address is required. ARP is used to map IP addresses into physical addresses.

3.7.2 Principles

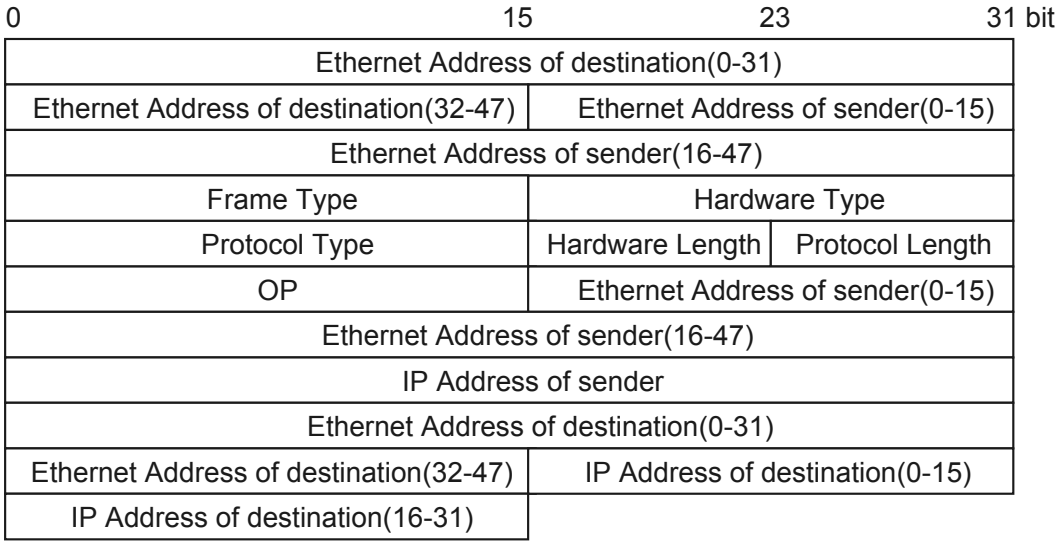
This section describes ARP principles, classification of proxy ARP, as well as functions of gratuitous ARP and ARP-Ping.

3.7.2.1 ARP Principles

Format of ARP Packets

Figure 3-29 shows the format of an ARP Request or Reply packet.

Figure 3-29 Format of an ARP Request or Reply packet



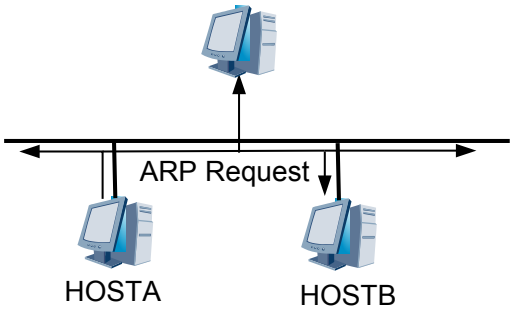
Description of the main fields is as follows:

- Hardware Type: indicates the hardware address type. For an Ethernet, the value of this field is 1.
- Protocol Type: indicates the type of the protocol address to be mapped. For an IP address, the value of this field is 0x0800.
- Hardware Length: indicates the hardware address length. For an ARP Request or Reply packet, the value of this field is 6.
- Protocol Length: indicates the protocol address length. For an ARP Request or Reply packet, the value of this field is 4.
- OP: indicates the operation type. The value 1 indicates ARP requesting, and the value 2 indicates ARP replying.
- Ethernet Address of sender: indicates the MAC address of the sender.
- IP Address of sender: indicates the IP address of the sender.
- Ethernet Address of destination: indicates the MAC address of the receiver.
- IP Address of destination: indicates the IP address of the receiver.

Address Resolution Process

ARP completes address resolution through two processes: ARP request process and ARP reply process.

Figure 3-30 ARP request process

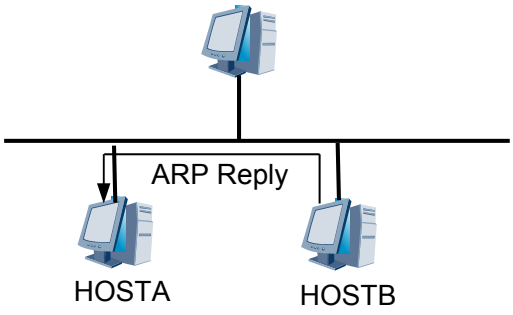


As shown in **Figure 3-30**, HOSTA and HOSTB are on the same network segment. HOSTA needs to send IP packets to HOSTB.

HOSTA searches the local ARP table for the ARP entry corresponding to HOSTB. If the corresponding ARP entry is found, HOSTA encapsulates the IP packets into Ethernet frames and forwards them to HOSTB based on its MAC address.

If the corresponding APR entry is not found, HOSTA caches the IP packets and broadcasts an ARP Request packet. In the ARP Request packet, the IP address and MAC address of the sender are the IP address and MAC address of HOSTA. The destination IP address is the IP address of HOSTB, and the destination MAC address contains all 0s. All hosts on the same network segment can receive the ARP Request packet, but only HOSTB processes the packet.

Figure 3-31 ARP reply process



HOSTB compares its IP address with the destination IP address in the ARP Request packet. If HOSTB finds that its IP address is the same as the destination IP address, HOSTB adds the IP address and MAC address of the sender (HOSTA) to the local ARP table. Then HOSTB unicasts an ARP Reply packet, which contains its MAC address, to HOSTA, as shown in **Figure 3-31**.

After receiving the ARP Reply packet, HOSTA adds HOSTB's MAC address into the local ARP table. Meanwhile, HOSTA encapsulates the IP packets and forwards them to HOSTB.

ARP Aging Mechanism

- ARP cache (ARP table)

  If HOSTA broadcasts an ARP Request packet every time it communicates with HOSTB, the communication traffic on the network will increase. Furthermore, all hosts on the network have to receive and process the ARP Request packet, which decreases network efficiency.

  To solve the preceding problems, each host maintains an ARP cache, which is the key to efficient operation of ARP. This cache contains the recent mapping from IP addresses to MAC addresses.

  Before sending IP packets, a host searches the cache for the MAC address corresponding to the destination IP address. If the cache contains the MAC address, the host does not send an ARP Request packet but directly sends the IP packets to the destination MAC address. If the cache does not contain the MAC address, the host broadcasts an ARP Request packet on the network.

- Aging time of dynamic ARP entries

  After HOSTA receives the ARP Reply packet from HOSTB, HOSTA adds the mapping between the IP address and the MAC address of HOSTB to the ARP cache. However, if a fault occurs on HOSTB or the network adapter of HOSTB is replaced but HOSTA is not notified, HOSTA still sends IP packets to HOSTB. This fault occurs because the APR entry of HOSTB in the ARP cache on HOSTA is not updated.

  To reduce address resolution errors, a timer is set for each ARP entry in an ARP cache. When a dynamic ARP entry expires, the device sends ARP aging probe packets to the corresponding host. If the host does not respond, the ARP entry is deleted, otherwise, the ARP entry is saved.

  Configuring the timer reduces address resolution errors but does not eliminate the problem because of the time delay. Specifically, if the length of a dynamic APR entry timer is N

seconds, the sender can detect the fault on the receiver after N seconds. During the N seconds, the cache on the sender is not updated.

- Number of probes for aging dynamic ARP entries

  Besides setting a timer for dynamic ARP entries, you can set the number of probes for aging dynamic ARP entries to reduce address resolution errors. Before aging a dynamic ARP entry, a host sends ARP aging probe packets. If the host receives no ARP Reply packet after the number of probes reaches the maximum number, the ARP entry is deleted.

- Aging probe modes for dynamic ARP entries

  Before a dynamic ARP entry on a device is aged out, the device sends ARP aging probe packets to other devices on the same network segment. An ARP aging probe packet can be a unicast or broadcast packet. By default, a device broadcasts ARP aging probe packets.

  If the IP address of the peer device remains the same but the MAC address changes frequently, it is recommended that you configure ARP aging probe packets to be broadcast.

  If the MAC address of the peer device remains the same, the network bandwidth is insufficient, and the aging time of ARP entries is short, it is recommended that you configure ARP aging probe packets to be unicast.

  When a non-Huawei device connected to a Huawei device receives an ARP aging probe packet whose destination MAC address is a broadcast address, the non-Huawei device checks the ARP table. If the mapping between the IP address and the MAC address of the Huawei device exists in the ARP table, the non-Huawei device drops the ARP aging probe packet. The Huawei device cannot receive a response and therefore deletes the corresponding ARP entry. As a result, traffic from the network cannot be forwarded. In this scenario, the Huawei device needs to send ARP aging probe packets in unicast mode and the non-Huawei device needs to respond to the ARP aging probe packets.

- Layer 2 topology detection

  The Layer 2 topology detection function enables a device to retransmit ARP probe packets to update ARP entries when a Layer 2 interface becomes Up and the aging time of the ARP entries in the corresponding VLAN becomes 0.

Dynamic ARP

Dynamic ARP entries are generated and maintained dynamically by using ARP packets. They can be aged out, updated, or overwritten by static ARP entries. When the aging time expires or the interface is Down, the corresponding dynamic ARP entries are deleted.

Static ARP

Static ARP entries record fixed mapping between IP addresses and MAC addresses and are configured manually by network administrators. Devices cannot dynamically change the mapping.

3.7.2.2 Proxy ARP

If an ARP Request packet is sent to a host on a different network, the device that connects the two networks can reply to this packet. This function is called proxy ARP.

Proxy ARP has the following characteristics:

- Proxy ARP is implemented on the ARP subnet gateway without any modifications on any hosts.
- Proxy ARP can shield topologies of physical networks so that hosts on different physical networks can use the same network ID to communicate. Proxy ARP enables hosts that are on the same network segment but on different physical networks to communicate.
- Proxy ARP affects only the ARP caches on hosts but does not affect the ARP cache or routing table on the gateway.
- After proxy ARP is enabled, the aging time of ARP entries on hosts should be shortened so that invalid ARP entries can be deleted as soon as possible. Then IP packet forwarding failures decrease on the Access Point.

The following table shows three types of proxy ARP.

Proxy ARP Type	Resolved Issue
Routed proxy ARP	Allows hosts on the same network segment but on different physical networks to communicate.
Intra-VLAN proxy ARP	Allows isolated hosts in a VLAN to communicate.

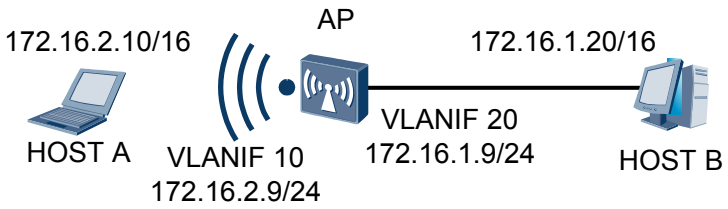
Routed Proxy ARP

Routed proxy ARP enables network devices on the same network segment but on different physical networks to communicate.

In practice, if a host connected to a Access Point is not configured with a default gateway address (that is, the host does not know how to reach the intermediate system of the network), the host cannot transmit packets.

As shown in **Figure 3-32**, Access Point is connected to two networks through VLAN10 and VLAN20. The IP addresses of VLANIF10 and VLANIF20 are on different network segments. However, the masks make HOSTA and VLANIF10 on the same network segment, HOSTB and VLANIF20 on the same network segment, and HOSTA and HOSTB on the same network segment.

Figure 3-32 Application of routed proxy ARP



The IP addresses of HOSTA and HOSTB are on the same network segment. When HOSTA needs to communicate with HOSTB, HOSTA broadcasts an ARP Request packet, requesting the MAC address of HOSTB. However, HOSTA and HOSTB are on different physical networks (in different broadcast domains). Therefore, HOSTB cannot receive the ARP Request packet sent from HOSTA and does not respond with an ARP Reply packet.

To solve this problem, enable proxy ARP on Access Point. After receiving an ARP Request packet, Access Point enabled with proxy ARP searches for the routing table corresponding to

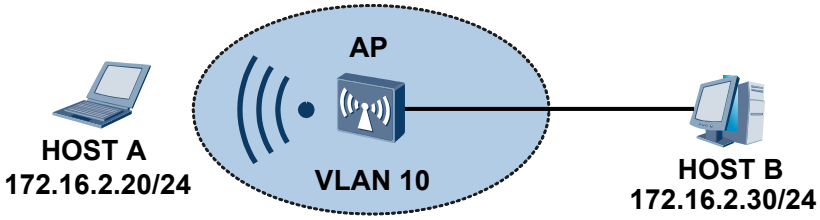
HOSTB. If the Access Point corresponding to HOSTB exists, Access Point responds to the ARP Request packet with its own MAC address. HOSTA forwards data based on the MAC address of Access Point. Access Point functions as the proxy of HOSTB.

Intra-VLAN Proxy ARP

If two hosts belong to the same VLAN but are isolated, enable intra-VLAN proxy ARP on an interface associated with the VLAN to allow the hosts to communicate.

As shown in **Figure 3-33**, HOSTA and HOSTB are connected to Access Point. The two interfaces connected to HOSTA and HOSTB belong to VLAN10.

Figure 3-33 Application of intra-VLAN proxy ARP



HOSTA and HOSTB cannot communicate at Layer 2 because interface isolation in a VLAN is configured on Access Point.

To solve this problem, enable intra-VLAN proxy ARP on the interfaces of Access Point. After Access Point's interface connected to HOSTA receives an ARP Request packet whose destination address is not its own address, Access Point does not discard the packet but searches for the ARP entry corresponding to HOSTB. If the ARP entry corresponding to HOSTB exists, Access Point sends its MAC address to HOSTA and forwards packets sent from HOSTA to HOSTB. Access Point functions as the proxy of HOSTB.

3.7.2.3 Gratuitous ARP

Gratuitous ARP enables a host to send an ARP Request packet using its own IP address as the destination address. Gratuitous ARP provides the following functions:

- Checks duplicate IP addresses: Normally, a host does not receive an ARP Reply packet after sending an ARP Request packet with the destination address being its own IP address. If the host receives an ARP Reply packet, another host has the same IP address.
- Advertises a new MAC address. If the MAC address of a host changes because its network adapter is replaced, the host sends a gratuitous ARP packet to notify all hosts of the change before the ARP entry is aged out.

3.7.3 Configuration Task Summary

ARP can be a dynamic ARP or a static ARP. ARP provides some extended functions, such as proxy ARP.

Table 3-19 describes the ARP configuration tasks.

Table 3-19 ARP configuration task summary

Scenario	Description	Task
Configuring Static ARP	Static ARP entries improve communication security. However, a large number of ARP entries increase configuration and maintenance costs. Static ARP entries can be configured on important network devices such as servers to specify member devices that they can communicate with. In this way, mappings between IP addresses and MAC addresses of these member devices cannot be modified by forged ARP packets and illegal ARP replies can be prevented. This protects servers against network attacks.	**3.7.5.1 Configuring Static ARP**
Optimizing Dynamic ARP	Dynamic ARP entries are generated and maintained automatically using the ARP protocol. ● They can be aged, updated, or overridden by static ARP entries. ● By default, ARP entries are dynamically learned and maintained.	**3.7.5.2 Optimizing Dynamic ARP**

Scenario	Description	Task
Configuring Proxy ARP	Proxy ARP is classified into the following two types: ● Routed Proxy ARP: Routed Proxy ARP enables network devices on the same network segment but on different physical networks to communicate. ● Intra-VLAN Proxy ARP: Intra-VLAN Proxy ARP enables isolated network devices in a VLAN to communicate.	3.7.5.3 Configuring Proxy ARP

3.7.4 Default Configuration

This section describes default ARP configurations.

Table 3-20 describes the default configuration of ARP.

Table 3-20 Default ARP configuration

Parameter	Default Configuration
Aging time of dynamic ARP entries	1200 seconds
Maximum number of probes for aging dynamic ARP entries	3 times
Aging detection mode of dynamic ARP entries	An interface sends ARP aging probe packets in broadcast mode.
Layer 2 topology detection	Layer 2 topology detection is disabled.
ARP proxy	ARP proxy is disabled.

3.7.5 Configuring ARP

This section describes how to configure Address Resolution Protocol (ARP).

3.7.5.1 Configuring Static ARP

Static ARP entries improve communication security.

Context

Static ARP entries are manually configured and maintained. They cannot be aged and overridden by dynamic ARP entries. Therefore, static ARP entries improve communication security. Static ARP entries ensure communication between the local device and a specified device by using a specified MAC address so that attackers cannot modify mappings between IP addresses and MAC addresses in static ARP entries.

NOTE

Static ARP entries cannot be modified. However, the configuration workload is heavy. Static ARP entries cannot apply to a network where IP addresses of hosts may change or a small-sized network.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
arp static ip-address mac-address [ vid vlan-id [ interface interface-type interface-number ] ]
```

A static ARP entry is configured.

----End

Checking the Configuration

After configuring the static ARP entries is complete, run the following commands to check the configuration.

- Run the **display arp** [**all** | **brief**] command to check all ARP mapping entries.
- Run the **display arp network** *net-number* [*net-mask* | *mask-length*] [**dynamic** | **static**] command to check ARP mapping entries of a specified network segment.
- Run the **display arp static** command to check static ARP mapping entries.
- Run the **display arp interface** *interface-type interface-number* command to check ARP mapping entries of a specified interface.

3.7.5.2 Optimizing Dynamic ARP

By default, hosts and access point dynamically learn ARP entries. You can adjust parameters of dynamic ARP entries based on network requirements.

Pre-configuration Tasks

Before optimizing dynamic ARP, complete the following tasks:

- Setting link layer protocol parameters for interfaces to ensure that the link layer protocol status of the interfaces is Up

3.7.5.2.1 Adjusting Aging Parameters of Dynamic ARP Entries

Context

Aging parameters of ARP entries include the aging time, the number of probes, and detection modes. Proper adjustment of aging parameters improves network reliability.

You can adjust the following parameters of dynamic ARP entries:

- Aging time of dynamic ARP entries: When the aging time of a dynamic ARP entry is reached, the device sends an ARP Request packet to the corresponding outbound interface and starts ARP aging detection.
- Number of aging probes to dynamic ARP entries: Before aging a dynamic ARP entry, the system first performs probes. If no answer is received after the times of probes reach the upper limit, the ARP entry is deleted.
- Aging detection modes of dynamic ARP entries: Before an ARP entry is aged, an interface sends an ARP aging probe packet.

  NOTE

  - If the IP address of the peer device remains the same but the MAC address changes frequently, it is recommended that you configure ARP aging probe packets to be broadcast.
  - If the MAC address of the peer device remains the same, and the network bandwidth is insufficient, it is recommended that you configure ARP aging probe packets to be unicast.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
arp expire-time expire-time
```

The aging time of dynamic ARP entries is set.

By default, the aging time of dynamic ARP entries is 1200 seconds, that is, 20 minutes.

Step 4 Run:

```
arp detect-times detect-times
```

The number of probes to dynamic ARP entries is set.

By default, the number of ARP probes is 3.

Step 5 Run:

```
arp detect-mode unicast
```

An interface is configured to send ARP aging probe packets in unicast mode.

By default, an interface sends ARP aging probe packets in broadcast mode.

----End

3.7.5.2.2 Enabling ARP Suppression Function

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
arp-suppress enable
```

ARP suppression is enabled on the current device.

By default, ARP suppression is disabled but is enabled on VLANIF interfaces.

----End

3.7.5.2.3 Enabling Layer 2 Topology Detection

Context

Layer 2 topology detection enables the system to update all the ARP entries in the VLAN that a Layer 2 interface belongs to when the Layer 2 interface status changes from Down to Up.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
l2-topology detect enable
```

Layer 2 topology detection is enabled.

By default, Layer 2 topology detection is disabled.

----End

3.7.5.2.4 Checking the Configuration

Procedure

- Run the **display arp** [**all** | **brief**] command to check all ARP mapping entries.
- Run the **display arp interface** *interface-type interface-number* command to check ARP mapping entries of a specified interface.
- Run the **display arp network** *net-number* [*net-mask* | *mask-length*] [**dynamic** | **static**] command to check ARP mapping entries of a specified network segment.
- Run the **display arp dynamic** command to check dynamic ARP mapping entries.

3.7.5.3 Configuring Proxy ARP

The access point can function as a proxy of the destination host to reply an ARP Request message.

Pre-configuration Tasks

Before configuring proxy ARP, complete the following task:

- Setting link layer protocol parameters for interfaces to ensure that the link layer protocol status of the interfaces is Up

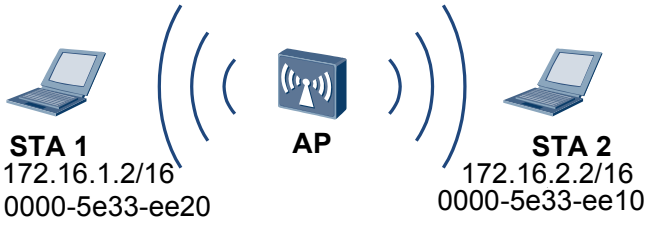
3.7.5.3.1 Configuring Routed Proxy ARP

Context

Proxy ARP enables PCs or access points on the same network segment but on different physical networks to communicate. In actual applications, if the current STA connected to the access point is not configured with a default gateway address (that is, the does not know how to reach the intermediate system of the network), the cannot forward data packets. Routed proxy ARP solves this problem.

Figure 3-34 shows the routed proxy ARP networking. AP uses VLAN10 and VLAN20 to connect two networks. IP addresses of the two VLAN interfaces are on different network segments. However, the masks make STA1 and VLANIF10 on the same network segment, STA2 and VLANIF20 on the same network segment, and STA1 and STA2 on the same network segment.

Figure 3-34 Networking diagram for configuring routed proxy ARP



STA1 sends an ARP Request packet, requesting the MAC address of STA2. After receiving the packet, AP uses its MAC address to reply the Request packet. STA1 then forwards data using the MAC address of AP.

NOTICE

IP addresses of the STAs on a subnet have the same network ID. Therefore, the default gateway address does not need to be configured on the STAs.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

On the device, routing proxy ARP can only be enabled on VLANIF interfaces.

Step 3 Run:

```
ip address ip-address { mask | mask-length }
```

IP addresses are configured for interfaces.

The IP address configured for the interface enabled with routed proxy ARP must be on the same network segment as the IP address of the connected STAserver on a LAN.

Step 4 Run:

```
arp-proxy enable
```

Routed proxy ARP is enabled on the interface.

After proxy ARP is enabled, the aging time of ARP entries on STAs should be shortened so that invalid ARP entries can be deleted as soon as possible. The number of packets received but cannot be forwarded by the device is decreased. To set ARP aging time, run the **arp expire-time** *expire-time* command.

----End

Checking the Configuration

After configuring routed proxy ARP is complete, run the following commands to check the configuration.

- Run the **display arp interface** *interface-type interface-number* command to check ARP mapping entries of a specified interface.

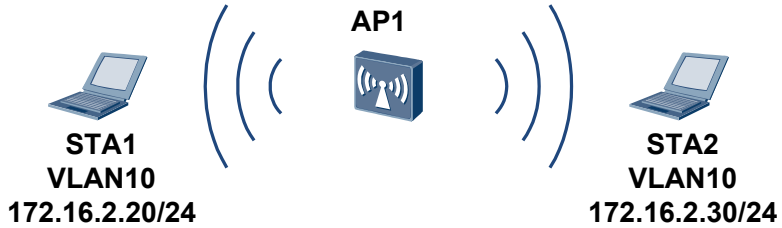
3.7.5.3.2 Configuring Intra-VLAN Proxy ARP

Context

If two STAs belong to the same VLAN but are isolated, enable intra-VLAN proxy ARP on an interface associated with the VLAN to allow the STAs to communicate.

As shown in **Figure 3-35**, STA1 and STA2 connect to AP1. The two interfaces that connect STA1 and STA2 to AP1 belong to VLAN10.

Figure 3-35 Intra-VLAN proxy ARP application



STA1 and STA2 cannot communicate at Layer 2 because interface isolation in a VLAN is configured on AP1.

To solve this problem, enable intra-VLAN proxy ARP on the interfaces of AP1. After an interface of AP1 receives an ARP Request packet whose destination address is STA2 and source address is STA1, AP1 does not discard the packet but searches for the ARP entry. If the ARP entry matching STA2 exists, AP1 sends its MAC address to STA1 and forwards packets sent from STA1 to STA2. AP1 functions as the proxy of STA2.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

On the device, Intra-VLAN Proxy ARP can only be enabled on VLANIF interfaces.

Step 3 Run:

```
arp-proxy inner-sub-vlan-proxy enable
```

Intra-VLAN proxy ARP is enabled.

----End

Checking the Configuration

After configuring intra-VLAN proxy ARP is complete, run the following commands to check the configuration.

- Run the **display arp interface** *interface-type interface-number* command to check ARP mapping entries of a specified interface.

3.7.6 Maintaining ARP

Maintaining ARP includes clearing ARP entries and monitoring ARP running status.

3.7.6.1 Clearing ARP Entries

Context

NOTICE

ARP entries cannot be restored after being cleared. When you delete static ARP entries, the (**arp static**) command is also deleted. Exercise caution when you delete the ARP entries.

Procedure

- Run the **reset arp** { **all** | **dynamic** [**ip** *ip-address*] | **interface** *interface-type interface-number* [**ip** *ip-address*] | **static** } command to clear ARP entries in the ARP mapping table.

----End

3.7.6.2 Monitoring the ARP Running Status

Context

Monitoring the ARP running status includes checking ARP mapping entries, strict ARP entry learning, ARP packet statistics, ARP packet processing rate, and maximum number of ARP entries learnt by an interface.

Procedure

- Run the **display arp** [**all** | **brief**] command in any view to check all ARP mapping entries.
- Run the **display arp interface** *interface-type interface-number* command in any view to check ARP mapping entries of a specified interface.
- Run the **display arp network** *net-number* [*net-mask* | *mask-length*] [**dynamic** | **static**] command in any view to check ARP mapping entries of a specified network segment.
- Run the **display arp statistics** { **all** | **interface** *interface-type interface-number* } command in any view to check ARP entry statistics.

----End

3.7.7 Configuration Examples

This section provides configuration examples including networking requirements and configuration roadmap.

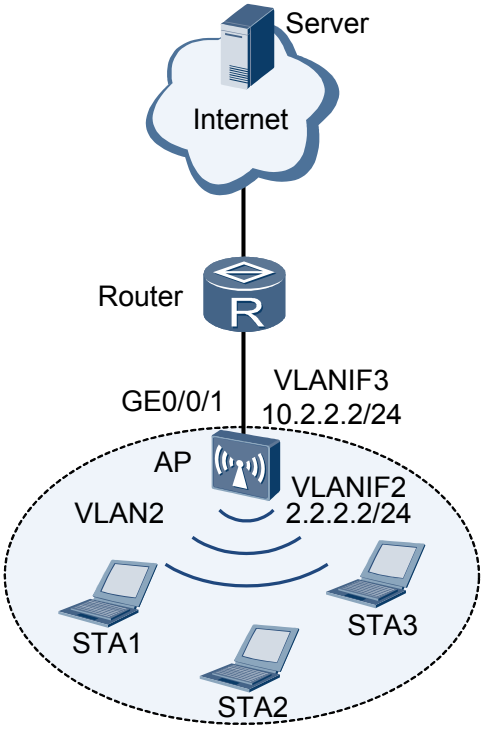
3.7.7.1 Example for Configuring ARP

Networking Requirements

As shown in **Figure 3-36**, an AP connects to STAs through air interfaces. AP's wired interface GE0/0/1 connects to the server through the router. STAs go online on the AP. VLAN2 is the the service VLAN. Service requirements are as follows:

- Dynamic ARP parameters should be configured for VLANIF2 of the AC so that packets are transmitted correctly regardless of network typology change.
- A static ARP entry should be configured on GE0/0/1 of the AP to ensure secure communication with the server and prevent illegal ARP packets. The IP address of the router should be 10.2.2.3/24 and the corresponding MAC address is 00e0-fc01-0000.

Figure 3-36 Networking diagram for configuring ARP



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs and add interfaces to the VLANs.
2. Set dynamic ARP parameters for the user-side VLANIF interface.
3. Configure a static ARP entry.

Procedure

Step 1 Create VLANs and add interfaces to the VLANs.

Create VLAN2 and VLAN3.

```
<Huawei> system-view
[Huawei] vlan batch 2 3
```

Add GE0/0/1 to VLAN3.

```
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] port hybrid tagged vlan 3
[Huawei-GigabitEthernet0/0/1] quit
```

Step 2 Set dynamic ARP parameters for the VLANIF interface.

Create VLANIF2.

```
[Huawei] interface vlanif 2
```

Configure an IP address for VLANIF2.

```
[Huawei-Vlanif2] ip address 2.2.2.2 255.255.255.0
```

Set the aging time of ARP entries to 60s.

```
[Huawei-Vlanif2] arp expire-time 60
```

Set the number of probes to ARP entries to 2.

```
[Huawei-Vlanif2] arp detect-times 2
[Huawei-Vlanif2] quit
```

Create VLANIF3.

```
[Huawei] interface vlanif 3
```

Configure an IP address for VLANIF3.

```
[Huawei-Vlanif3] ip address 10.2.2.2 255.255.255.0
[Huawei-Vlanif3] quit
```

Step 3 Configure a static ARP entry.

Configure a static ARP entry with IP address 10.2.2.3, MAC address 00e0-fc01-0000, VLAN ID 3, and outbound interface GE0/0/1.

```
[Huawei] arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface gigabitethernet 0/0/1
[Huawei] quit
```

Step 4 Verify the configurations.

Run the **display current-configuration** command to check the aging time, number of probes, and ARP mapping entries.

```
<Huawei> display current-configuration | include arp
 arp detect-times 2
 arp expire-time 60
 arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface GigabitEthernet0/0/1
```

----End

Configuration Files

Configuration file of the AP

```
#
vlan batch 2 to 3
#
interface Vlanif2
 arp detect-times 2
 arp expire-time 60
 ip address 2.2.2.2 255.255.255.0
#
interface Vlanif3
 ip address 10.2.2.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid tagged vlan 3
#
 arp static 10.2.2.3 00e0-fc01-0000 vid 3 interface GigabitEthernet0/0/1
#
return
```

3.7.8 References

This section lists references of ARP.

The following table lists the references of this document.

Document	Description	Remarks
RFC826	Ethernet Address Resolution Protocol	-
RFC903	Reverse Address Resolution Protocol	-
RFC1027	Using ARP to Implement Transparent Subnet Gateways	-
RFC1042	Standard for the Transmission of IP Datagrams over IEEE 802 Networks	-

3.8 DHCP Configuration

DHCP dynamically manages and configures clients in a concentrated manner. It ensures proper IP address allocation and improves IP address use efficiency.

3.8.1 DHCP Overview

This section describes the definition and purpose of DHCP.

Definition

The Dynamic Host Configuration Protocol (DHCP) dynamically assigns IP addresses to users and manages user configurations in a centralized manner.

Purpose

As the network expands and becomes complex, the number of hosts often exceeds the number of available IP addresses. As portable computers and wireless networks are widely used, the positions of computers often change, causing IP addresses of the computers to be changed accordingly. As a result, network configurations become increasingly complex. To properly and dynamically assign IP addresses to hosts, DHCP is used.

DHCP is developed based on the BOOTstrap Protocol (BOOTP). BOOTP runs on networks where each host has a fixed network connection. The administrator configures a BOOTP parameter file for each host, and the file remains unchanged for a long period of time. DHCP has the following new features compared with BOOTP:

- Dynamically assigns IP addresses and configuration parameters to clients.
- Enables a host to obtain an IP address dynamically, but does not specify an IP address for each host.

DHCP rapidly and dynamically allocates IP addresses, which improves IP address usage.

3.8.2 Principles

This section describes the implementation of DHCP.

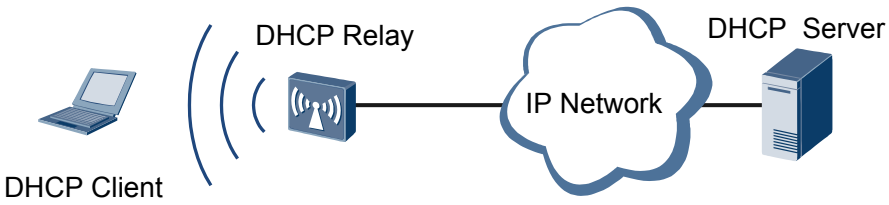
3.8.2.1 DHCP Overview

DHCP uses the client/server model. A DHCP client sends a packet to a DHCP server to request configuration parameters such as the IP address, subnet mask, and default gateway address. The DHCP server responds with a packet carrying the requested configurations based on a policy.

DHCP Architecture

Figure 3-37 shows the DHCP architecture.

Figure 3-37 DHCP architecture



DHCP involves the following roles:

- DHCP Client

  A DHCP client exchanges messages with a DHCP server to obtain an IP address and other configuration parameters. On the device, an interface can function as a DHCP client to dynamically obtain configuration parameters such as an IP address from a DHCP server. This facilitates configurations and centralized management.

- DHCP Relay

  A DHCP relay agent forwards DHCP packets exchanged between a DHCP client and a DHCP server that are located on different network segments so that they can complete their address configuration. Using a DHCP relay agent eliminates the need for deploying a DHCP server on each network segment. This feature reduces network deployment costs and facilitates device management.

  In the DHCP architecture, the DHCP relay agent is optional. A DHCP relay agent is required only when the server and client are located on different network segments.

- DHCP Server

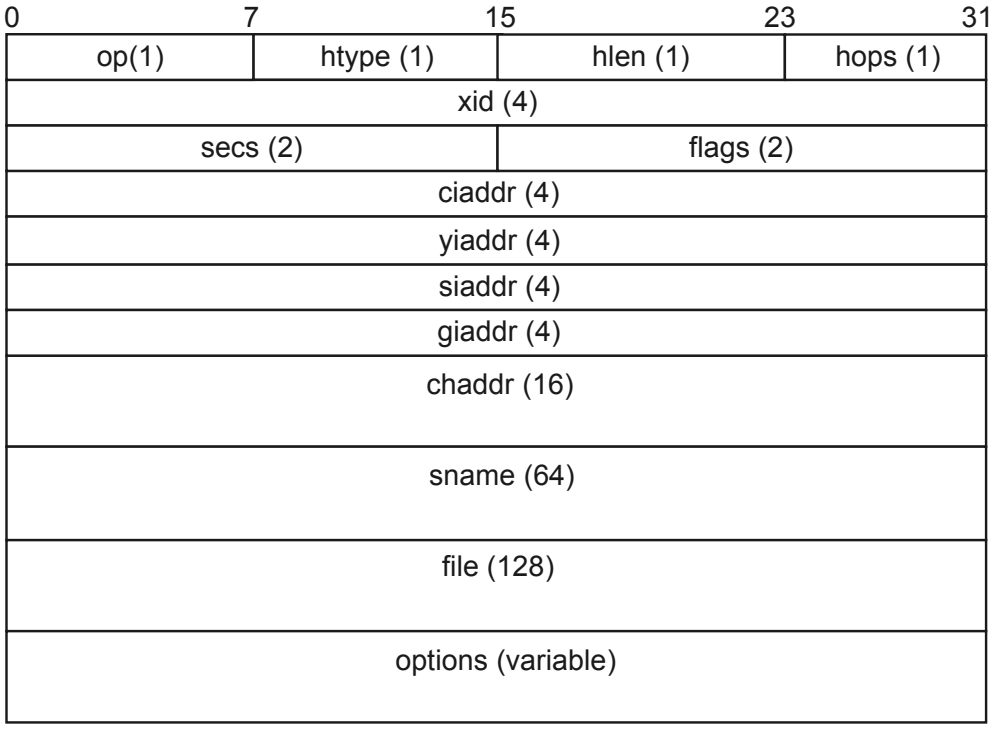
  A DHCP server processes requests of address allocation, address lease extending, and address releasing from a DHCP client or a DHCP relay agent, and allocates IP addresses and other network configuration parameters to the DHCP client.

3.8.2.2 Introduction to DHCP Messages

DHCP Message Format

Figure 3-38 shows the format of a DHCP message.

Figure 3-38 Format of a DHCP message



In **Figure 3-38**, numbers in the round brackets indicate the field length, expressed in bytes.

Table 3-21 Description of each field in a DHCP message

Field	Length	Description
op(op code)	1 byte	Indicates the message type. The options are as follows: ● 1: DHCP Request message ● 2: DHCP Reply message
htype (hardware type)	1 byte	Indicates the hardware address type. For Ethernet, the value of this field is 1.
hlen (hardware length)	1 byte	Indicates the length of a hardware address, expressed in bytes. For Ethernet, the value of this field is 6.

Field	Length	Description
hops	1 byte	Indicates the number of DHCP relay agents that a DHCP Request message passes through. This field is set to 0 by a DHCP client or a DHCP server. The value increases by 1 each time a DHCP Request message passes through a DHCP relay agent. This field limits the number of DHCP relay agents that a DHCP message can pass through. **NOTE** A maximum of 16 DHCP relay agents are allowed between a server and a client. That is, the number of hops must be smaller than or equal to 16. Otherwise, DHCP messages are discarded.
xid	4 bytes	Indicates a random number chosen by a DHCP client. It is used by the DHCP client and DHCP server to exchange messages.
secs (seconds)	2 bytes	Indicates the time elapsed since the client obtained or renewed an IP address, in seconds.
flags	2 bytes	Indicates the Flags field. Only the leftmost bit of the Flags field is valid and other bits are set to 0. The leftmost bit determines whether the DHCP server unicasts or broadcasts a DHCP Reply message. The options are as follows: ● 0: The DHCP server unicasts a DHCP Reply message. ● 1: The DHCP server broadcasts a DHCP Reply message.
ciaddr (client ip address)	4 bytes	Indicates the IP address of a client. The IP address can be an existing IP address of a DHCP client or an IP address assigned by a DHCP server to a DHCP client. During initialization, the client has no IP address and the value of this field is 0.0.0.0. **NOTE** The IP address 0.0.0.0 is used only for temporary communication during system startup in DHCP mode. It is an invalid address.
yiaddr (your client ip address)	4 bytes	Indicates the DHCP client IP address assigned by the DHCP server. The DHCP server fills this field into a DHCP Reply message.
siaddr (server ip address)	4 bytes	Server IP address from which a DHCP client obtains the startup configuration file.

Field	Length	Description
giaddr (gateway ip address)	4 bytes	Indicates the IP address of the first DHCP relay agent. If the DHCP server and client are located on different network segments, the first DHCP relay agent fills its IP address into this field of the DHCP Request message sent by the client and forwards the message to the DHCP server. The DHCP server determines the network segment where the client resides based on this field, and assigns an IP address on this network segment from an address pool. The DHCP server also returns a DHCP Reply message to the first DHCP relay agent. The DHCP relay agent then forwards the DHCP Reply message to the client. **NOTE** If the DHCP Request message passes through multiple DHCP Relay agents before reaching the DHCP server, the value of this field is the IP address of the first DHCP relay agent and remains unchanged. However, the value of the Hops field increases by 1 each time a DHCP Request message passes through a DHCP relay agent.
chaddr (client hardware address)	16 bytes	Indicates the client MAC address. This field must be consistent with the hardware type and hardware length fields. When sending a DHCP Request message, the client fills its hardware address into this field. For Ethernet, a 6-byte Ethernet MAC address must be filled in this field when the hardware type and hardware length fields are set to 1 and 6 respectively.
sname (server host name)	64 bytes	Indicates the name of the server from which a client obtains configuration parameters. This field is optional and is filled in by the DHCP server. The field must be filled in with a character string that ends with 0.
file (file name)	128 bytes	Indicates the Bootfile name specified by the DHCP server for a DHCP client. This field is filled in by the DHCP server and is delivered to the client when the IP address is assigned to the client. This field is optional. The field must be filled in with a character string that ends with 0.
options	Variable	Indicates the DHCP Options field, which has a maximum of 312 bytes. This field contains the DHCP message type and configuration parameters assigned by a server to a client, including the gateway IP address, DNS server IP address, and IP address lease. For details about the Options field, see **3.8.2.3 DHCP Options**.

DHCP Message Types

DHCP messages are classified into eight types. A DHCP server and a DHCP client communicate by exchanging DHCP messages.

Table 3-22 DHCP message types

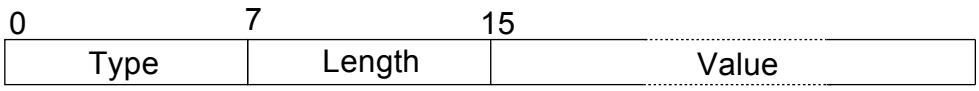
Message Name	Description
DHCP DISCOVER	A DHCP Discover message is broadcast by a DHCP client to locate a DHCP server when the client attempts to connect to a network for the first time.
DHCP OFFER	A DHCP Offer message is sent by a DHCP server to respond to a DHCP Discover message. A DHCP Offer message carries various configuration information.
DHCP REQUEST	A DHCP Request message is sent in the following conditions: ● After a DHCP client is initialized, it broadcasts a DHCP Request message to respond to the DHCP Offer message sent by a DHCP server. ● After a DHCP client restarts, it broadcasts a DHCP Request message to confirm the configuration including the assigned IP address. ● After a DHCP client obtains an IP address, it unicasts or broadcasts a DHCP Request message to update the IP address lease.
DHCP ACK	A DHCP ACK message is sent by a DHCP server to acknowledge the DHCP Request message from a DHCP client. After receiving a DHCP ACK message, the DHCP client obtains the configuration parameters including the IP address.
DHCP NAK	A DHCP NAK message is sent by a DHCP server to reject the DHCP Request message from a DHCP client. For example, after a DHCP server receives a DHCP Request message, it cannot find matching lease records. Then the DHCP server sends a DHCP NAK message, notifying that no IP address is available for the DHCP client.
DHCP DECLINE	A DHCP Decline message is sent by a DHCP client to notify the DHCP server that the assigned IP address conflicts with another IP address. Then the DHCP client applies to the DHCP server for another IP address.
DHCP RELEASE	A DHCP Release message is sent by a DHCP client to release its IP address. After receiving a DHCP Release message, the DHCP server can assign this IP address to another DHCP client.
DHCP INFORM	A DHCP Inform message is sent by a DHCP client to obtain other network configuration parameters such as the gateway address and DNS server address after the DHCP client has obtained an IP address.

3.8.2.3 DHCP Options

Options Field in a DHCP Packet

The Options field in a DHCP packet carries control information and parameters that are not defined in common protocols. When a DHCP client requests an IP address from the DHCP server configured with the Options field, the server replies a packet containing the Options field. **Figure 3-39** shows the format of the Options field.

Figure 3-39 Format of the Options field



The Options field consists of Type, Length, and Value. The following table provides the details.

Table 3-23 Description of the Options field

Field	Length	Description
Type	1 byte	Indicates the type of the message content.
Length	1 byte	Indicates the length of the message content.
Value	Depending on the setting of the Length field	Indicates the message content.

The value of the Options field ranges from 1 to 255. **Table 3-24** lists common DHCP options.

Table 3-24 Description of the Options field in DHCP packets

Options No.	Function
1	Specifies the subnet mask.
3	Specifies the gateway address.
6	Specifies the DNS server IP address.
12	Specifies the hostname.
15	Specifies the domain name.
33	Specifies a group of classful static routes. This option contains a group of classful static routes. When a DHCP client receives DHCP packets with this option, it adds the classful static routes contained in the option to its routing table. In classful routes, masks of destination addresses are natural masks and masks cannot be used to divide subnets. If Option 121 exists, this option is ignored.
44	Specifies the NetBIOS name.
46	Specifies the NetBIOS object type.
50	Specifies the requested IP address.
51	Specifies the IP address lease.

Options No.	Function
52	Specifies the additional option.
53	Specifies the DHCP packet type.
54	Specifies the server identifier.
55	Specifies the parameter request list. It is used by a DHCP client to request specified configuration parameters.
58	Specifies the lease renewal time (T1), which is 50% of the lease time.
59	Specifies the lease renewal time (T2), which is 87.5% of the lease time.
60	Specifies the vendor classification information option, which identifies the DHCP client type and configuration.
61	Specifies Client identifier.
66	Specifies the TFTP server name allocated to DHCP clients.
67	Specifies the Bootfile name allocated to DHCP clients.
77	Specifies the user type.
121	Specifies a group of classless routes. This option contains a group of classless static routes. After a DHCP client receives DHCP packets with this option, it adds the classless static routes contained in the option to its routing table. Classless routes are routes of which masks of destination addresses can be any values and masks can be used to divide subnets.

The objects of this field vary with the functions of the Options field. For example, Option 77 is used on a DHCP client to identify user types of the DHCP client. The DHCP server selects an address pool to allocate an IP address and configuration parameters to the DHCP client based on the User Class in the Option field. Option 77 is manually configured only on the DHCP client but not on the server.

NOTE

When the device functions as the DHCP client, the client can identify the Option121 field describing static routes in the DHCP packet sent by the DHCP server.

For more information about common DHCP options, see RFC 2132.

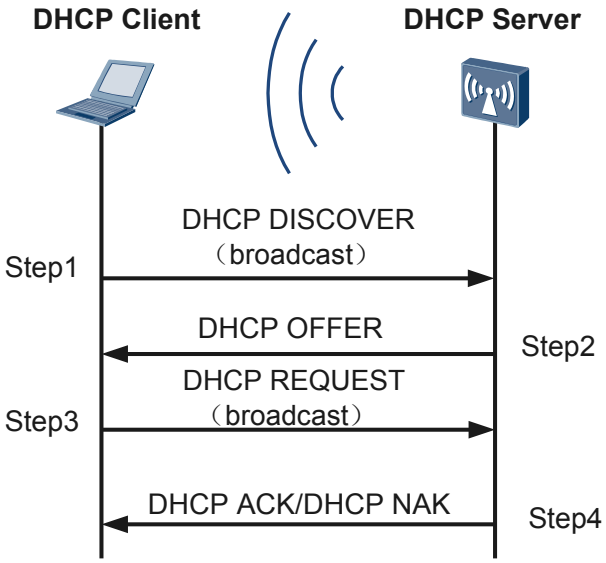
3.8.2.4 DHCP Principles

Modes for Interaction Between the DHCP Client and Server

To obtain a valid dynamic IP address, a DHCP client exchanges different messages with the server at different stages. Generally, the DHCP client and server interact in the following modes.

- The DHCP client dynamically obtains an IP address.

Figure 3-40 Procedure for a DHCP client to dynamically obtain an IP address



As shown in **Figure 3-40**, when a DHCP client accesses the network for the first time, the DHCP client sets up a connection with a DHCP server through the following four stages.

- Discovery stage: The DHCP client searches for the DHCP server.

  In this stage, the DHCP client sends a DHCP Discover message to search for the DHCP server. The DHCP server address is unknown to the client, so the DHCP client broadcasts the DHCP Discover message. All the DHCP servers send Reply messages after they receive the Discover message. In this way, the DHCP client knows locations of the DHCP servers on the network.

- Offer stage: The DHCP server offers an IP address to the DHCP client.

  The DHCP server receives the DHCP Discover message, selects an IP address from the address pool, and sends a DHCP Offer message to the DHCP client. The Offer message carries information such as the IP address, lease of the IP address, gateway address, and DNS server address.

- Request stage: The DHCP client selects an IP address.

  If multiple DHCP servers send DHCP Offer messages to the DHCP client, the client receives the first DHCP Offer message. Then the client broadcasts a DHCP Request message including the information about the DHCP server address (Option 54 field).

  The client broadcasts a DHCP Request message to notify all the DHCP servers that the client uses the IP address provided by the DHCP server in the Option 54 field and that all the other servers can use the assigned IP addresses.

- Acknowledgment stage: The DHCP server acknowledges the IP address that is offered.

  When the DHCP server receives the DHCP Request message from the DHCP client, the server searches the lease record based on the MAC address in the Request message. If there is the IP address record, the server sends a DHCP ACK message to the client, carrying the IP address and other configurations. After receiving the DHCP ACK message, the DHCP client broadcasts gratuitous ARP packets to detect whether any

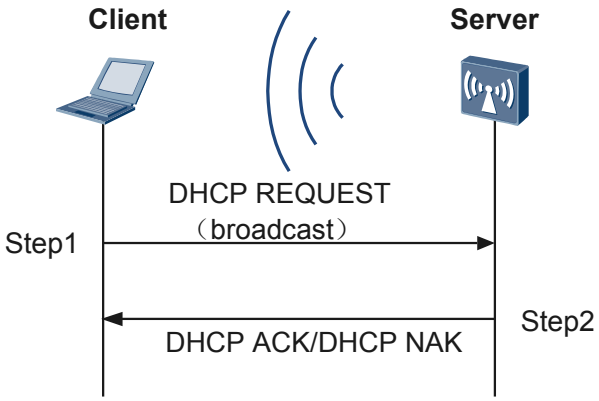
host is using the IP address assigned by the DHCP server. If no response is received within the specified time, the DHCP client uses the IP address.

If there is no IP address record or the server cannot assign IP addresses, the server sends a DHCP NAK message to notify the DHCP client that the server cannot assign IP addresses. The DHCP client needs to send a new DHCP Discover message to request a new IP address.

After obtaining the IP address, the DHCP client checks the status of the gateway in use before the client goes online. If the gateway address is incorrect or the gateway device fails, the DHCP client requests a new IP address using the four modes for interaction.

- The DHCP client uses the assigned IP address.

Figure 3-41 Procedure for the DHCP client to use the assigned IP address



As shown in **Figure 3-41**, when the DHCP client accesses a network for the second time, it set ups a connection with the DHCP server in the following procedure.

- The client accesses a network for the second time with the IP address that does not expire. The client does not need to send a DHCP Discover message again. It directly sends a DHCP Request message carrying the IP address assigned in the first time, namely, the Option 50 field in the message.
- After receiving the DHCP Request message, if the requested IP address is not assigned to another DHCP client, the DHCP server sends a DHCP ACK message to instruct the DHCP client to use the IP address again.
- If the IP address cannot be assigned to the DHCP client, for example, it has been assigned to another DHCP client, the DHCP server sends a DHCP NAK message to the DHCP client. After receiving the DHCP NAK message, the DHCP client sends a DHCP Discover message to request a new IP address.

- The DHCP client renews the IP address lease.

  An expected lease can be contained in the DHCP Request message sent to the server for an IP address. The server compares the expected lease with the lease in the address pool and assigns a shorter lease to the client.

  The IP address dynamically assigned to the DHCP client usually has a validity period. The DHCP server withdraws the IP address after the validity period expires. To keep using the IP address, the DHCP client needs to renew the IP address lease.

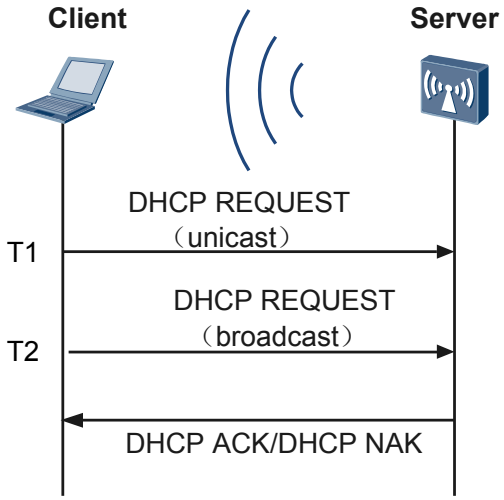
  When obtaining an IP address, the DHCP client enters the binding state. The client is configured with three timers to control lease renewal, rebinding, and lease expiration

respectively. When assigning an IP address to the DHCP client, the DHCP server also specifies values for the timers. If the server does not specify values for the timers, the client uses the default values. **Table 3-25** lists the default timer values.

Table 3-25 Default values of timers

Timer	Default Value
Lease renewal	50% of the lease
Rebinding	87.5% of the lease
Lease expiration	Overall lease

Figure 3-42 Procedure for a DHCP client to renew the IP address lease



As shown in **Figure 3-42**, when the DHCP client renews the IP address lease, it set ups a connection with the DHCP server in the following procedures:

- When 50% of the IP address lease (T1) has passed, the DHCP client unicasts a DHCP Request message to the DHCP server to renew the lease. If the client receives a DHCP ACK message, the address lease is successfully renewed. If the client receives a DHCP NAK message, it sends a request again.
- When 87.5% of the IP address lease (T2) has passed and the client has not received the Reply message, the DHCP client automatically sends a broadcast message to the DHCP server to renew the IP address lease. If the client receives a DHCP ACK message, the address lease is successfully renewed. If the client receives a DHCP NAK message, it sends a request again.
- If the client has not received a Reply message from the server when the IP address lease expires, the client must stop using the current IP address and send a DHCP Discover message to request a new IP address.

- The DHCP client releases an IP address.

  When the DHCP client does not use the assigned IP address, it sends a DHCP Release message to notify the DHCP server of releasing the IP address. The DHCP server retains

the DHCP client configurations so that the configurations can be used when the client requests an address again.

3.8.2.5 DHCP Relay Principles

The DHCP relay function enables message exchanges between a DHCP server and a client on different network segments. When the DHCP client and server are on different network segments, the DHCP relay agent transparently transmits DHCP messages to the destination DHCP server. In this way, DHCP clients on different network segments can communicate with one DHCP server.

Figure 3-43 shows how a DHCP client uses the DHCP relay agent to apply for an IP address for the first time.

Figure 3-43 Working process of a DHCP relay agent

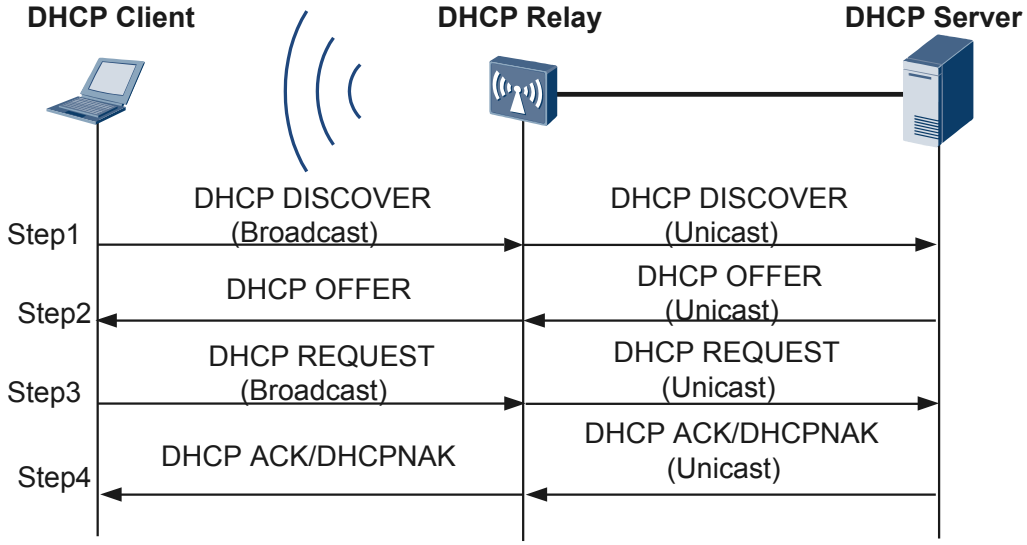


Figure 3-43 shows the working process of a DHCP relay agent. The DHCP client sends a Request message to the DHCP server. When receiving the message, the DHCP relay agent processes and unicasts the message to the specified DHCP server on the other network segment. The DHCP server sends requested configurations to the client through the DHCP relay agent based on information in the Request message.

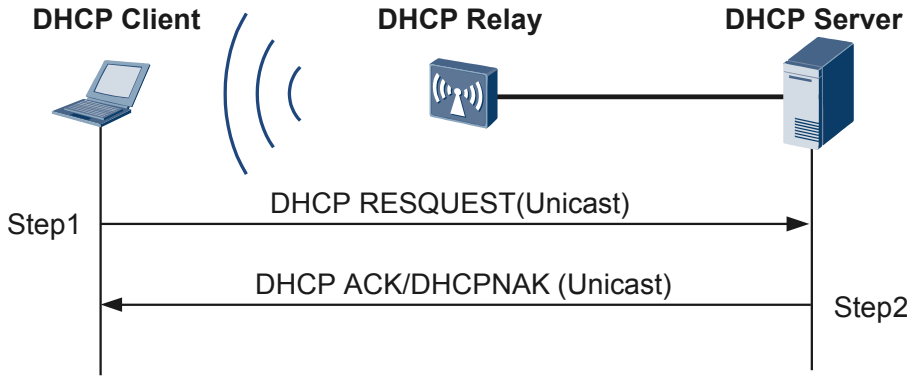
1. After receiving a DHCP Discover message or a Request message, the DHCP relay agent performs the following operations:
   - Discards DHCP Request messages whose number of hops is larger than the hop limit to prevent loops. Or, increases the value of the hop by 1, indicating that the message passes through a DHCP relay agent.
   - Checks the giaddr field. If the value is 0, set the value of the giaddr field to the IP address of the interface which receives the Request message. Selects one IP address if the interface has multiple IP addresses. All the Request messages received by the interface later use this IP address to fill the giaddr field. If the value is not 0, do not change the value.

- Sets the TTL in the request packets to the default value in the DHCP relay device, not the value calculated by decreasing the original TTL by 1. You can change the value of the hops field to prevent loops and limit hops.
- Changes the destination IP address of the DHCP Request message to the IP address of the DHCP server or the IP address of the next DHCP relay agent. In this way, the DHCP Request message can be forwarded to the DHCP server or the next DHCP relay agent.

2. The DHCP server assigns IP addresses to the client based on the Relay Agent IP Address field and sends the DHCP Reply message to the DHCP relay agent specified in the Relay Agent IP Address field. After receiving the DHCP Reply message, the DHCP relay agent performs the following operations:
   - The DHCP relay agent assumes that all the Reply messages are sent to the directly-connected DHCP clients. The Relay Agent IP Address field identifies the interface directly connected to the client. If the value of the Relay Agent IP Address field is not the IP address of a local interface, the DHCP relay agent discards the Reply message.
   - The DHCP relay agent checks the broadcast flag bit of the message. If the broadcast flag bit is 1, the DHCP relay agent broadcasts the DHCP Reply message to the DHCP client; otherwise, the DHCP relay agent unicasts the DHCP Reply message to the DHCP client. The destination IP address is the value in the Your (Client) IP Address field, and the MAC address is the value in the Client Hardware Address field.

Figure 3-44 shows how a DHCP client extends the IP address lease through the DHCP relay agent.

Figure 3-44 Extending the IP address lease through the DHCP relay agent



1. After accessing the network for the first time, the DHCP client only needs to unicast a DHCP Request message to the DHCP server that assigned its currently-used IP address.
2. The DHCP server then directly unicasts a DHCP ACK message or a DHCP NAK message to the client.

DHCP Releasing

The DHCP relay agent, instead of the client, can send a Release message to the DHCP server to release the IP addresses that assigned to the DHCP clients. You can configure a command on the DHCP relay agent to release the IP addresses that the DHCP server assigns to the DHCP client.

3.8.2.6 IP Address Assignment and Renewal

IP Address Assignment Sequence

The DHCP server assigns IP addresses to a client in the following sequence:

- IP address that is in the database of the DHCP server and is statically bound to the MAC address of the client
- IP address that has been assigned to the client before, that is, IP address in the Requested IP Addr Option of the DHCP Discover message sent by the client
- IP address that is first found when the DHCP server searches the DHCP address pool for available IP addresses
- If the DHCP address pool has no available IP address, the DHCP server searches the expired IP addresses and conflicting IP addresses, and then assigns a valid IP address to the client. If all the IP addresses are in use, an error is reported.

Method of Preventing Repeated IP Address Assignment

Before assigning an IP address to a client, the DHCP server needs to ping the IP address to avoid address conflicts.

By using the ping command, you can check whether a response to the ping packet is received within the specified period. If no response to the ping packet is received, the DHCP server keeps sending ping packets to the IP address to be assigned until the number of the sent ping packets reaches the maximum value. If there is still no response, this IP address is not in use, and the DHCP server assigns the IP address to a client. (This is implemented based on RFC 2132.)

IP Address Reservation

DHCP supports IP address reservation for clients. The reserved IP addresses can be those in the address pool or not. If an address in the address pool is reserved, it is no longer assignable. Addresses are usually reserved for DNS servers.

Method of IP Address Releasing and Lease Renewal on the PCs

The PCs (DHCP clients) must release the original IP addresses before obtaining new IP addresses.

- Releasing the original IP address

  Commands for renewing the lease of an IP address vary in different operating systems. You can use either of the following methods to renew the lease of an IP address:

  - Run the **ipconfig**/**release** command in the Window Vista/Windows XP/Windows2000/ DOS environment of the user PC to release the IP address of the PC.
  - Run the **winipcfg**/**release** command in the MS-DOS interface of Windows 98 to release the IP address of the PC.

  The user PC needs to send a DHCP Release message to the DHCP server.

- Renewing the IP address lease or applying for a new IP address

  The same command is used to apply for a new IP address and renew the IP address in the same operating system. Before applying for a new IP address, the PCs (DHCP clients) must

release the original IP addresses. If you want to renew the IP address lease, you do not have to release the IP address.

Different commands are used in different operating systems. You can use either of the following methods to apply for a new IP address:

- Run the **ipconfig**/**renew** command in the Windows Vista/Windows XP/Windows2000/ DOS environment of the user PC to apply for a new IP address.
- Run the **winipcfg**/**renew** command in the MS-DOS interface of Windows 98 to apply for a new IP address.

The user PC needs to send a DHCP Discover message to the DHCP server.

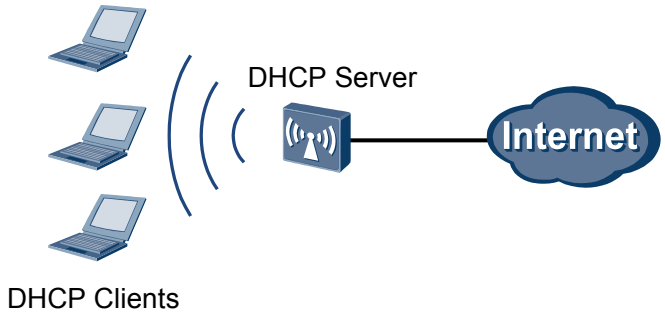
3.8.3 Application

This section describes the applicable scenario of DHCP.

3.8.3.1 DHCP Server Application

As it is shown in **Figure 3-45**, a DHCP server and multiple DHCP clients (such as PCs and portable computers) are deployed.

Figure 3-45 Typical networking of the DHCP server



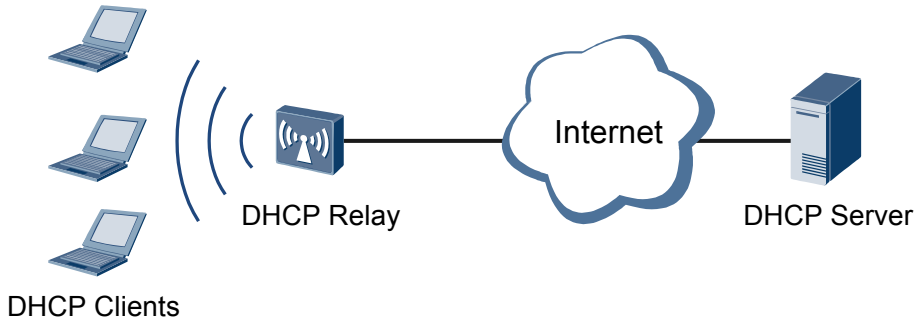
Generally, the DHCP server is used to assign IP addresses in the following scenarios:

- On a large network, manual configurations take a long time and bring difficulties to centralized management over the entire network.
- Hosts on the network are more than available IP addresses. Thus, not every host has a fixed IP address. Many hosts need to dynamically obtain IP addresses through the DHCP server. In addition, network administrators hope that there is a limit to the number of users of on-line at the same time.
- Only a few hosts on the network require fixed IP addresses.

3.8.3.2 DHCP Relay Application

Figure 3-46 shows typical networking of DHCP relay.

Figure 3-46 Typical networking of DHCP relay



The earlier DHCP protocol applies to only the scenario that the DHCP client and DHCP server are on the same network segment. To dynamically assign IP addresses to hosts on network segments, the network administrator needs to configure a DHCP server on each network segment, which increases costs.

The DHCP relay function is introduced to solve this problem. A DHCP client can apply to the DHCP server on another network segment to obtain a valid IP address. In this manner, DHCP clients on multiple network segments can share one DHCP server. This reduces costs and facilitates centralized management.

3.8.4 Default Configuration

This section provides default DHCP configurations.

Table 3-26 DHCP default configuration

Parameter	Default Value
Time interval at which the DHCP server waits for the response to ping packets to avoid IP address conflicts	500 ms
IP address lease	1 day
Interval for saving DHCP data to the storage device	300s
Rate of sending DHCP messages to the DHCP stack	100 pps

3.8.5 Configuring DHCP

3.8.5.1 Configuring a DHCP Server Based on the Global Address Pool

If a DHCP server based on a global address pool is configured, all online users of the server can obtain IP addresses from this address pool.

Pre-configuration Tasks

Before configuring a DHCP server based on the global address pool, complete the following tasks:

- Ensuring that the link between the DHCP client and the device works properly and the DHCP client can communicate with the device
- (Optional) Configuring the DNS service for the DHCP client
- (Optional) Configuring the NetBIOS service for the DHCP client
- Configuring routes from the device to the DNS server and the NetBIOS server (The routes are required only when the servers are configured.)
- (Optional) Configuring the customized DHCP option

3.8.5.1.1 Configuring the Global Address Pool

Context

The global address pool attributes include the IP address range, IP address lease, IP addresses not to be automatically allocated, and IP addresses to be statically bound to MAC addresses. IP addresses in the global address pool can be assigned dynamically or bound manually as required.

A maximum of 128 address pools, including global address pools and interface address pools, can be created on the access point.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip pool ip-pool-name
```

A global address pool is created and the global address pool view is displayed.

By default, no global address pool exists on the access point.

Step 3 Run:

```
network ip-address [ mask { mask | mask-length } ]
```

The range of IP addresses that can be allocated dynamically in the global address pool is specified.

By default, no network segment address for a global address pool is specified.

An address pool can contain only one address segment. The address range of the address pool is set by the mask.

NOTE

When configuring the range of dynamically assignable IP addresses in the global address pool, ensure that the range is the same as the network segment on which the DHCP server interface address or the DHCP relay agent interface address resides. This avoids incorrect assignment of IP addresses.

Step 4 (Optional) Run:

```
lease { day day [ hour hour [ minute minute ] ] | unlimited }
```

The IP address lease is set.

By default, the IP address lease is one day.

Different address pools on a DHCP server can be set with different IP address leases, but the IP addresses in one address pool must be configured with the same lease.

Step 5 (Optional) Run:

```
excluded-ip-address start-ip-address [ end-ip-address ]
```

The IP addresses that cannot be automatically allocated in the global address pool are configured.

By default, all IP addresses in the address pool can be automatically assigned to clients.

Some IP addresses in the global address pool are reserved for other services, for example, the IP address of the DNS server cannot be allocated to clients. If you run this command multiple times, you can set multiple IP address ranges that cannot be automatically allocated in the DHCP address pool.

Step 6 (Optional) Run:

```
gateway-list ip-address &<1-8>
```

The egress gateway address is configured for the DHCP clients.

When a DHCP client connects to the server or host outside the network segment, data must be forwarded through the egress gateway. Skip this step if the IP address of the interface connected to the DHCP server or the DHCP relay agent is used as the gateway IP address.

To load balance traffic and improve network reliability, configure multiple gateways. An address pool can be configured with a maximum of eight gateway addresses. Gateway addresses cannot be subnet broadcast addresses.

Step 7 (Optional) Run:

```
static-bind ip-address ip-address mac-address mac-address
```

An IP address in the global address pool is statically bound to the MAC address of a DHCP client.

By default, the IP address in a global address pool is not bound to any MAC address.

When a client requires a fixed IP address, bind an idle IP address in the address pool to the client MAC address.

NOTE

When the IP address in the global address pool is statically bound to a MAC address, the IP address must be in the range of IP addresses that can be allocated dynamically.

Step 8 (Optional) Run:

```
force insert option code &<1-254>
```

A DHCP server is configured to forcibly insert an Option field specified in the global address pool to a DHCP Response packet that it sends to a DHCP client.

By default, a DHCP server is not configured to forcibly insert an Option field to a DHCP Response packet that it sends to a DHCP client.

Step 9 (Optional) Run the following commands to configure the DHCP client to automatically obtain the startup configuration file.

1. Run:
   bootfile *bootfile*

   The name of the startup configuration file is configured for the DHCP client.

   By default, the startup configuration file name is not configured for the DHCP client.
2. Run:
   sname *sname*

   The name of the server where the DHCP client obtains the startup configuration file is configured.

   By default, the name of the server where the DHCP client obtains the startup configuration file is not configured.

NOTE

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP clients. Usually, the startup configuration file is saved on a specified file server. Therefore, the route between the DHCP client and the file server must be reachable.

Step 10 (Optional) Run:
next-server *ip-address*

The server IP address for DHCP clients is configured.

By default, no server IP address is specified.

Step 11 (Optional) Run:
lock

The IP address pool is locked.

By default, the IP address pool is unlocked.

Step 12 Run:
quit

The system view is displayed.

Step 13 (Optional) Run:
dhcp server bootp

The DHCP server is configured to respond to BOOTP requests.

By default, a DHCP server does not respond to BOOTP requests.

Step 14 (Optional) Run:
dhcp server bootp automatic

The DHCP server is configured to dynamically allocate IP addresses to BOOTP clients.

By default, the DHCP server does not dynamically allocate IP addresses to BOOTP clients.

When the device functions as the DHCP server, the device can allocate IP addresses to BOOTP clients if the BOOTP clients reside on the same network as the DHCP server. You can run the **dhcp server bootp automatic** command to dynamically allocate IP addresses. You can also run

the **static-bind ip-address** *ip-address* **mac-address** *mac-address* command to allocate IP addresses to BOOTP clients in the static binding mode.

----End

3.8.5.1.2 Configuring an Interface to Use the Global Address Pool

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp enable
```

DHCP is enabled.

Step 3 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 4 Run:

```
ip address ip-address { mask | mask-length }
```

An IP address is assigned to the interface.

When users connected to the interface that has an IP address configured request IP addresses:

- If the access point used as the DHCP server is on the same network segment as DHCP clients, and no relay agent is deployed between them, the access point assigns IP addresses on the same network segment as the interface to users who get online from the interface. If the interface is not configured with an IP address or no address pool is on the same network segment as the interface address, the clients cannot go online.
- If the access point used as the DHCP server and DHCP clients are on different network segments, and a DHCP relay agent is deployed between them, the access point parses the giaddr field of a DHCP Request message to obtain an IP address. If the IP address does not match the corresponding address pool, the user cannot get online.

Step 5 Run:

```
dhcp select global
```

The interface is configured to use the global address pool.

After the configuration is complete, users who get online from this interface can obtain IP addresses and other configuration parameters from the global address pool.

NOTE

If there is a DHCP relay agent between the DHCP client and server, this step is optional. Otherwise, this step is mandatory.

----End

3.8.5.1.3 (Optional) Configuring the DNS Service and NetBIOS Service on the DHCP Client

Context

To ensure normal operations of DHCP clients, you can specify the DNS server address and the NetBIOS server address when the DHCP server assigns an IP address to the DHCP client.NetBIOS:Network Basic Input Output System. When a DHCP client uses the NetBIOS protocol for communication, host names must be mapped to IP addresses. Based on the modes of obtaining mapping, NetBIOS nodes are classified into the following types:

- b-node: indicates a node in broadcast mode. This node obtains mappings in broadcast mode.
- p-node: indicates a node in peer-to-peer mode. This node obtains mappings by communicating with the NetBIOS server.
- m-node: indicates a node in mixed mode. An m-node is a p-node that has some broadcast features.
- h-node: indicates a node in hybrid mode. An h-node is a b-type node enabled with the end-to-end communication mechanism.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip pool ip-pool-name
```

The IP address pool view is displayed.

Step 3 Run:

```
domain-name domain-name
```

The DNS domain name to be assigned to a DHCP client is configured.

Step 4 Run:

```
dns-list ip-address &<1-8>
```

The IP address of the DNS server is configured for a DHCP client.

To load balance the traffic and improve network reliability, configure multiple DNS servers. Each address pool can be configured with a maximum of eight DNS server addresses.

Step 5 Run:

```
nbns-list ip-address &<1-8>
```

The IP address of the NetBIOS server used by the DHCP client is assigned.

Each address pool can be configured with a maximum of eight NetBIOS server address.

Step 6 Run:

```
netbios-type { b-node | h-node | m-node | p-node }
```

The NetBIOS node type of the DHCP client is configured.

By default, no NetBIOS node type is specified for DHCP clients.

----End

3.8.5.1.4 (Optional) Configuring a Customized DHCP Option for the Global Address Pool

Context

DHCP provides various options. To use these options, add them to the attribute list of the DHCP server manually. If the DHCP server is configured with the Options field, the DHCP client obtains the configuration of the Options field from the DHCP packet replied by the DHCP server when the client requests an IP address from the server.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip pool ip-pool-name
```

The IP address pool view is displayed.

Step 3 Run:

```
option code [ sub-option sub-code ] { ascii ascii-string | hex hex-string | ip-address ip-address &<1-8> }
```

The customized DHCP option is configured.

After the **option** command is used, the specified option is carried by the reply message returned by the DHCP server. Before using this command, ensure that you know the functions of the option to be configured. For details on DHCP options, see RFC 2132.

----End

3.8.5.1.5 (Optional) Preventing Repeated IP Address Allocation

Context

Before assigning an address to a client, the access point used as the DHCP server needs to ping the IP address to avoid address conflicts.

After the **dhcp server ping** command is executed, the DHCP server can prevent repeated IP address allocation. The DHCP server pings an IP address to be allocated. If there is no response to the ping packet within a certain period, the DHCP server continues to send ping packets to this IP address until the number of ping packets reaches the maximum value. If there is still no response, this IP address is not in use, and the DHCP server allocates the IP address to a client.

Duplicate IP address detection on the DHCP server should not be too long. Otherwise, the client cannot obtain an IP address. It is recommended that the configured total detection time (Maximum number of send ping packets x Maximum response time) be smaller than 8s.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp server ping packet number
```

The maximum number of ping packets to be sent by the access point is set.

Step 3 Run:

```
dhcp server ping timeout milliseconds
```

The period in which the access point waits for the response is set.

By default, the period in which the access point waits for the response is 500 ms.

----End

3.8.5.1.6 (Optional) Configuring Automatic Saving of DHCP Data

Context

When the device functions as the DHCP server, you can enable automatic saving of DHCP data so that IP address information is saved to the storage device periodically.

You can configure the device to save DHCP data to the storage device. When a fault occurs, you can restore data from the storage device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp server database enable
```

The function that saves DHCP data to the storage device is enabled.

By default, DHCP data is not saved to the storage device.

After this command is executed, the system generates the **lease.txt** and **conflict.txt** files and saves them in the dhcp folder of the storage device. The two files save the address lease information and address conflict information. Run the command **display dhcp server database** to check the storage device for saving DHCP data.

Step 3 Run:

```
dhcp server database write-delay interval
```

The interval for saving DHCP data is set.

After the device is configured to automatically save DHCP data, the device saves data every 300 seconds by default and the latest data overwrites the previous data.

Step 4 Run:

```
dhcp server database recover
```

The DHCP data in the storage device is restored.

After this command is executed, the device restores DHCP data from the storage device during a restart.

----End

3.8.5.1.7 (Optional) Configuring the DHCP Server to trust Option 82

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp server trust option82
```

The access point is configured to trust Option 82.

By default, the DHCP server trusts Option 82.

----End

3.8.5.1.8 Checking the Configuration

Procedure

- Run the **display ip pool** [**name** *ip-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]] command to check information about the specified global address pool.
- Run the **display dhcp server database** command to check information about the DHCP database.

----End

3.8.5.2 Configuring a DHCP Server Based on an Interface Address Pool

After a DHCP server based on an interface address pool is configured, only users that go online from this interface can obtain IP addresses from this address pool.

Pre-configuration Tasks

Before configuring a DHCP server based on an interface address pool, complete the following tasks:

- Ensuring that the link between the DHCP client and the device works properly and the DHCP client can communicate with the device
- (Optional) Configuring the DNS server
- (Optional) Configuring the NetBIOS server

- Configuring routes from the device to the DNS server and the NetBIOS server (The routes are required only when the servers are configured.)

3.8.5.2.1 Configuring an Interface Address Pool

Context

The interface address pool attributes include the IP address lease, IP addresses not to be automatically allocated, and IP addresses to be statically bound to MAC addresses. IP addresses in the interface address pool can be assigned dynamically or bound manually as required.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp enable
```

DHCP is enabled.

Step 3 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 4 Run:

```
ip address ip-address { mask | mask-length }
```

An IP address is assigned to the interface.

Step 5 Run:

```
dhcp select interface
```

The interface is configured to use the interface address pool.

The interface address pool is actually the network segment to which the interface belongs, and such an interface address pool only applies to this interface.

Step 6 (Optional) Run:

```
dhcp server lease { day day [ hour hour [ minute minute ] ] | unlimited }
```

The IP address lease is set.

By default, the IP address lease is one day.

Step 7 (Optional) Run:

```
dhcp server excluded-ip-address start-ip-address [ end-ip-address ]
```

The IP addresses that cannot be automatically allocated in the interface address pool are configured.

Some IP addresses in the interface address pool are reserved for other services, for example, the IP address of the DNS server cannot be allocated to clients. If you run this command multiple

times, you can set multiple IP address ranges that cannot be automatically allocated in the DHCP address pool.

Step 8 (Optional) Run:

```
dhcp server static-bind ip-address ip-address mac-address mac-address
```

An IP address in the interface address pool is statically bound to the MAC address of a DHCP client.

When a client requires a fixed IP address, bind an idle IP address in the address pool to the client MAC address.

NOTE

When the IP address in the interface address pool is statically bound to a MAC address, the IP address must be in the range of IP addresses that can be allocated dynamically.

Step 9 (Optional) Run:

```
dhcp server force insert option  code &<1-254>
```

A DHCP server is configured to forcibly insert the specified Option field to a DHCP Response packet that it sends to a DHCP client.

By default, no DHCP server forcibly inserts the specified Option field to a DHCP Response packet that it sends to a DHCP client.

Step 10 (Optional) Run the following commands to configure the DHCP client to automatically obtain the startup configuration file.

1. Run:

   ```
   dhcp server bootfile bootfile
   ```

   The name of the startup configuration file is configured for the DHCP client.

   By default, the startup configuration file name is not configured for a DHCP client.

2. Run:

   ```
   dhcp server sname sname
   ```

   The name of the server from which the DHCP client obtains the startup configuration file is configured.

   By default, the name of the server from which the DHCP client obtains the startup configuration file is not configured.

NOTE

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP client. Usually, the startup configuration file is saved on a specified file server. Therefore, the route between the DHCP client and the file server must be reachable.

Step 11 Run:

```
dhcp server next-server ip-address
```

The IP address of a server is configured for the client after the client automatically obtains the IP address.

By default, the IP address of a server is not configured for the client after the client automatically obtains the IP address.

Step 12 Run:

```
quit
```

The system view is displayed.

Step 13 (Optional) Run:

```
dhcp server bootp
```

The DHCP server is configured to respond to BOOTP requests.

By default, a DHCP server does not respond to BOOTP requests.

Step 14 (Optional) Run:

```
dhcp server bootp automatic
```

The DHCP server is configured to dynamically allocate IP addresses to BOOTP clients.

By default, a DHCP server does not dynamically allocate IP addresses to BOOTP clients.

When the device functions as the DHCP server, the device can allocate IP addresses to BOOTP clients if the BOOTP clients reside on the same network as the DHCP server. You can run the **dhcp server bootp automatic** command to dynamically allocate IP addresses. You can also run the **dhcp server static-bind ip-address** *ip-address* **mac-address** *mac-address* command to allocate IP addresses to BOOTP clients in the static binding mode.

----End

3.8.5.2.2 (Optional) Configuring the DNS Service and NetBIOS Service on the DHCP Client

Context

The DNS and NetBIOS configurations must be specified before the DHPC server assigns IP addresses to the DHCP client.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
dhcp server domain-name domain-name
```

The DNS domain name is assigned to the DHCP client.

Step 4 Run:

```
dhcp server dns-list ip-address &<1-8>
```

The IP address of the DNS server is assigned to the DHCP client.

Each address pool can be configured with a maximum of eight DNS server addresses.

Step 5 Run:

```
dhcp server nbns-list ip-address &<1-8>
```

The IP address of the NetBIOS server used by the DHCP client is assigned.

Each address pool can be configured with a maximum of eight NetBIOS server addresses.

Step 6 Run:

```
dhcp server netbios-type { b-node | h-node | m-node | p-node }
```

The NetBIOS node type of the DHCP client is configured.

By default, no NetBIOS node type is specified for DHCP clients.

----End

3.8.5.2.3 (Optional) Configuring a Customized DHCP Option for an Interface Address Pool

Context

DHCP provides various options. To use these options, add them to the attribute list of the DHCP server manually.

When a DHCP client requests an IP address from the DHCP server configured with the Options field, the server returns a DHCP Reply message containing the Options field.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
dhcp server option code [ sub-option sub-code ] { ascii ascii-string | hex hex-string | ip-address ip-address &<1-8> }
```

The customized DHCP option is configured.

After the **dhcp server option** command is run, the specified option is carried by the DHCP Reply message returned by the DHCP server. Before using this command, ensure that you know the functions of the option to be configured. For details on DHCP options, see RFC 2132.

----End

3.8.5.2.4 (Optional) Preventing Repeated IP Address Allocation

Context

Before assigning an address to a client, the access point used as the DHCP server needs to ping the IP address to avoid address conflicts.

After the **dhcp server ping** command is executed, the DHCP server can prevent repeated IP address allocation. The DHCP server pings an IP address to be allocated. If there is no response

to the ping packet within a certain period, the DHCP server continues to send ping packets to this IP address until the number of ping packets reaches the maximum value. If there is still no response, this IP address is not in use, and the DHCP server allocates the IP address to a client.

Duplicate IP address detection on the DHCP server should not be too long. Otherwise, the client cannot obtain an IP address. It is recommended that the configured total detection time (Maximum number of send ping packets x Maximum response time) be smaller than 8s.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp server ping packet number
```

The maximum number of ping packets to be sent by the access point is set.

Step 3 Run:

```
dhcp server ping timeout milliseconds
```

The period in which the access point waits for the response is set.

By default, the period in which the access point waits for the response is 500 ms.

----End

3.8.5.2.5 (Optional) Configuring Automatic Saving of DHCP Data

Context

When the device functions as the DHCP server, you can enable automatic saving of DHCP data so that IP address information is saved to the storage device periodically.

You can configure the device to save DHCP data to the storage device. When a fault occurs, you can restore data from the storage device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp server database enable
```

The function that saves DHCP data to the storage device is enabled.

By default, DHCP data is not saved to the storage device.

After this command is executed, the system generates the **lease.txt** and **conflict.txt** files and saves them in the dhcp folder of the storage device. The two files save the address lease

information and address conflict information. Run the command **display dhcp server database** to check the storage device for saving DHCP data.

Step 3 Run:

```
dhcp server database write-delay interval
```

The interval for saving DHCP data is set.

After the device is configured to automatically save DHCP data, the device saves data every 300 seconds by default and the latest data overwrites the previous data.

Step 4 Run:

```
dhcp server database recover
```

The DHCP data in the storage device is restored.

After this command is executed, the device restores DHCP data from the storage device during a restart.

----End

3.8.5.2.6 (Optional) Configuring the DHCP Server to trust Option 82

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp server trust option82
```

The access point is configured to trust Option 82.

By default, the DHCP server trusts Option 82.

----End

3.8.5.2.7 Checking the Configuration

Procedure

- Run the **display ip pool** [**interface** *interface-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]] command to view information about the IP address pool.

----End

3.8.5.3 Configuring a DHCP Relay Agent

By using a DHCP relay agent, a DHCP client can communicate with a DHCP server on another network segment to obtain an IP address and other configuration information.

Pre-configuration Tasks

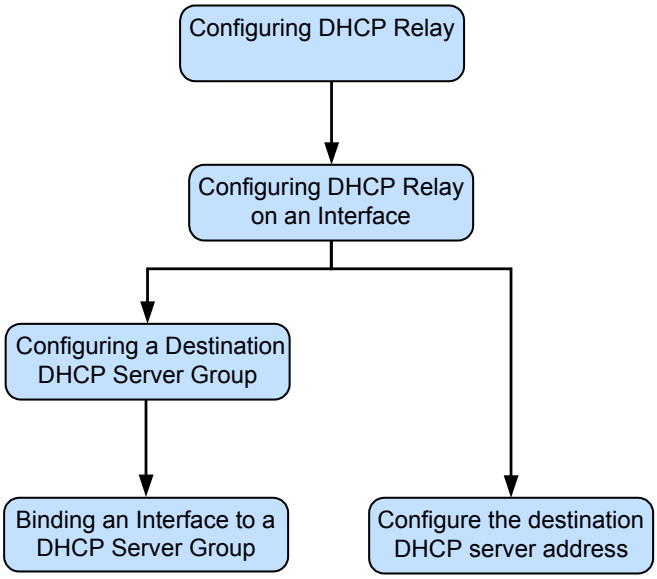
Before configuring a DHCP relay agent, complete the following tasks:

- Configuring a DHCP server
- Configuring a route from the device used as the DHCP relay agent to the DHCP server

Configuration Process

Figure 3-47 shows the configuration process.

Figure 3-47 DHCP relay agent configuration process



3.8.5.3.1 Configuring DHCP Relay on an Interface

Context

When the network where a DHCP client resides does not have a DHCP server, a DHCP relay agent can be configured to forward DHCP messages of the client to a DHCP server.

NOTE

A DHCP message is forwarded between a DHCP client and a DHCP server at most 16 times, and then the DHCP message is discarded.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp enable
```

DHCP is enabled.

Step 3 Run:

dhcp relay detect enable

User entry detection is enabled on a DHCP relay agent.

By default, user entry detection is disabled on a DHCP relay agent.

If multiple DHCP relay agents exist on the network, run the **dhcp relay detect enable** command to enable user entry detection on the DHCP relay agent to prevent the IP addresses assigned to clients from conflicting with those of other clients.

Step 4 (Optional) Run:

ip relay address cycle

The DHCP server polling function on a DHCP relay agent is enabled.

By default, the DHCP server polling function is disabled on the DHCP relay agent.

Step 5 Run:

interface *interface-type interface-number*

The interface view is displayed.

Step 6 Run:

ip address *ip-address* { *mask* | *mask-length* }

An IP address is assigned to the interface.

Step 7 Run:

dhcp select relay

The DHCP relay function is enabled on the interface.

Step 8 Run:

quit

Return to the system view.

Step 9 (Optional) Run:

dhcp relay trust option82

The device is configured to trust Option 82.

By default, the device does not discard DHCP messages with Option 82 and giaddr field of the packet is 0.

----End

Follow-up Procedure

When the DHCP relay function is enabled on an interface, specify the DHCP server IP address on the interface in either of the following ways:

- Configure a destination DHCP server group and bind the group to the interface. For details, see **3.8.5.3.2 Configuring a Destination DHCP Server Group** and **3.8.5.3.3 Binding an Interface to a DHCP Server Group**.
- Run the **dhcp relay server-ip** *ip-address* command in the interface view to configure the destination DHCP server address.

3.8.5.3.2 Configuring a Destination DHCP Server Group

Context

After a DHCP server group is created and server IP addresses are added to the group, the access point used as the DHCP relay agent can forward messages to multiple servers.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp server group group-name
```

A DHCP server group is created and the DHCP server group view is displayed.

You can configure a maximum of 32 DHCP server groups in the system, and a maximum of 20 DHCP servers in a DHCP server group.

Step 3 Run:

```
dhcp-server ip-address [ ip-address-index ]
```

A DHCP server is added to a DHCP server group.

A maximum of 20 DHCP servers can be added to a DHCP server group.

Step 4 (Optional)Run:

```
gateway ip-address
```

A gateway address is configured for the DHCP server.

----End

3.8.5.3.3 Binding an Interface to a DHCP Server Group

Context

After the DHCP relay function is enabled on an interface, bind a DHCP server group to the interface so that DHCP clients can access DHCP servers in the bound server group.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
dhcp relay server-select group-name
```

A DHCP server group is bound to the interface.

One interface can be configured with only one DHCP server group.

----End

3.8.5.3.4 (Optional) Configuring the DHCP Relay Agent to Send DHCP Release Messages

Context

If a user is forcibly disconnected, you can manually release the IP address assigned to the user on the DHCP server. You can configure the DHCP relay agent to actively send DHCP Release messages to the DHCP server. The DHCP server then releases the specified IP addresses.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 (Optional) Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
dhcp relay release client-ip-address mac-address [ server-ip-address ]
```

The DHCP relay agent is configured to send DHCP Release messages to the DHCP server.

- When you use the **dhcp relay release** command in the system view:
  - If no DHCP server is specified, the DHCP relay agent will send DHCP Release messages to the servers in all DHCP server groups bound to the DHCP relay interfaces.
  - If a DHCP server is specified, the DHCP relay agent sends DHCP Release messages to only the specified DHCP server.
- When you use the **dhcp relay release** command in the VLANIF interface view:
  - If no DHCP server is specified, the DHCP relay agent will send DHCP Release messages to all the servers in the DHCP server group bound to this VLANIF interface.
  - If a DHCP server is specified, the DHCP relay agent sends DHCP Release messages to only the specified DHCP server.

----End

3.8.5.3.5 (Optional) Configuring Strategies for Processing Option 82 Information on the DHCP Relay Agenet

Context

When DHCP Request messages carry Option 82 information, the DHCP server can locate user positions accurately and assign IP addresses to users using different policies. You can configure strategies that the DHCP relay agent uses to process Option 82 information.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
dhcp relay information enable
```

The Option 82 function is enabled on the DHCP relay agent.

By default, the Option 82 function is disabled for the DHCP relay agent.

Step 4 Run:

```
dhcp relay information strategy { drop | keep | replace }
```

Strategies used by the DHCP relay agent to process Option 82 information are configured.

By default, the strategy used by the DHCP relay agent to process Option 82 information is **replace**.

----End

3.8.5.3.6 (Optional) Configuring User Entry Detection on a DHCP Relay Agent

Context

After user entry detection is enabled on a DHCP relay agent, the DHCP relay agent creates a user entry after a user obtains an IP address through DHCP relay.

- When receiving a Release or Decline message from a DHCP client, the DHCP relay agent deletes the matching user entry.
- When receiving an ACK message from the DHCP server, the DHCP relay agent checks whether the IP address and MAC address of the DHCP client match the user entry.
  - If the IP address and MAC address are the same as those in the user entry, the DHCP relay agent continues to forward the ACK message.
  - If the IP address and MAC address are different from those in the user entry, the DHCP relay agent sends a Decline message to the DHCP server and sends a NAK message to the DHCP client to prohibit the client from using the IP address.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dhcp relay detect enable
```

User entry detection is enabled on a DHCP relay agent.

By default, user entry detection is disabled on a DHCP relay agent.

----End

3.8.5.3.7 Checking the Configuration

Procedure

- Run the **display dhcp relay** { **all** | **interface** *interface-type interface-number* } command to view the DHCP server group or the DHCP servers on the DHCP relay interface.
- Run the **display dhcp relay statistics** command to view packet statistics on the DHCP relay agent.
- Run the **display dhcp server group** [*group-name*] command to view the DHCP server group configuration.
- Run the **display dhcp relay user-table** { **all** | **ip-address** *ip-address* | **mac-address** *mac-address* } command to view user entries on a DHCP relay agent

----End

3.8.6 Maintaining DHCP

After DHCP configurations are complete, you can clear DHCP statistics and monitor DHCP operation.

3.8.6.1 Clearing DHCP Statistics

Context

During routine maintenance, you can use the reset commands to clear DHCP statistics.

NOTICE

DHCP statistics cannot be restored after they are cleared. Exercise caution when running the reset commands.

Procedure

- Run the **reset dhcp server statistics** command in the user view to clear DHCP server statistics.
- Run the **reset dhcp statistics** command in the user view to clear the DHCP message statistics.
- Run the **reset dhcp relay statistics** [**server-group** *group-name*] command in the user view to clear DHCP relay agent statistics.
- Run the **reset dhcp relay user-table** { **all** | **ip-address** *ip-address* | **mac-address** *mac-address* } command in the user view to clear user entries on a DHCP relay agent.

----End

3.8.6.2 Clearing the DHCP Address Pool

Procedure

- Run the **reset ip pool** { **interface** *pool-name* | **name** *ip-pool-name* } { *start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used** } command to reset the configured IP address pool on the device.

----End

3.8.6.3 Monitoring DHCP Operation

Context

DHCP packet statistics contain only the number of packets received and sent by the DHCP module.

Procedure

- Run the **display dhcp statistics** command to view DHCP message statistics.
- Run the **display dhcp relay statistics** [**server-group** *group-name*] command to view statistics on the DHCP Relay Agent.
- Run the **display dhcp server statistics** command to view statistics on the DHCP Server.
- Run the **display dhcp relay** { **all** | **interface** *interface-type interface-number* } command to view the DHCP server group or the DHCP server on a VLANIF interface.

----End

3.8.7 Configuration Examples

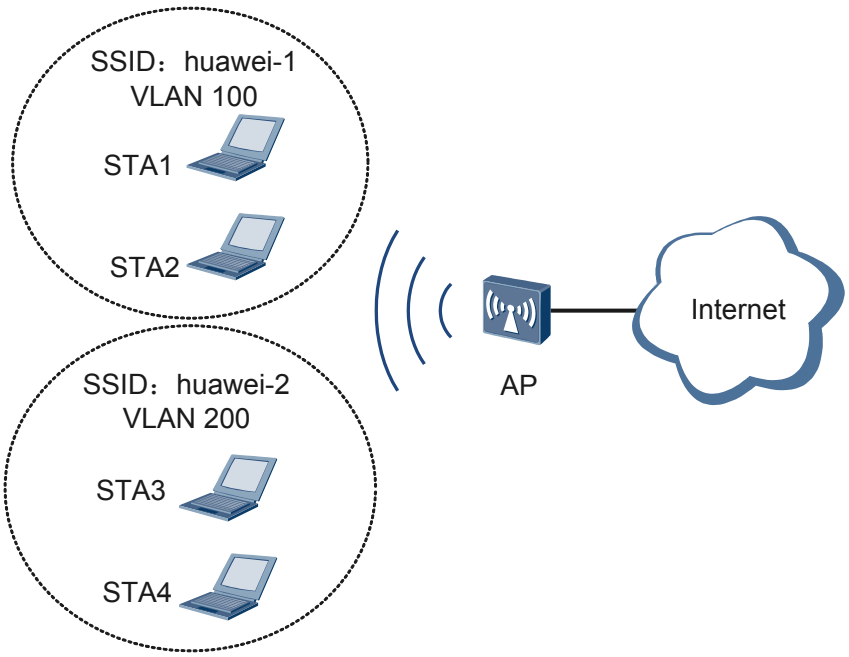
This section provides DHCP configuration examples including networking requirements and configuration roadmap.

3.8.7.1 Example for Configuring a DHCP Server Based on the Global Address Pool in the Same Network Segment

Networking Requirements

As shown in **Figure 3-48**, an enterprise provides WLAN services for employees and external users, and expects that the employees and external users can obtain IP addresses dynamically. The employees access the Internet through the network named **huawei-1** and belong to service VLAN 100. The employees are located on the network segment 10.1.1.0/25 and the lease of the IP addresses is 10 days. The external users access the Internet through the network named **huawei-2** and belong to service VLAN 200. The external users are located on the network segment 10.1.1.128/25 and the lease of the IP addresses is 2 days.

Figure 3-48 Networking diagram for configuring the DHCP server based on the global address pool



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure two global address pools on the AP and set corresponding attributes to dynamically assign IP addresses for employees and external users as required.

Procedure

Step 1 Enable the DHCP service.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] dhcp enable
```

Step 2 Create address pools and set corresponding attributes.

Set attributes for IP address pool 1, including the address pool range, egress gateway, and address lease.

```
[AP] ip pool 1
[AP-ip-pool-1] network 10.1.1.0 mask 255.255.255.128
[AP-ip-pool-1] gateway-list 10.1.1.1
[AP-ip-pool-1] lease day 10
[AP-ip-pool-1] quit
```

Set attributes for IP address pool 2, including the address pool range, egress gateway, and address lease.

```
[AP] ip pool 2
[AP-ip-pool-2] network 10.1.1.128 mask 255.255.255.128
[AP-ip-pool-2] gateway-list 10.1.1.129
```

```
[AP-ip-pool-2] lease day 2
[AP-ip-pool-2] quit
```

Step 3 # Configure clients connected to the VLANIF interface to obtain IP addresses from the global address pools.

```
[AP] vlan batch 100 200
[AP] interface vlanif 100
[AP-Vlanif100] ip address 10.1.1.1 255.255.255.128
[AP-Vlanif100] dhcp select global
[AP-Vlanif100] quit
[AP] interface vlanif 200
[AP-Vlanif200] ip address 10.1.1.129 255.255.255.128
[AP-Vlanif200] dhcp select global
[AP-Vlanif200] quit
```

Step 4 Verify the configuration.

Run the **display ip pool** command on the AP to check configurations of the IP address pools.

```
[AP] display ip pool
   ------------------------------------------------------------------------
  Pool-name      : 1
  Pool-No        : 0
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.1.1.1
  Mask           : 255.255.255.128
  VPN instance   : --

  ------------------------------------------------------------------------
  Pool-name      : 2
  Pool-No        : 1
  Position       : Local           Status           : Unlocked
  Gateway-0      : 10.1.1.129
  Mask           : 255.255.255.128
  VPN instance   : --


   IP address Statistic
    Total       :250
    Used        :4          Idle        :246
    Expired     :0          Conflict    :0          Disable   :0
```

----End

Configuration File

Configuration file of the AP

```
#
 sysname AP
#
 vlan batch 100 200
#
dhcp enable
#
ip pool 1
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.128
 lease day 10 hour 0 minute 0
#
ip pool 2
 gateway-list 10.1.1.129
 network 10.1.1.128 mask 255.255.255.128
 lease day 2 hour 0 minute 0
#
interface Vlanif100
```

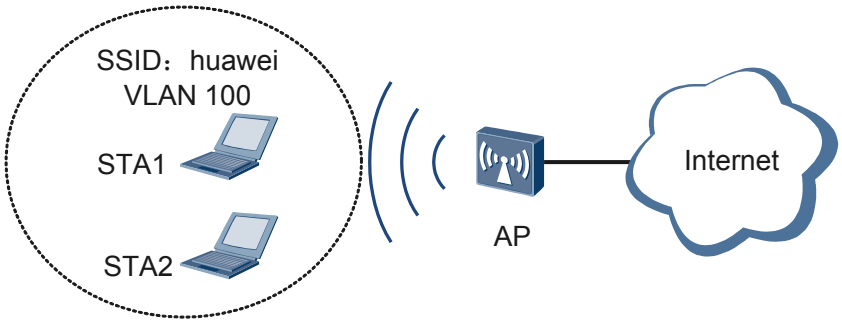
```
 ip address 10.1.1.1 255.255.255.128
 dhcp select global
#
interface Vlanif200
 ip address 10.1.1.129 255.255.255.128
 dhcp select global
#
return
```

3.8.7.2 Example for Configuring a DHCP Server Based on the Interface Address Pool in the Same Network Segment

Networking Requirements

As shown in **Figure 3-49**, an enterprise provides the WLAN service for employees, and expects that the employees can dynamically obtain IP addresses. The employees access the Internet through the network named **huawei** and belong to service VLAN 100. They are located on the network segment 10.1.1.0/24 and the lease of the IP addresses is 5 days.

Figure 3-49 Networking diagram for configuring a DHCP server based on a VLANIF interface address pool



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a DHCP server based on a VLANIF interface address pool on the AP to dynamically assign IP addresses to employees.

Procedure

Step 1 Enable the DHCP service.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] dhcp enable
```

Step 2 Configure the clients connected to VLANIF 100 to obtain IP addresses from the interface address pool.

```
[AP] vlan 100
[AP] interface vlanif 100
[AP-Vlanif100] ip address 10.1.1.1 24
[AP-Vlanif100] dhcp select interface
```

```
[AP-Vlanif100] dhcp server lease day 5
[AP-Vlanif100] quit
```

Step 3 Verify the configuration.

Run the **display ip pool interface** command on the AP to check the configuration of the interface address pool.

```
[AP] display ip pool interface vlanif 100
  Pool-name      : Vlanif100
  Pool-No        : 0
  Lease          : 5 Days 0 Hours 0 Minutes
  Domain-name    : huawei.com
  DNS-server0    : -
  NBNS-server0   : -
  Netbios-type   : -
  Position       : Interface       Status           : Unlocked
  Gateway-0      : 10.1.1.1
  Mask           : 255.255.255.0
  VPN instance   : --
 ------------------------------------------------------------------------------
         Start           End     Total  Used  Idle(Expired)  Conflict  Disable
 ------------------------------------------------------------------------------
       10.1.1.1       10.1.1.254  253    2       251(0)          0        0
 ------------------------------------------------------------------------------
```

----End

Configuration File

Configuration file of the AP

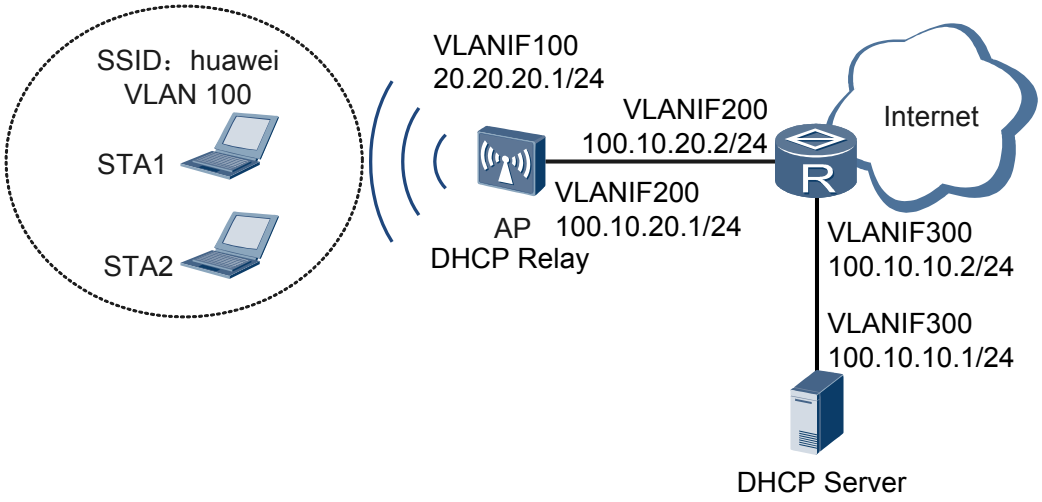
```
#
 sysname AP
#
 vlan batch 100
#
dhcp enable
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 dhcp server lease day 5 hour 0 minute 0
#
return
```

3.8.7.3 Example for Configuring a DHCP Relay Agent

Networking Requirements

As shown in **Figure 3-50**, an enterprise provides the WLAN service for employees. The enterprise has multiple offices, which are distributed in different office buildings. Wireless users in different buildings belong to different VLANs. The enterprise expects to use the same DHCP server to allocate IP addresses to all users. Office A is located on the network segment 20.20.20.0/24 but the DHCP server is on the network segment 100.10.10.0/24.

Figure 3-50 Networking diagram for configuring a DHCP relay agent



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the DHCP relay function on the AP so that the AP can forward DHCP packets from a different network segment and DHCP clients can obtain IP addresses from the DHCP server.
2. Configure a global address pool 20.20.20.0/24 on the DHCP server so that the DHCP server can assign IP addresses to clients from a different network segment.

Procedure

Step 1 Configure the DHCP relay function on the AP.

1. Create a DHCP server group and add a DHCP server to the group.

   # Create a DHCP server group.

   ```
   <Huawei> system-view
   [Huawei] sysname AP
   [AP] dhcp server group dhcpgroup1
   ```

   # Add a DHCP server to the DHCP server group.

   ```
   [AP-dhcp-server-group-dhcpgroup1] dhcp-server 100.10.10.1
   [AP-dhcp-server-group-dhcpgroup1] quit
   ```

2. Enable the global DHCP function and the DHCP relay function on the interface.

   ```
   [AP] dhcp enable
   [AP] vlan batch 100
   [AP] interface vlanif 100
   [AP-Vlanif100] ip address 20.20.20.1 24
   [AP-Vlanif100] dhcp select relay
   [AP-Vlanif100] dhcp relay server-select dhcpgroup1
   [AP-Vlanif100] quit
   ```

Step 2 Configure a default route on the AP.

```
[AP] interface vlanif 200
[AP-Vlanif200] ip address 100.10.20.1 24
```

```
[AP-Vlanif200] quit
[AP] ip route-static 0.0.0.0 0.0.0.0 100.10.20.2
```

Step 3 Configure a DHCP server.

Configure the global address pool 20.20.20.0/24 on the DHCP server and configure the egress gateway address as 20.20.20.1. Then, configure a default route with the next hop address 100.10.10.2/24. The configuration procedure varies according to devices. For details, see corresponding manuals.

Step 4 Verify the configuration.

Run the **display dhcp relay interface vlanif 100** command on the AP to check the DHCP relay configuration on the interface.

```
[AP] display dhcp relay interface vlanif 100
 DHCP relay agent running information of interface Vlanif100 :
 Server group name : dhcpgroup1
 Gateway address in use : 20.20.20.1
```

----End

Configuration File

Configuration file of the AP

```
#
 sysname AP
#
 vlan batch 100
#
 dhcp enable
#
 dhcp server group dhcpgroup1
  dhcp-server 100.10.10.1 0
#
 interface Vlanif100
 ip address 20.20.20.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select dhcpgroup1
#
 interface Vlanif200
 ip address 100.10.20.1 255.255.255.0
#
 ip route-static 0.0.0.0 0.0.0.0 100.10.20.2
#
return
```

3.8.8 Common Configuration Errors

This section provides DHCP troubleshooting procedures.

3.8.8.1 DHCP Client Cannot Obtain IP Addresses When access point Functions as the DHCP Server

Fault Description

When the access point functions as the DHCP server, the DHCP client cannot obtain IP addresses.

Procedure

Step 1 Run the **display current-configuration | include dhcp enable** command to check whether DHCP is enabled. By default, DHCP is disabled.

- If no DHCP information is displayed, DHCP is disabled. Run the **dhcp enable** command to enable DHCP.
- If **dhcp enable** is displayed, DHCP is enabled. Go to step 2.

Step 2 In the access point interface view, run the **display this** command to check whether the DHCP address assignment mode is set.

Command Output	Description	Follow-up Operation
dhcp select global	The DHCP server has assigned IP addresses to clients from the global address pool.	Go to step 3.
dhcp select interface	The DHCP server has assigned IP addresses to clients from the interface address pool.	Go to step 4.
The preceding information is not displayed.	The DHCP address assignment mode is not set on the VLANIF interface.	Run the **dhcp select global** or **dhcp select interface** command to set the DHCP address assignment mode on the interface.

Step 3 Run the **display ip pool** command to check whether the global address pool has been created.

- If the global address pool has not been created, run the **ip pool** *ip-pool-name* and **network** *ip-address* [**mask** { *mask* | *mask-length* }] commands to create a global address pool and set the range of IP addresses that can be dynamically assigned.
- If the global address pool has been created, obtain the value of *ip-pool-name*. Then run the **display ip pool name** *ip-pool-name* command to check whether the IP addresses in the global address pool are on the same network segment with the IP address on the interface.
  - If the client and server are located on the same network segment and no relay agent is deployed:
    - If IP addresses in the global address pool and the VLANIF interface IP address are located on different network segments, run the **ip address** *ip-address* { *mask* | *mask-length* } [**sub**] command to change the VLANIF interface IP address to be on the same network segment as IP addresses in the global address pool.
    - If IP addresses in the global address pool and the access point interface IP address are located on the same network segment, go to step 4.
  - If the client and server are located on different network segments and a relay agent is deployed:
    - If IP addresses in the global address pool and the relay agent IP address are located on different network segments, run the **ip address** *ip-address* { *mask* | *mask-length* }

[**sub**] command to change the IP address to be on the same network segment as IP addresses in the global address pool.

- If IP addresses in the global address pool and the relay agent interface IP address are located on the same network segment, go to step 4.

Step 4 Run the **display ip pool** [{ **interface** *interface-pool-name* | **name** *ip-pool-name* } [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]] command to check the usage of IP addresses in the global or interface address pool. If the value of **Idle (Expired)** is 0, IP addresses in the address pool have been used up.

- If the server assigns IP addresses to clients from the global address pool on the interface, re-create a global address pool where the network segment can be connected to the previous network segment but cannot overlap with the previous network segment.
- If the DHCP server allocates IP addresses to clients from the interface address pool, you can reduce the mask length of IP address so that more IP addresses can be allocated.

----End

3.8.8.2 DHCP Client Cannot Obtain IP Addresses When access point Functions as the DHCP Relay Agent

Fault Description

When the access point functions as the DHCP relay agent, the DHCP client cannot obtain IP addresses.

Procedure

Step 1 Run the **display current-configuration** | **include dhcp enable** command to check whether DHCP is enabled. By default, DHCP is disabled.

- If no DHCP information is displayed, DHCP is disabled. Run the **dhcp enable** command to enable DHCP.
- If **dhcp enable** is displayed, DHCP is enabled.

Step 2 In the access point interface view, run the **display this** command to check whether the DHCP relay function is enabled.

- If **dhcp select relay** is displayed, the DHCP relay function is enabled. Go to step 3.
- If no information is displayed, the DHCP relay function is disabled. Then run the **dhcp select relay** command to enable the DHCP relay function.

Step 3 In the access point interface view, run the **display this** command to check whether the DHCP server is configured on the DHCP relay agent.

- If **dhcp relay server-ip** *ip-address* is displayed, the DHCP server IP address is configured on the DHCP relay agent.
- If **dhcp relay server-select** *group-name* is displayed, the interface on the DHCP relay agent is bound to a DHCP server group. Go to step 4.
- If no information is displayed, the DHCP server IP address is not configured on the DHCP relay agent. Configure the DHCP server using either of the following methods:

- Run the **dhcp relay server-ip** *ip-address* command to configure the DHCP server IP address on the DHCP relay agent.
- Run the **dhcp-server** command to add DHCP servers to the DHCP server group and run the **dhcp relay server-select** *group-name* command to bind the VLANIF interface to a DHCP server group.

Step 4 Run the **display dhcp server group** *group-name* command to check whether DHCP servers are configured in the DHCP server group.

- If the **Server-IP** field is displayed, DHCP servers are configured in the DHCP server group.
- If the **Server-IP** field is not displayed, DHCP servers are not configured in the DHCP server group. Then run the **dhcp-server** command to add DHCP servers to the DHCP server group.

----End

3.8.9 References

This section lists references of DHCP.

The following table lists the references of this document.

Document	Description	Remarks
RFC951	BOOTSTRAP PROTOCOL (BOOTP)	-
RFC1533	DHCP Options and BOOTP Vendor Extensions	-
RFC1534	Interoperation Between DHCP and BOOTP	-
RFC2131	Dynamic Host Configuration Protocol	-
RFC2132	DHCP Options and BOOTP Vendor Extensions	-
RFC3046	DHCP Relay Agent Information Option	-
RFC5417	Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option	-

3.9 DNS Configuration

This chapter describes the principles, basic functions and configuration procedures of DNS on the access point, and provides configuration examples.

3.9.1 DNS Overview

This section describes the definition and purpose of DNS.

Definition

Domain Name System (DNS) is a distributed database used in TCP and IP applications and completes resolution between IP addresses and domain names.

Purpose

Each host on the network is identified by an IP address. To access a host, a user must obtain the host IP address first. It is difficult for users to remember IP addresses of hosts. Therefore, host names in the format of strings are designed. Each host name maps an IP address. In this way, users can use the simple and meaningful domain names instead of the complicated IP addresses to access hosts.

3.9.2 Principles

This section describes the implementation of DNS.

3.9.2.1 Working Principle of DNS

Domain name resolution is classified into dynamic resolution and static resolution that complement each other. During domain name resolution, static resolution is preferentially used. If static resolution fails, dynamic resolution is used. Dynamic DNS resolution takes a period of time, and the cooperation of the DNS server is required. To improve the domain name resolution efficiency, you are advised to add commonly used domain names to a static domain name resolution table.

Static DNS

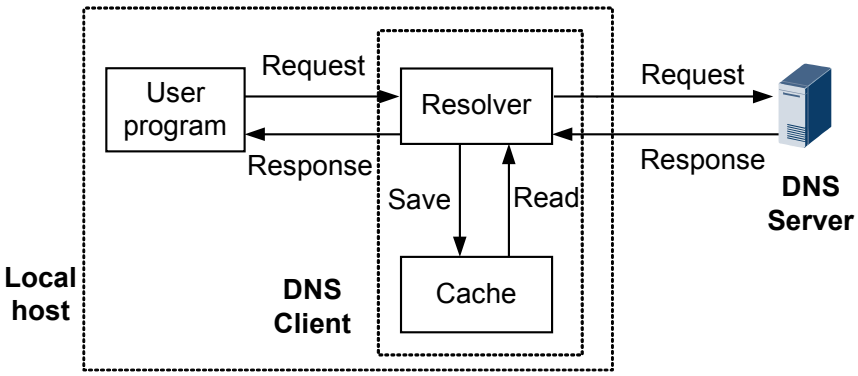
A static domain name resolution table is manually set up, describing the mappings between domain names and IP addresses. Some common domain names are added to the table. To obtain the IP address by resolving a domain name,domain names are resolved based on the static domain name resolution table. In this manner, the efficiency of domain name resolution is improved.

Dynamic DNS

User programs, such as ping and tracert, access the DNS server using the resolver of the DNS client.

Figure 3-51 shows the relationship between user programs, the resolver, the DNS server, and the cache on the resolver.

Figure 3-51 Dynamic DNS



The DNS client, consisting of the resolver and the cache, is used to accept and respond to the DNS queries from user programs. Generally, user programs(ping,Tracert), the cache, and the resolver are on the same host; whereas the DNS server is on another host.

Working Process of the Dynamic DNS

1. When a user accesses some applications by domain name, the user program sends a request to the resolver on the DNS client.
2. After receiving the request, the resolver searches the local domain name cache.
   - If the domain name matches an entry in the local cache, the resolver sends the corresponding IP address to the user program.
   - If the domain name matches no entry in the local cache, the resolver sends a query message to the DNS server.
3. When receiving the query message, the DNS server first checks whether the domain name to be resolved is in an authorized sub-domain. Then, the DNS server sends a response packet according to the check result.
   - If the domain name is in an authorized sub-domain, the DNS server searches for the corresponding IP address in the local database.
   - If the domain name is out of authorized sub-domains, the DNS server sends a query message to a higher-level DNS server. This process continues until the DNS server finds the corresponding IP address or detects that the corresponding IP address of the domain name does not exist. Then the DNS server returns a result to the DNS client.
4. After receiving the response packet from the DNS server, the DNS client sends the resolution result to the user program.

   Mappings between domain names and IP addresses are stored in the dynamic domain name cache. When resolving a domain name that is stored in the cache, the DNS client obtains the corresponding IP address from the cache directly and does not send a query message to the DNS server. Mappings stored in the cache will be deleted when the aging time expires to ensure that the latest mappings can be obtained from the DNS server. The aging time is set by the DNS server. The DNS client obtains the aging time from protocol packets.

Domain Name Suffix List

Dynamic domain name resolution supports the domain name suffix list. Users can preset domain name suffixes. Users only need to enter partial content of a domain name, and the system adds a suffix to the domain name for resolution. For example, a user has set the domain name suffix com in the suffix list. To visit huawei.com, the user only needs to enter **huawei**. The system adds the suffix com to the domain name.

When the domain name suffix list is used, the resolution modes vary according to domain names entered by users.

- If a user enters a domain name without a dot (.), for example, **huawei**, the system identifies it as a host name and adds a suffix to the domain name for resolution. If the resolution fails, the system resolves the entered domain name.

- If a user enters a domain name with a dot (.), for example, **www.huawei** or **huawei.com.**, the system resolves the domain name. If the resolution fails, the system adds a suffix to the domain name for resolution.

Query Type

Class-A query is a common type of query, which is used to obtain the IP address corresponding to a specified domain name. For example, when you ping or tracert a domain name, the ping or tracert, as a user program, sends a query to the DNS client for the IP address corresponding to the domain name. If the corresponding IP address does not exist on the DNS client, the DNS client sends a Class-A query to the DNS server to obtain the corresponding IP address.

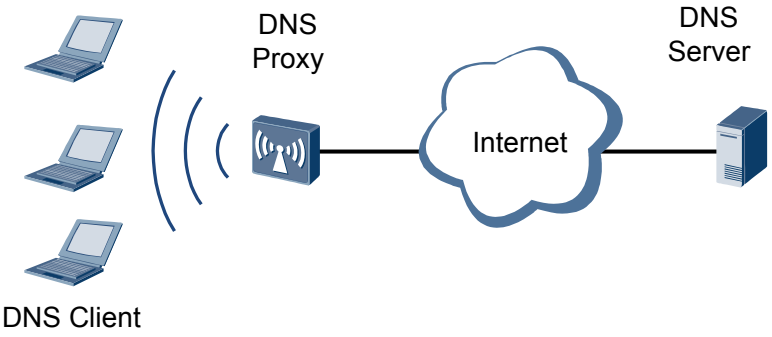
3.9.2.2 Working Principle of DNS Proxy

DNS proxy is used to forward DNS request and reply packets between the DNS client and DNS server. The DNS client sends DNS request packets to the DNS proxy. The DNS proxy forwards request packets to the DNS server and sends reply packets to the DNS client. After DNS proxy is enabled, if the IP address of the DNS server changes, you only need to change the configuration on the DNS proxy.

The DNS proxy searches for DNS entries saved in the local domain name cache after receiving DNS query messages from DNS clients. If requested DNS entries are not saved in the cache, DNS query messages are forwarded to the DNS server.

Figure 3-52 shows the typical networking of DNS proxy.

Figure 3-52 Typical networking of DNS proxy



The working process of DNS proxy is as follows:

1. The DNS client sends a request packet to the DNS proxy. The DNS proxy IP address is the destination address of the request packet.
2. After receiving the request packet, the DNS proxy searches for DNS entries saved in the local domain name resolution tables. If mapping information exists, the DNS proxy sends a reply packet carrying the resolution result to the DNS client.
3. If no mapping information exists, the DNS proxy sends the request packet to the DNS server for resolution.

4. After receiving the reply packet from the DNS server, the DNS proxy records the resolution result and forwards the reply packet to the DNS client.

Only when the IP address of the DNS server and the route to the DNS server exist on the DNS proxy, the DNS proxy sends domain name resolution requests to the DNS server. Otherwise, the DNS proxy neither sends any domain name resolution request to the DNS server nor replies any request from the DNS client.

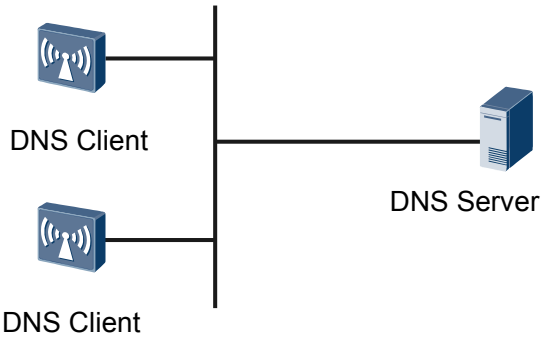
3.9.3 Applications

This section describes the applicable scenario of DNS.

3.9.3.1 DNS Client Application

Figure 3-53 shows typical networking of a DNS client.

Figure 3-53 Typical networking of a DNS client

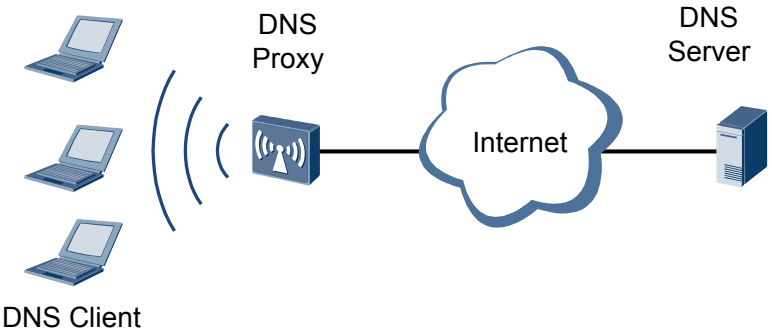


As shown in **Figure 3-53**, the device functions as a DNS client and can dynamically obtain the corresponding IP address of a domain name from a DNS server. This facilitates user communication.

3.9.3.2 DNS Proxy Application

Figure 3-54 shows the typical networking of DNS proxy.

Figure 3-54 Typical networking of DNS proxy



The device functions as an egress router and is configured with DNS proxy in an enterprise. The device can forward DNS request and reply packets between DNS clients in the enterprise and DNS servers out of the enterprise. When the IP address of a DNS server changes, you only need to change the configuration on the DNS proxy,this will be beneficial to Network management.

3.9.4 Configuring DNS

This section describes the configuration methods of DNS.

3.9.4.1 Configuring the DNS Client

This section describes how to configure the access point as a DNS client to allow users to use domain names to access other devices.

Pre-configuration Tasks

Before configuring a DNS client, complete the following tasks:

- Configuring link layer protocol parameters for interfaces to ensure that the link layer protocol status on the interfaces is Up
- Configuring a route between the access point and the DNS server

3.9.4.1.1 Configuring the Static DNS

Context

A static domain name resolution table is manually set up, describing the mappings between domain names and IP addresses. Some common domain names are added to the table. Static domain name resolution can be performed based on the static domain name resolution table. To obtain the IP address by resolving a domain name, the client searches the static domain name resolution table for the specified domain name. In this manner, the efficiency of domain name resolution is improved.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip host host-name ip-address
```

Static DNS entries are configured.

By default, no static DNS entries are configured.

----End

Follow-up Procedure

Each host name can be mapped to only one IP address. When multiple IP addresses are mapped to a host name, only the latest configuration takes effect. If multiple host names need to be resolved, repeat step 2.

3.9.4.1.2 Configuring the Dynamic DNS

Context

To implement dynamic DNS, you need to enable dynamic DNS resolution, configure a DNS server, and configure a source IP address for the local device and a domain name suffix. If the local device uses an IP address allocated by the DHCP server and the information delivered by the DHCP server to the local device contains the DNS server IP address and the domain name suffix list, you only need to enable dynamic DNS resolution.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dns resolve
```

Dynamic domain name resolution is enabled.

By default, dynamic DNS resolution is disabled.

Step 3 Run:

```
dns server ip-address
```

The IP address of the DNS server is configured.

By default, no IP address of the DNS server is configured.

A maximum of six DNS server IP addresses can be configured on the device.

Step 4 (Optional) Run:

```
dns server source-ip ip-address
```

The source IP address is configured for the local device to function as the DNS client to send and receive DNS packets.

By default, no source IP address is configured for the device.

The local device uses the specified IP address to communicate with the DNS server. This ensures communication security.

Step 5 (Optional) Run:

```
dns-server-select-algorithm { fixed | auto }
```

The algorithm for selecting a destination DNS server is configured.

By default, the device uses the auto algorithm to select the DNS server.

Step 6 (Optional) Run:

```
dns forward retry-number number
```

The number of times for retransmitting Query packets to the destination DNS server is set.

By default, the device retransmits Query packets to the destination DNS server twice.

Step 7 (Optional) Run:

```
dns forward retry-timeout time
```

The retransmission timeout period that the device sends Query packets to the destination DNS server is set.

By default, the retransmission timeout period is 3 seconds.

Step 8 (Optional) Run:

```
dns domain domain-name
```

A domain name suffix is configured.

By default, no domain name suffix is configured on a DNS client.

----End

Follow-up Procedure

The system supports a maximum of six DNS servers, one specified source address, and ten domain name suffixes. If multiple DNS servers are required, repeat step 3. If multiple domain name suffixes are required, repeat step 8.

3.9.4.1.3 Checking the Configuration

Procedure

- Run the **display dns configuration** command to display the global DNS configurations.
- Run the **display ip host** command to check static DNS entries.
- Run the **display dns server** [**verbose**] command to check the DNS server configuration.
- Run the **display dns domain** [**verbose**] command to check the domain name suffix configuration.

----End

3.9.4.2 Configuring DNS Proxy

The device can function as a DNS proxy to forward DNS request and reply packets and provide domain name resolution for DNS clients.

Pre-configuration Tasks

Before configuring DNS proxy, complete the following tasks:

- Configuring link layer protocol parameters for interfaces to ensure that the link layer protocol status on the interfaces is Up
- Configuring the DNS server

- Configuring routes between the device and the DNS server and between the device and the DNS client

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dns proxy enable
```

DNS Proxy is enabled.

Step 3 Choose either of the following methods to configure domain name resolution.

- Configure static domain name resolution.

  Run:

  ```
  ip host host-name ip-address
  ```

  A static DNS entry is configured.

  By default, no static DNS entry is configured.

  You can manually configure the mappings between domain names and IP addresses by configuring static DNS entries. When a DNS client requests the IP address corresponding to a domain name, the device does not forward the request to the DNS server but searches the static domain name resolution table for the IP address and returns the IP address to the DNS client.

- Configure dynamic domain name resolution.

  1. Run:

     ```
     dns resolve
     ```

     Dynamic domain name resolution is enabled.

     By default, dynamic DNS resolution is disabled.

     After dynamic domain name resolution is enabled, the DNS proxy searches the dynamic domain name resolution table after receiving a DNS request packet and checks whether the requested IP address exists. If yes, the DNS proxy returns a DNS reply packet that carries the resolution result to the DNS client. If not, the DNS proxy forwards the DNS request packet to the DNS server.

  2. Run:

     ```
     dns server ip-address
     ```

     The DNS server that the DNS Proxy connects to is configured.

     By default, no IP address is configured for the DNS server.

  3. (Optional) Run:

     ```
     dns server source-ip ip-address
     ```

     The source IP address that the device uses to exchange packets with the DNS server is configured.

     By default, no source IP address is configured for the device.

  4. (Optional) Run:

     ```
     dns-server-select-algorithm { fixed | auto }
     ```

An algorithm used by the DNS Proxy to access the destination DNS server is configured.

By default, the auto algorithm is used.

5. (Optional) Run:

   dns forward retry-number *number*

   The number of times for the DNS Proxy to retransmit query requests to the destination DNS server is set.

   By default, the number of times for the DNS Proxy to retransmit query requests to the destination DNS server is 2.

6. (Optional) Run:

   dns forward retry-timeout *time*

   The retransmission timeout period that the DNS proxy sends Query packets to the destination DNS server is set.

   By default, the retransmission timeout period is 3 seconds.

----End

Checking the Configuration

- Run the **display dns configuration** command to display the global DNS configurations.
- Run the **display ip host** command to check static DNS entries.
- Run the **display dns server** [**verbose**] command to check the DNS server configuration.

3.9.5 Maintaining DNS

Maintaining DNS includes clearing dynamic DNS entries, clearing DNS forwarding entries, and monitoring DNS running status.

3.9.5.1 Deleting Dynamic DNS Entries

Context

NOTICE

Dynamic DNS entries cannot be restored after being deleted. Exercise caution when you run the command.

Procedure

- Run the **reset dns dynamic-host** command to delete dynamic DNS entries.

----End

3.9.5.2 Deleting DNS Entries of the DNS Proxy

Context

NOTICE

DNS entries of the DNS proxy cannot be restored after being deleted. Exercise caution when you run the command.

Procedure

- Run the **reset dns forward table** [**source-ip** *ip-address*] command to delete DNS entries of the DNS proxy.

----End

3.9.5.3 Monitoring the Running Status of DNS

Context

In routine maintenance, you can run the following commands in any view to check the running status of DNS.

Procedure

- Run the **display dns forward table** [**source-ip** *ip-address*] command to check the DNS forwarding table.
- Run the **display dns dynamic-host** command to display dynamic DNS entries.

----End

3.9.6 Configuration Examples

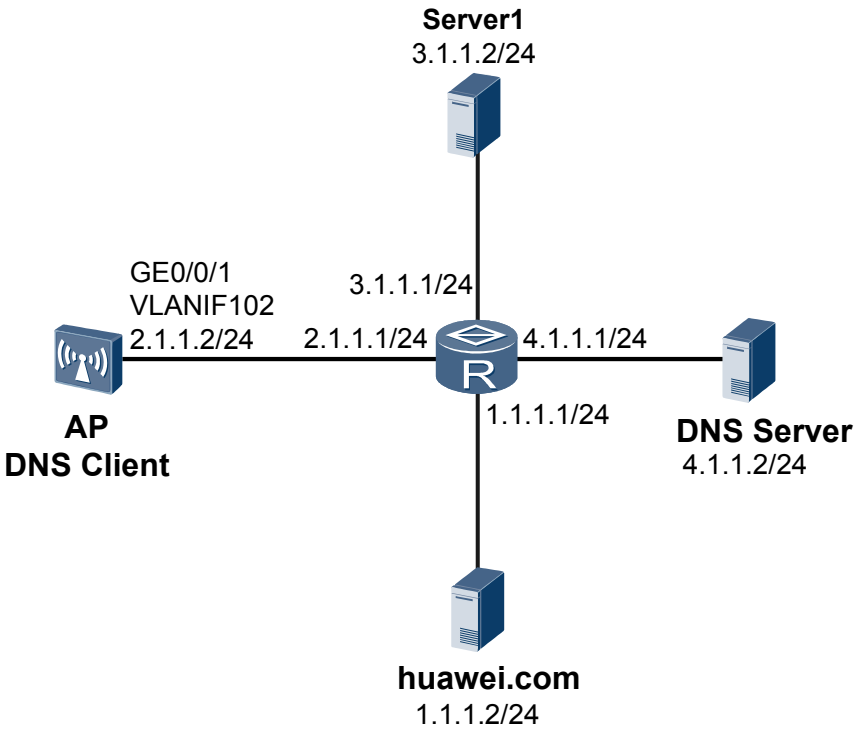
This section provides DNS configuration example, including networking requirements, configuration roadmap, and configuration procedure.

3.9.6.1 Example for Configuring the DNS Client

Networking Requirements

IP addresses are difficult to remember. Users want to access network servers using domain names. When users input part of a domain name, the DNS server is required to correctly parse the domain name so that users can access network servers. For example, when users want to access the server with domain name huawei.com, they only need to input huawei. In this example, users want to rapidly access the server with domain name Server1, requiring domain name resolution efficiency to be improved.

Figure 3-55 Networking for configuring the DNS client



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an IP address for each interface, and configure a static routing protocol to ensure that there are reachable routes between devices.
2. Configure static DNS entries on the AP to ensure that users access Server1 using a domain name.
3. Configure the dynamic DNS function on the AP to enable the AP to communicate with network servers using the dynamic DNS query mode.

Procedure

Step 1 Configure an IP address for each interface. The following uses the configuration of the AP as an example.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 102
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port hybrid pvid vlan 102
[AP-GigabitEthernet0/0/1] port hybrid untagged vlan 102
[AP-GigabitEthernet0/0/1] quit
[AP] interface vlanif 102
[AP-Vlanif102] ip address 2.1.1.2 255.255.255.0
[AP-Vlanif102] quit
```

Step 2 Configure a static route.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 2.1.1.1
```

Step 3 Configure static DNS.

```
[AP] ip host Server1 3.1.1.2
```

Step 4 Configure dynamic DNS.

```
[AP] dns resolve
[AP] dns server 4.1.1.2
[AP] dns domain com
```

Step 5 Verify the configuration.

Run the **ping Server1** command on the AP. You can see that the ping operation succeeds and the destination IP address is 3.1.1.2.

```
<AP> ping Server1
 PING Server1 (3.1.1.2): 56  data bytes, press CTRL_C to break
    Reply from 3.1.1.2: bytes=56 Sequence=1 ttl=127 time=4 ms
    Reply from 3.1.1.2: bytes=56 Sequence=2 ttl=127 time=1 ms
    Reply from 3.1.1.2: bytes=56 Sequence=3 ttl=127 time=1 ms
    Reply from 3.1.1.2: bytes=56 Sequence=4 ttl=127 time=1 ms
    Reply from 3.1.1.2: bytes=56 Sequence=5 ttl=127 time=1 ms

  --- Server1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/4 ms
```

Run the **ping huawei.com** command on the AP. You can see that the ping operation succeeds and the destination IP address is 1.1.1.2.

```
<AP> ping huawei.com
  PING huawei.com (1.1.1.2): 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.2: bytes=56 Sequence=1 ttl=127 time=6 ms
    Reply from 1.1.1.2: bytes=56 Sequence=2 ttl=127 time=4 ms
    Reply from 1.1.1.2: bytes=56 Sequence=3 ttl=127 time=4 ms
    Reply from 1.1.1.2: bytes=56 Sequence=4 ttl=127 time=4 ms
    Reply from 1.1.1.2: bytes=56 Sequence=5 ttl=127 time=4 ms

  --- huawei.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/6 ms
```

Run the **ping huawei** command on the AP. You can see that the ping operation succeeds, the corresponding domain name is huawei.com, and the destination IP address is 1.1.1.2.

```
<AP> ping huawei
  PING huawei.com (1.1.1.2): 56  data bytes, press CTRL_C to break
    Reply from 1.1.1.2: bytes=56 Sequence=1 ttl=127 time=6 ms
    Reply from 1.1.1.2: bytes=56 Sequence=2 ttl=127 time=4 ms
    Reply from 1.1.1.2: bytes=56 Sequence=3 ttl=127 time=4 ms
    Reply from 1.1.1.2: bytes=56 Sequence=4 ttl=127 time=4 ms
    Reply from 1.1.1.2: bytes=56 Sequence=5 ttl=127 time=4 ms

  --- huawei.com ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 4/4/6 ms
```

Run the **display ip host** command on the AP. You can view mappings between host names and IP addresses in static DNS entries.

```
<AP> display ip host
Host                 Age         Flags  Address
Server1              0           static 3.1.1.2
```

Run the **display dns dynamic-host** command on the AP. You can view information about dynamic DNS entries in the domain name cache.

```
<AP> display dns dynamic-host
Host                                    TTL   Type   Address(es)
huawei.com                              114   IP     1.1.1.2
```

----End

Configuration Files

- Configuration file of the AP

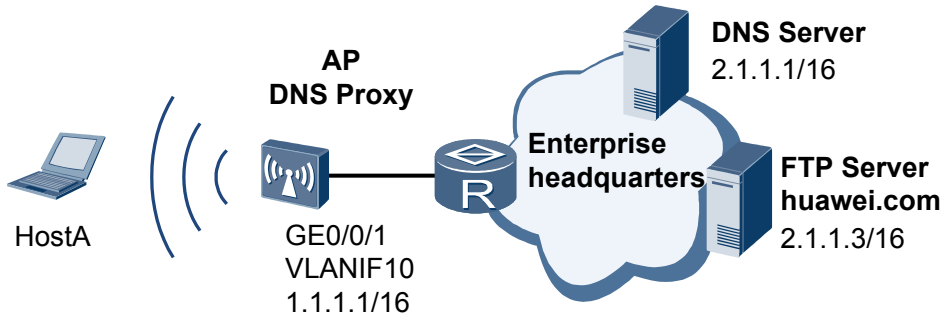
```
#
 sysname AP
#
 ip host Server1 3.1.1.2
#
 dns resolve
 dns server 4.1.1.2
 dns domain com
#
 vlan batch 102
#
interface Vlanif102
 ip address 2.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
#
ip route-static 0.0.0.0 0.0.0.0 2.1.1.1
#
return
```

3.9.6.2 Example for Configuring DNS Proxy

Networking Requirements

As shown in **Figure 3-56**, the enterprise deploys a DNS server only on the headquarters network to save costs. The route between the AP and the DNS server or between the AP and the FTP server is reachable. The mapping between the domain name (huawei.com) of the FTP server and the IP address 2.1.1.3 is recorded on the DNS server. Enterprise users on the branch network expect to access the FTP server through the DNS domain name. To facilitate maintenance, the enterprise requires that users be unaware of the DNS server address change.

Figure 3-56 Network diagram for configuring DNS Proxy



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure DNS Proxy on the AP to implement domain name resolution for clients.

   NOTE

   After DNS Proxy is enabled, the AP can be regarded as the DNS server of HostA. You need to configure the AP's IP address as the IP address of the DNS server on HostA and configure the IP address (2.1.1.1) of the DNS server on the headquarters network on the AP. In this way, when the DNS server address changes, you only need to modify the configurations on the AP, which is not detected by the users.

Procedure

Step 1 Configure an IP address for the interface.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 10
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[AP-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[AP-GigabitEthernet0/0/1] quit
[AP] interface vlanif 10
[AP-Vlanif10] ip address 1.1.1.1 255.255.0.0
[AP-Vlanif10] quit
```

Step 2 Configure DNS Proxy.

```
[AP] dns proxy enable
[AP] dns resolve
[AP] dns server 2.1.1.1
```

Step 3 Configure the default route from the DNS proxy to the DNS server.

Assume that the IP address of the next hop from the DNS proxy to the DNS server is 1.1.1.2/16.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
```

Step 4 Specify the IP address of the DNS server on HostA as 1.1.1.1.

Step 5 Verify the configuration.

Run the **display current-configuration** command on the AP to check DNS Proxy configurations.

```
<AP> display current-configuration | include dns
 dns resolve
 dns server 2.1.1.1
 dns proxy enable
```

Run the **ping huawei.com** command on HostA. The ping operation succeeds.

```
C:\Documents and Settings\HostA>ping huawei.com
  PING huawei.com [2.1.1.3] with 32 bytes of data:
    Reply from 2.1.1.3: bytes=32 time=16ms TTL=255
    Reply from 2.1.1.3: bytes=32 time<1ms TTL=255
    Reply from 2.1.1.3: bytes=32 time<1ms TTL=255
    Reply from 2.1.1.3: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.168.1:
    Packets: Sent = 4, Received = 4, Lost = 0(0% loss),
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 16ms, Average = 4ms
```

----End

Configuration Files

Configuration file of the AP

```
#
 sysname AP
#
interface Vlanif10
 ip address 1.1.1.1 255.255.0.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
 dns resolve
 dns server 2.1.1.1
 dns proxy enable
#
 ip route-static 0.0.0.0 0.0.0.0 1.1.1.2
#
return
```

3.9.7 Common Configuration Errors

This section describes common faults caused by incorrect DNS configurations and provides the troubleshooting procedure.

3.9.7.1 Dynamic Domain Name Resolution Cannot Be Implemented on a DNS Client

Fault Description

The access point functions as a DNS client that is configured with dynamic domain name resolution but cannot resolve domain names to IP addresses correctly.

Procedure

Step 1 Run the **display dns dynamic-host** command check whether the specified domain name exists in the dynamic domain name cache.

- If not, check whether the DNS client communicates with the DNS server properly, the DNS server runs properly, and dynamic domain name resolution is enabled.
- If so, but the IP address is incorrect, go to step 2.

Step 2 Run the **display dns server** command to verify that the IP address of the DNS server is correct on the DNS client.

If the DNS server IP address is incorrect, run the **undo dns server** *ip-address* command to delete the configured DNS server IP address, and run the **dns server** *ip-address* command to reconfigure a correct IP address for the DNS server.

----End

3.9.8 References

This section lists references of DNS.

The following table lists the references of this document:

Document	Description	Remarks
RFC1034	DOMAIN NAMES - CONCEPTS AND FACILITIES	-
RFC1035	DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION	-

3.10 IP Performance Configuration

You can optimize IP performance by adjusting parameters on the network.

3.10.1 IP Performance Overview

Parameters on certain networks need to be modified to optimize network performance.

A large number of packets need to be forwarded on the network, which may cause network congestion and degrade network performance.IP performance optimization can solve the problem. You can adjust parameters or forwarding modes for IP packets to achieve optimal network performance.

3.10.2 Default Configuration

This section provides the default IP performance configuration.

Table 3-27 describes the default configuration of IP performance.

Table 3-27 Default IP performance configuration

Parameter	Default Configuration
Source IP address verification	Disabled
IP packet fragmentation on outbound interface	Disabled
Fast ICMP reply function	Enabled
Discarding ICMP packets whose TTL values are 1	Disabled
Discarding ICMP packets that carry options	Disabled

Parameter	Default Configuration
Discarding ICMP destination unreachable packets	Disabled
Sending ICMP port unreachable packets	Enabled
Sending ICMP redirection packets	Enabled
TCP SYN-Wait timer	75s
TCP FIN-Wait timer	675s
TCP window size	8k bytes

3.10.3 Optimizing IP Performance

This section describes how to optimize IP performance. You can set IP performance parameters to achieve best network performance.

Prerequisite

Before optimizing IP performance, complete the following task:

- Configuring IP addresses for interfaces

3.10.3.1 Configuring Source IP Addresses Verification

Context

Configuring source IP address verification enables an interface to check validity of source IP addresses of received packets. Packets with invalid addresses are discarded. The interface only check validity of source IP addresses of the packets that are forwarded to the CPU and does not check validity of source IP addresses of the packets that will be directly forwarded according to the FIB table.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed. The interface can be a VLANIF or loopback interface.

NOTE

If the interface is a VLANIF interface, a VLAN must be created.

Step 3 Run:

```
ip verify source-address
```

Source IP address verification is configured.

The device only verify the source IP addresses of packets forwarded from an interface to the CPU.

By default, an interface does not check validity of source IP addresses of received packets.

----End

3.10.3.2 Configuring an Outbound Interface to Fragment IP Packets

Context

If the size of IP packets exceeds the MTU, oversized packets will be discarded. After IP packet fragmentation is enabled, the system sets the DF field of an IP packet to 0 and fragments the IP packet to ensure that all packets are forwarded.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed. The interface can be a VLANIF or loopback interface.

NOTE

If the interface is a VLANIF interface, a VLAN must be created.

The function that clears the DF field is valid for outgoing packets; therefore, this function must be configured on the outbound interface.

Step 3 Run:

```
clear ip df
```

The function that clears the DF field is configured to enable IP packet fragmentation on an outbound interface.

By default, an outbound interface does not fragment IP packets.

----End

3.10.3.3 Configuring ICMP properties

Context

By default, an interface is enabled to send ICMP redirection packets.

NOTICE

If an interface is not enabled to send ICMP redirection packets, the Access Point does not send ICMP redirection packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
icmp-reply fast
```

The fast ICMP reply function is enabled.

By default, the fast ICMP reply function is enabled on the device.

NOTE

After the fast ICMP reply function is enabled on access point, access point respond to ICMP Echo packets quickly in any of the following situations:

- access point do not have the ARP entry of the device that initiates the ping and cannot learn the ARP entry of the device.
- access point do not have route entries to the device that initiates the ping.
- access point receive ICMP Echo packets with incorrect checksum.

Step 3 Run:

```
icmp ttl-exceeded drop
```

The device is configured to discard the ICMP packets whose TTL values are 1.

By default, the function of discarding ICMP packets with TTL values 1 is disabled.

Step 4 Run:

```
icmp with-options drop
```

The device is configured to discard the ICMP packets that carry options.

By default, the function of discarding ICMP packets that carry options is disabled.

Step 5 Run:

```
icmp unreachable drop
```

The function of discarding ICMP destination unreachable packets is enabled.

By default, the function of discarding ICMP destination unreachable packets is disabled.

Step 6 Run:

```
icmp port-unreachable send
```

The function of sending ICMP port unreachable packets is enabled.

By default, the function of sending ICMP port unreachable packets is enabled.

Step 7 Run:

interface *interface-type interface-number*

The interface view is displayed.

Step 8 Run:

icmp host-unreachable send

The function of sending ICMP host unreachable packets is enabled.

By default, the function of sending ICMP host unreachable packets is enabled.

Step 9 Run:

icmp redirect send

The interface is enabled to send ICMP redirection packets.

By default, the function of sending ICMP redirection packets is enabled..

----End

3.10.3.4 Controlling IP packets with Source Route Options

Context

By controlling IP packets with source route options, the device can prevent malicious attackers from detecting network topologies by using source route options. This improves network security.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

interface *interface-type interface-number*

The interface view is displayed.

Step 3 Run:

discard srr

The interface is configured to discard IP packets with source route options.

By default, the function of discarding IP packets with source-route options is not enabled. That is, a device processes the IP packets with source-route options.

----End

3.10.3.5 Configuring TCP Properties

Context

When a TCP connection is set up between access point and other devices, TCP properties need to be configured.

The following TCP properties can be configured on access point:

- SYN-Wait timer: When SYN packets are sent, the SYN-Wait timer is started. If no response packet is received after the SYN-Wait timer expires, the TCP connection is closed.
- FIN-Wait timer: When the TCP connection status changes from FIN_WAIT_1 to FIN_WAIT_2, the FIN-Wait timer is started. If no response packet is received after the FIN-Wait timer expires, the TCP connection is closed.
- Receive/send buffer size of connection-oriented socket *window-size*.

If you configure TCP properties in the system view for multiple times, only the last configuration takes effect.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
tcp timer syn-timeout interval
```

The SYN-Wait timer of TCP connections is configured.

The value of the TCP SYN-Wait timer is an integer that ranges from 2 to 600, in seconds. The default value is 75.

Step 3 Run:

```
tcp timer fin-timeout interval
```

The FIN-WAIT timer of TCP connections is configured.

The value of the TCP FIN-Wait timer is an integer that ranges from 76 to 3600, in seconds. The default value is 675.

Step 4 Run:

```
tcp window window-size
```

The socket receive/send buffer size is configured.

The value of *window-size* ranges from 1k bytes to 32k bytes. The default value is 8k bytes.

----End

3.10.3.6 Checking the Configuration

Procedure

- Run the **display tcp status** [[**task-id** *task-id*] [**socket-id** *socket-id*] | [**local-ip** *ip-address*] [**local-port** *local-port-number*] [**remote-ip** *ip-address*] [**remote-port** *remote-port-number*]] command to check the TCP connection status.
- Run the **display tcp statistics** command to view the TCP traffic statistics.
- Run the **display udp statistics** command to view the UDP traffic statistics.
- Run the **display ip statistics** command to view the IP traffic statistics.

- Run the **display ip socket** [**monitor**] [**task-id** *task-id* **socket-id** *socket-id* | **socket-type** *socket-type*] command to view information about the created IPv4 socket.
- Run the **display icmp statistics** command to view the ICMP traffic statistics.

----End

3.10.4 Maintaining IP Performance

This section describes how to clear IP performance statistics to maintain IP performance.

3.10.4.1 Clearing IP Performance Statistics

Context

NOTICE

The IP/TCP/UDP traffic statistics cannot be restored after being cleared. Therefore, confirm your operation before clearing the IP performance statistics.

Procedure

- Run the **reset ip statistics** [**interface** *interface-type interface-number*] command in the user view to clear IP statistics.
- Run the **reset ip socket monitor** [**task-id** *task-id* **socket-id** *socket-id*] command in the user view to clear information in a socket monitor.
- Run the **reset rawip statistics** command in the user view to clear statistics about RawIP packets.
- Run the **reset tcp statistics** command in the user view to clear TCP statistics.
- Run the **reset udp statistics** command in the user view to clear UDP statistics.

----End

3.10.5 Configuration Examples

This section provides IP performance configurations including the networking requirements, networking diagram, configuration roadmap, and configuration procedures.

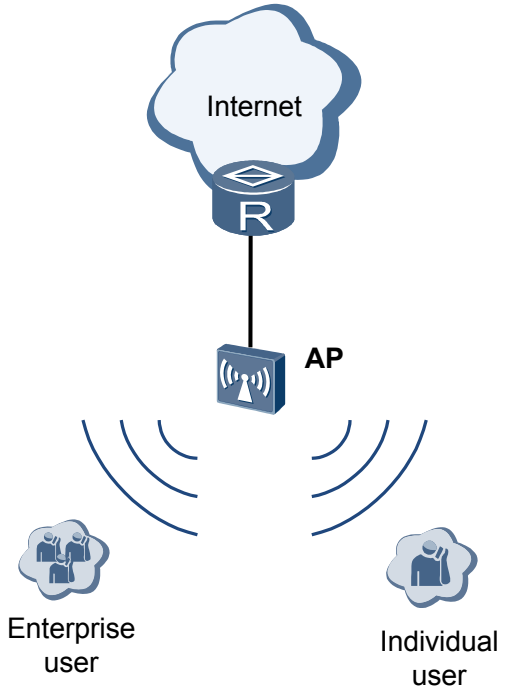
3.10.5.1 Example for Optimizing System Performance by Discarding Certain ICMP Packets

Networking Requirements

The AP in **Figure 3-57** functions as the aggregation device. Enterprise users and individual users are attached to the AP and the AP is connected to the Internet through a router. When a large amount of information is exchanged on the network or the network is attacked, lots of ICMP

packets are forwarded and the network performance is degraded. In this case, some ICMP packets are required to be discarded to reduce the burden on the AP.

Figure 3-57 Networking diagram for configuring ICMP security function



Configuration Roadmap

The configuration roadmap is as follows:

Configure the function of discarding ICMP packets whose TTL value is 1, ICMP packets that carry options, and ICMP destination unreachable packets to reduce the burden of the device in processing a large number of ICMP packets.

Procedure

Step 1 Configure the device to discard certain ICMP packets.

Configure the device to discard ICMP packets whose TTL value is 1.

```
<Huawei> system-view
[Huawei] icmp ttl-exceeded drop
```

Configure the device to discard ICMP packets that carry options.

```
[Huawei] icmp with-options drop
```

Configure the device to discard ICMP packets whose destination addresses are unreachable.

```
[Huawei] icmp unreachable drop
```

Step 2 Verify the configuration.

Run the **display this** command in the system view to view the ICMP security configurations.

```
[Huawei] display this
#
 icmp unreachable drop
 icmp ttl-exceeded drop
 icmp with-options drop
#
```

----End

Configuration Files

Configuration file of the AP

```
#
 icmp unreachable drop
 icmp ttl-exceeded drop
 icmp with-options drop
#
return
```

3.11 Static Route Configuration

Static routes apply to simple networks. Proper static routes can improve network performance and ensure bandwidth for important applications.

3.11.1 Introduction to Static Routes

This section describes the definition and purpose of Static Routes.

Definition

Static routes are routes that are manually configured by the administrator.

Purpose

Static routes provide different functions on different networks.

- On a simple network, only static routes are required to ensure normal running of the network.
- On a complex network, static routes improve the network performance and ensure the required bandwidth for important applications.

3.11.2 Principles

This section describes the implementation of Static Routes.

3.11.2.1 Basics of Static Routes

A router forwards data packets based on routing entries containing route information. The routing entries can be manually configured or calculated by dynamic routing protocols. Static routes refer to the routes that are manually added to the routing table.

Static routes use less bandwidth than dynamic routes. No CPU resource is used for calculating or analyzing routing update. When a fault occurs on the network or the topology changes, static

routes cannot automatically change and must be changed manually. The configuration of a static route includes destination IP address and mask, outbound interface and next-hop address, and preference.

Destination Address and Mask

The destination IPv4 address is expressed in dotted decimal notation. The mask can be expressed either in dotted decimal notation or by the mask length, that is, the number of consecutive 1s in the mask. When the destination and mask are set to all 0s, the default static route is configured. For details about the default static route, see Application of the Static Default Route.

Outbound Interface and Next-Hop IP Address

When configuring a static route, you can specify the outbound interface and the next-hop IP address based on outbound interfaces types.

- Configure the outbound interface for point-to-point (P2P) interfaces. For a P2P interface, the next-hop address is specified after the outbound interface is specified. That is, the address of the remote interface (interface on the peer device) connected to this interface is the next-hop address. For example, the protocol used to encapsulate 10GE is the Point-to-Point protocol (PPP). The remote IP address is obtained through PPP negotiation. You need specify only the outbound interface.
- Configure the next hop for Non Broadcast Multiple Access (NBMA) interfaces. You need to configure the IP route and the mapping between IP addresses and link-layer addresses.
- Configure the next hop for broadcast interfaces (for example, Ethernet interfaces) and virtual template (VT) interfaces. The Ethernet interface is a broadcast interface, and the VT interface can be associated with several virtual access (VA) interfaces. If the Ethernet interface or the VT interface is specified as the outbound interface, multiple next hops exist and the system cannot decide which next hop is to be used. Therefore, this configuration is not recommended.

Static Route Preference

Different static routes can be configured with different preferences. A smaller preference value indicates a higher priority of static routes. If you specify the same preference for the static routes to the same destination, you can implement load balancing among these routes. If you specify different preferences for the static routes, you can implement route backup among the routes. For details, see Load Balancing and Route Backup.

3.11.2.2 Permanent Advertisement of Static Routes

Permanent advertisement of static routes provides a low-cost and simple link detection mechanism and improves compatibility between Huawei devices and non-Huawei devices. If service traffic needs to be forwarded along a specified path, you can ping the destination addresses of static routes to detect the link connectivity.

Link connectivity determines the stability and availability of a network. Therefore, link detection plays an important role in network maintenance. BFD, as a link detection mechanism, is inapplicable to certain scenarios. For example, a simpler and more natural method is required for link detection between different ISPs.

After permanent advertisement of static routes is configured, the static routes that cannot be advertised are still preferred and are added to the routing table in the following cases:

- If an outbound interface configured with an IP address is specified for a static route, the static route is always preferred and added to the routing table regardless of whether the outbound interface is Up or Down.
- If no outbound interface is specified for a static route, the static route is always preferred and added to the routing table regardless of whether the static route can be iterated to an outbound interface.

In this way, you can enable IP packets to be always forwarded through this static route. The permanent advertisement mechanism provides a way for you to monitor services and detect link connectivity.

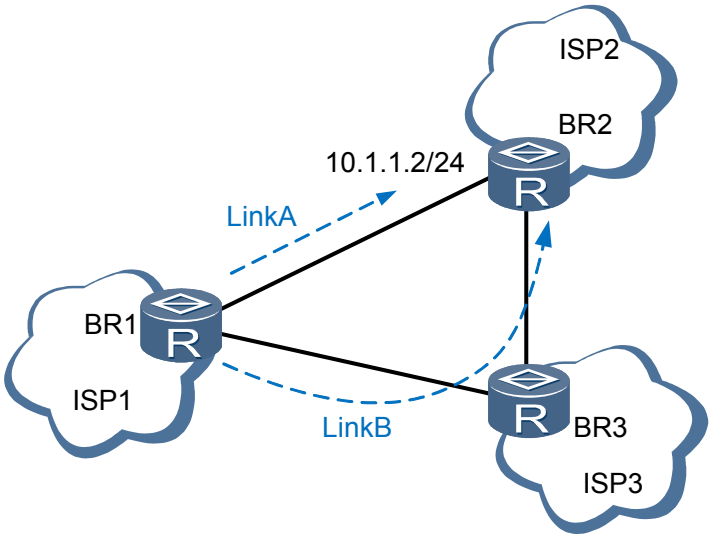
NOTICE

A device enabled with this feature always stores static routes in its IP routing table, regardless of whether the static routes are reachable. If a path is unreachable, the corresponding static route may become a blackhole route.

Applications

In **Figure 3-58**, BR1, BR2, and BR3 belong to ISP1, ISP2, and ISP3 respectively. Between BR1 and BR2 are two links, Link A and Link B. ISP1, however, requires that service traffic be forwarded to ISP2 over Link A without traveling through ISP3.

Figure 3-58 Networking for applying permanent advertisement of static routes



The External Border Gateway Protocol (EBGP) peer relationship is established between BR1 and BR2. For service monitoring, a static route destined for the BGP peer (BR2) at 10.1.1.2/24 is configured on BR1, and permanent advertisement of static routes is enabled. The interface that connects BR1 to BR2 is specified as the outbound interface of the static route. Then, the network monitoring system periodically pings 10.1.1.2 to determine the status of Link A.

If Link A works properly, ping packets are forwarded over Link A. If Link A becomes faulty, although service traffic can reach BR2 over Link B, the static route is still preferred because permanent advertisement of static routes is enabled. Therefore, ping packets are still forwarded over Link A, but packet forwarding fails. This scenario is also applicable to BGP packets. That is, a link fault causes the BGP peer relationship to be interrupted. The monitoring system detects service faults as returned in the ping result and prompts maintenance engineers to rectify the faults before services are affected.

3.11.3 Default Configuration of Static Routes

This section describes the default configuration of static routes, which can be changed according to network requirements.

Table 3-28 describes the default configuration of static routes.

Table 3-28 Default configuration of static routes

Parameter	Default Setting
Preference of static routes	60

3.11.4 Configuring Static Routes

Static routes are applicable to the networks with simple structures. Proper configuration and usage of static routes improve the network performance and meet the bandwidth requirement of important applications.

3.11.4.1 Configuring IPv4 Static Routes

On a network, you can accurately control route selection by configuring IPv4 static routes.

Pre-configuration Tasks

Before configuring IPv4 static routes, complete the following task:

- Configuring IP addresses for interfaces to ensure network-layer communication between neighbor nodes

Configuration Procedures

You can perform the following configuration tasks (excluding the task of Checking the Configuration) in any sequence as required.

3.11.4.1.1 Creating IPv4 Static Routes

Context

When creating static routes, you can specify both the outbound interface and next hop. Alternatively, you can specify only the outbound interface or next hop based on the outbound interface type.

- Specify the outbound interface for P2P interfaces.
- Specify the next hop for non broadcast multiple access (NBMA) interfaces.
- Specify the next hop for broadcast interfaces (for example, Ethernet interfaces).

If you specify the same preference for static routes to the same destination, you can implement load balancing among these routes. If you specify different preferences for static routes, you can implement route backup among the routes.

If the destination IP address and mask are set to all 0s, an IPv4 static default route is configured. By default, no IPv4 static default route is configured.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static ip-address { mask | mask-length } { nexthop-address | interface-type interface-number [ nexthop-address ] } [ preference preference | tag tag ] * [ description text ]
```

An IPv4 static route is configured.

----End

3.11.4.1.2 (Optional) Setting the Default Preference for IPv4 Static Routes

Context

The default preference of IPv4 static routes affects route selection. When an IPv4 static route is configured, the default preference is used if no preference is specified for the static route.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static default-preference preference
```

The default preference of static routes is set.

By default, the preference of static routes is 60.

NOTE

After the default preference is reconfigured, the new default preference is valid only for new IPv4 static routes.

----End

3.11.4.1.3 (Optional) Configuring Static Route Selection Based on Iteration Depth

Context

Route iteration refers to the process of finding the directly-connected outbound interface based on the next hop of a route. The iteration depth indicates the number of times the system searches for routes. A smaller number of route iterations indicates a smaller iteration depth.

When there are multiple static routes with the same prefix but different iteration depths, the system selects the static route with the smallest iteration depth as the active route and delivers it to the FIB table after static route selection based on iteration depth is configured. The other static routes then become inactive. A smaller iteration depth indicates a more stable route.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static selection-rule relay-depth
```

Static route selection based on iteration depth is configured.

By default, static routes are not selected based on iteration depth.

----End

3.11.4.1.4 (Optional) Configuring Permanent Advertisement of IPv4 Static Routes

Context

Link connectivity directly affects network stability and availability. Monitoring link status is an important measure for network maintenance. If service traffic needs to be forwarded along a specified path, you can monitor the status of the path using a ping operation. In this manner, you can monitor services at a very low cost.

With permanent advertisement of static routes, you can detect link connectivity by pinging the destination addresses of static routes. After permanent advertisement of static routes is configured, static routes always take effect regardless of the outbound interface status. In this case, the system forwards ping packets along a specified path only, which helps monitor the link status of the path.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ip route-static ip-address { mask | mask-length } { nexthop-address | interface-type interface-number [ nexthop-address ] } permanent
```

Permanent advertisement of IPv4 static routes is configured.

By default, permanent advertisement of IPv4 static routes is not configured.

----End

3.11.4.1.5 Checking the Configuration

Procedure

- Run the **display ip routing-table** command to check brief information about the IPv4 routing table.
- Run the **display ip routing-table verbose** command to check detailed information about the IPv4 routing table.

----End

3.11.5 Configuration Examples

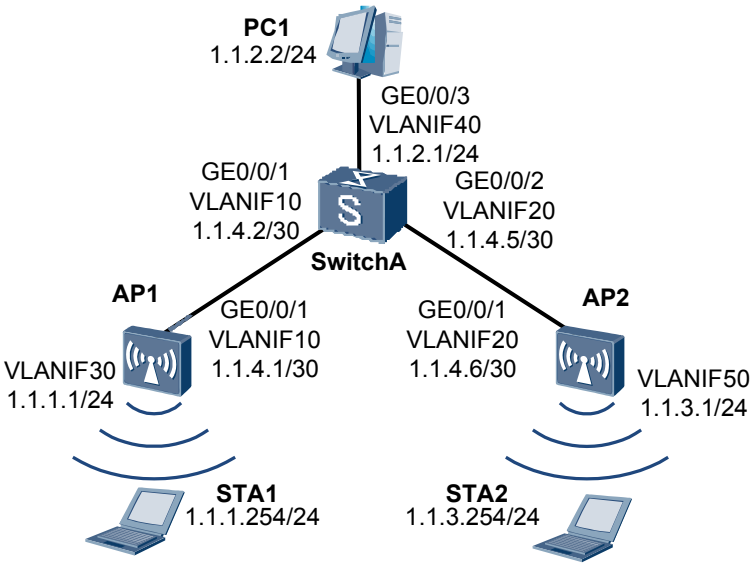
This section provides configuration examples of static routes. Configuration examples explain networking requirements, networking diagram, configuration notes, configuration roadmap, and configuration procedure.

3.11.5.1 Example for Configuring IPv4 Static Routes

Networking Requirements

As shown in **Figure 3-59**, STA1, STA2, and PC1 belong to different network segments. STA1 and STA2 go online respectively on AP1 and AP2. It is required that static routes be configured to allow PC1 to communicate with STA1 and STA2.

Figure 3-59 Networking diagram of configuring IPv4 static routes



Configuration Roadmap

The configuration roadmap is as follows:

1. Create VLANs, add interfaces to the VLANs, and assign IPv4 addresses to VLANIF interfaces so that the adjacent devices can communicate with each other.
2. Configure the default IP gateway on PC1, and configure IPv4 static routes and default routes on AP1, AP2, and SwitchA so that PC1 can communicate with STA1 and STA2.

Procedure

Step 1 Configure STA1 and STA2 to go online respectively on AP1 and AP2.

Configure VLAN 30 as AP1's service VLAN and configure STA1 to go online on AP1. STA1 obtains the IP address 1.1.1.254/24. For details, see **4.8.1 Example for Configuring the WLAN Service on a Small-Scale Network**.

Configure STA2 to go online on AP2. (The configuration procedure is not provided here.)

Step 2 On AP1, create VLANs and add interfaces to the VLANs.

```
<Huawei> system-view
[Huawei] sysname AP1
[AP1] vlan batch 10 30
[AP1] interface gigabitethernet 0/0/1
[AP1-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[AP1-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[AP1-GigabitEthernet0/0/1] quit
```

The configuration of AP2 is similar to that of AP1, and is not provided here.

Add interfaces of SwitchA to VLANs. (The configuration procedure is not provided here.)

Step 3 Assign IPv4 addresses to the VLANIF interfaces on AP1.

```
[AP1] interface vlanif 10
[AP1-Vlanif10] ip address 1.1.4.1 30
[AP1-Vlanif10] quit
[AP1] interface vlanif 30
[AP1-Vlanif30] ip address 1.1.1.1 24
[AP1-Vlanif30] quit
```

The configuration of AP2 is similar to that of AP1, and is not provided here.

Configure IP addresses for VLANIF interfaces on SwitchA. (The configuration procedure is not provided here.)

Step 4 Configure PC1 and STAs.

Configure 1.1.2.1 as the default gateway of PC1. STA1 and STA2 go online respectively on AP1 and AP2; therefore, the gateways of STA1 and STA2 are respectively 1.1.1.1 and 1.1.3.1.

Step 5 Configure static routes.

Configure a default IPv4 route on AP1.

```
[APA] ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
```

Configure two IPv4 static routes on SwitchA.

```
[SwitchA] ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
[SwitchA] ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
```

Configure a default IPv4 route on AP2.

```
[AP2] ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
```

Step 6 Verify the configurations.

Check the routing table on AP1.

```
[AP1] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 10       Routes : 10

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0          RD   1.1.4.2         Vlanif10
        1.1.1.0/24  Direct  0    0           D   1.1.1.1         Vlanif30
        1.1.1.1/32  Direct  0    0           D   127.0.0.1       Vlanif30
      1.1.1.255/32  Direct  0    0           D   127.0.0.1       Vlanif30
        1.1.4.0/30  Direct  0    0           D   1.1.4.1         Vlanif10
        1.1.4.1/32  Direct  0    0           D   127.0.0.1       Vlanif10
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
```

Run the **ping** command to verify the connectivity.

```
[AP1] ping 1.1.3.1
  PING 1.1.3.1: 56  data bytes, press CTRL_C to break
    Reply from 1.1.3.1: bytes=56 Sequence=1 ttl=254 time=62 ms
    Reply from 1.1.3.1: bytes=56 Sequence=2 ttl=254 time=63 ms
    Reply from 1.1.3.1: bytes=56 Sequence=3 ttl=254 time=63 ms
    Reply from 1.1.3.1: bytes=56 Sequence=4 ttl=254 time=62 ms
    Reply from 1.1.3.1: bytes=56 Sequence=5 ttl=254 time=62 ms

  --- 1.1.3.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 62/62/63 ms
```

Run the **tracert** command to verify the connectivity.

```
[AP1] tracert 1.1.3.1
 traceroute to  1.1.3.1(1.1.3.1), max hops: 30 ,packet length: 40, press CTRL_C to
break
 1 1.1.4.2 31 ms  32 ms  31 ms
 2 1.1.4.6 62 ms  63 ms  62 ms
```

----End

Configuration Files

- Configuration file of AP1

```
#
sysname AP1
#
vlan batch 10 30
#
interface Vlanif10
 ip address 1.1.4.1 255.255.255.252
#
interface Vlanif30
 ip address 1.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
```

```
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.2
#
return
```

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 10 20 40
#
interface Vlanif10
 ip address 1.1.4.2 255.255.255.252
#
interface Vlanif20
 ip address 1.1.4.5 255.255.255.252
#
interface Vlanif40
 ip address 1.1.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
interface GigabitEthernet0/0/2
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
interface GigabitEthernet0/0/3
 port hybrid pvid vlan 40
 port hybrid untagged vlan 40
#
ip route-static 1.1.1.0 255.255.255.0 1.1.4.1
ip route-static 1.1.3.0 255.255.255.0 1.1.4.6
#
return
```

- Configuration file of AP2

```
#
sysname AP2
#
vlan batch 20 50
#
interface Vlanif20
 ip address 1.1.4.6 255.255.255.252
#
interface Vlanif50
 ip address 1.1.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port hybrid pvid vlan 20
 port hybrid untagged vlan 20
#
ip route-static 0.0.0.0 0.0.0.0 1.1.4.5
#
return
```

3.12 Managing IP Routing Tables

This section describes how to manage IP routing tables. Through this section, you can understand the traffic forwarding paths.

3.12.1 Displaying and Maintaining a Routing Table

You can view routing tables to learn about the network topology and locate routing faults.

Context

You can view routing table information to locate routing faults. The following describes the commands used to display and maintain routing table information.

The display commands can be used in all views. The reset commands are used in the user view.

If the access point imports a large number of routes, system performance may be affected when services are being processed because the routes consume a lot of system resources. To improve system security and reliability, configure a limit on the number of public route prefixes. When the number of public route prefixes exceeds the limit, an alarm is generated, prompting you to check whether unnecessary public route prefixes exist.

Procedure

- Run the **display ip routing-table** command to check brief information about the active routes in the IPv4 routing table.
- Run the **display ip routing-table verbose** command to check detailed information about the IPv4 routing table.
- Run the **display ip routing-table** *ip-address* [*mask* | *mask-length*] [**longer-match**] [**verbose**] command to check detailed information about the routes with the specified destination address in the IPv4 routing table.
- Run the **display ip routing-table** *ip-address1* { *mask1* | *mask-length1* } *ip-address2* { *mask2* | *mask-length2* } [**verbose**] command to check detailed information about the routes within the specified destination address range in the IPv4 routing table.
- Run the **display ip routing-table protocol** *protocol* [**inactive** | **verbose**] command to check detailed information about the routes discovered by the specified routing protocol in the IPv4 routing table.
- Run the **display ip routing-table statistics** command to check route statistics in the IPv4 routing table.
- Run the **reset ip routing-table statistics protocol** { **all** | *protocol* } command to clear route statistics in the IPv4 routing table.

----End

3.12.2 Displaying the Routing Management Module

You can view information about the routing management module to locate routing faults.

Procedure

- Run the **display rm interface** [*interface-type interface-number*] command to check IPv4 routing management (RM) information on the specified interface.

----End

3.12.3 FIB Query

You can check the forwarding information base (FIB) to locate forwarding faults.

Context

NOTE

Unless otherwise stated, the FIB in this document refers to unicast FIB.

A device selects routes according to the routing table and forwards packets according to the FIB. If the FIB is overloaded, new active routes cannot be delivered to the FIB, affecting packet forwarding.

Procedure

- Check FIB entries.
  - Run the **display fib** [*slot-id*] [**verbose**] command to check IPv4 FIB entries.
  - Run the **display fib acl** *acl-number* [**verbose**] command to check IPv4 FIB entries that match a specified ACL rule.
  - Run the **display fib ip-prefix** *prefix-name* [**verbose**] command to check IPv4 FIB entries that match a specified IP prefix list.
  - Run the **display fib** [*slot-id*] *destination-address1* [**verbose**] command to check IPv4 FIB entries that match a specified destination IP address.
  - Run the **display fib** [*slot-id*] *destination-address1 destination-mask1* [**verbose**] command to check IPv4 FIB entries that exactly match a specified destination IP address and mask.
  - Run the **display fib** [*slot-id*] *destination-address1* **longer** [**verbose**] command to check all IPv4 FIB entries that match destination IP addresses in the natural mask range.
  - Run the **display fib** [*slot-id*] *destination-address1 destination-mask1* **longer** [**verbose**] command to check all IPv4 FIB entries that match destination IP addresses in a specified mask range.
  - Run the **display fib** [*slot-id*] *destination-address1 destination-mask1 destination-address2 destination-mask2* [**verbose**] command to check IPv4 FIB entries that match destination IP addresses in the range of *destination-address1 destination-mask1* and *destination-address2 destination-mask2*.
  - Run the **display fib next-hop** *ip-address* command to check IPv4 FIB entries that match a specified next-hop IP address.
  - Run the **display fib** [*slot-id*] **statistics** command to check the total number of IPv4 FIB entries.
  - Run the **display fib statistics all** command to check IPv4 FIB entry statistics.

----End

4 Configuration Guide - WLAN Service

About This Chapter

You can configure the WLAN service to enable users to easily access a wireless network and move around within the coverage of the wireless network.

4.1 Introduction to WLAN

This section describes the definition and functions of WLAN.

Definition

A wireless local area network (WLAN) is a network that uses wireless channels such as radio waves, laser, and infrared rays to replace the transmission media used on a wired LAN. The WLAN technology described in this document is implemented based on 802.11 standards. That is, a WLAN is a network that uses high-frequency signals (for example, 2.4 GHz or 5 GHz signals) as transmission media.

802.11 was originally a wireless LAN communications standard defined by the Institute of Electrical and Electronics Engineers (IEEE) in 1997. The IEEE then made amendments to the standard, forming the 802.11 family, including 802.11, 802.11a, 802.11b, 802.11e, 802.11g, 802.11i, and 802.11n.

Purpose

Wired LANs use wired cables or optical fibers as transmission media, which are expensive and have fixed locations. As people have increasing requirements on network mobility, wired LANs cannot meet these requirements. WLAN technology is then developed. Currently, WLAN has become a cost-efficient network access mode. WLAN technology allows you to easily access a wireless network and move around within the coverage of the wireless network.

Benefits

- High network mobility: WLANs can be connected easily, which is not limited by cable and port positions. WLANs especially apply to scenarios such as office buildings, airport halls, resorts, hotels, stadiums, and cafes.
- Flexible network deployment: WLANs can provide wireless network coverage in places where cables are difficult to deploy, such as subways and highways. This solution reduces cables, offers ease of implementation at a low cost, and has high scalability.

4.2 Principles

This section describes principles for implementing basic WLAN services.

4.2.1 Concepts

- Station (STA): a terminal that supports 802.11 standards, such as a PC that has a wireless NIC or a mobile phone that supports WLAN.
- Radio signal: high-frequency electromagnetic wave that has long-distance transmission capabilities. Radio signals provide transmission media for 802.11-compliant WLANs. Radio signals described in this document are electromagnetic waves in 2.4 GHz or 5 GHz frequency band.
- Access point (AP): a device that provides 802.11-compliant wireless access for STAs to connect wired networks and wireless networks.

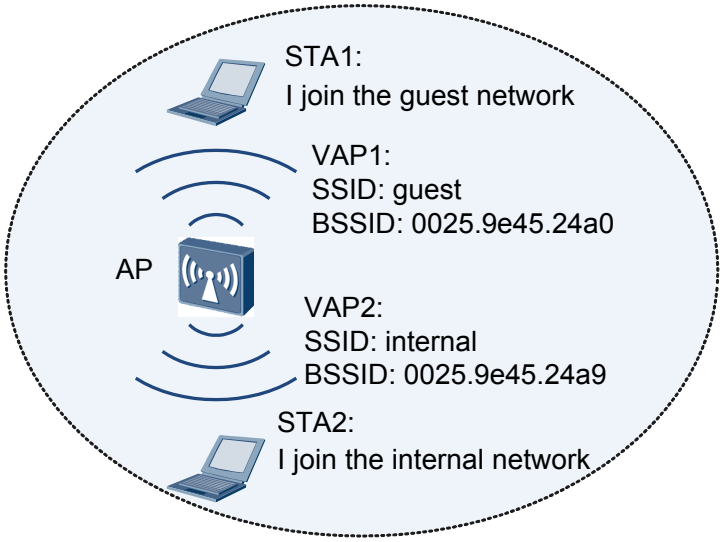
- Fat AP: provides wireless access for STAs in the **autonomous architecture**. A Fat AP provides wireless connection, security, and management functions.

- Virtual access point (VAP): a WLAN service entity on an AP. You can create different VAPs on an AP to provide wireless access service for different user groups.
- Service set identifier (SSID): a unique identifier that identifies a wireless network. When you search for available wireless networks on your laptop, SSIDs are displayed to identify the available wireless networks.

  SSIDs are classified into two types:

  - Basic service set identifier (BSSID): a link-layer MAC address of a VAP on an AP. **Figure 4-1** shows the relationship between VAP and BSSID.

    Figure 4-1 Relationship between VAP and BSSID

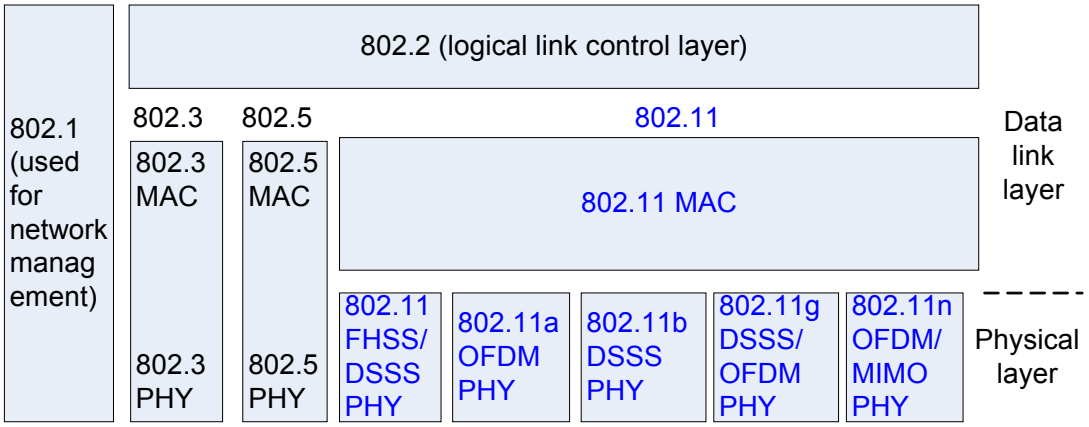
  - Extended service set identifier (ESSID): an identifier of one or a group of wireless networks. For example, in **Figure 4-1**, SSID **guest** identifies a wireless network, and SSID **internal** identifies another wireless network. A STA scans all wireless networks and selects a wireless network based on the SSID. Generally, an SSID refers to an ESSID.
- Basic service set (BSS): an area covered by an AP. STAs in a BSS can communicate with each other.

4.2.2 802.11 Standards

Introduction to 802.11

Figure 4-2 shows the role of 802.11 standards in the IEEE 802 standard family, involving the physical layer and data link layer.

Figure 4-2 Role of 802.11 standards in the IEEE 802 standard family



- Physical Layer

  802.11 standards use different physical layer technologies, including frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), orthogonal frequency division multiplexing (OFDM), and multiple-input multiple-output (MIMO). These physical layer technologies support different frequency bands and transmission rates, as shown in **Table 4-1**.

Table 4-1 Comparisons between 802.11 standards

802.11 Standard	Physical Layer Technology	Frequency Band (GHz)	Transmission Rate (Mbit/s)	Compatibility with Other 802.11 Standards	Commercial Use
802.11	FHSS/ DSSS	2.4	1, 2	Incompatible	Earlier standard, supported by most products
802.11b	DSSS	2.4	1, 2, 5.5, 11	Incompatible	Earlier standard, supported by most products
802.11a	OFDM	5	6, 9, 12, 18, 24, 36, 48, 54	Incompatible	Rarely used
802.11g	DSSS/ OFDM	2.4	1, 2, 5.5, 11, 6, 9, 12, 18, 24, 36, 48, 54	Compatible with 802.11b	Widely used

802.11 Standard	Physical Layer Technology	Frequency Band (GHz)	Transmission Rate (Mbit/s)	Compatibility with Other 802.11 Standards	Commercial Use
802.11n	OFDM/ MIMO	2.4, 5	A maximum of 600 Mbit/s, depending on the modulation and coding scheme (MCS)	Compatible with 802.11a, 802.11b, and 802.11g	Widely used

- Data Link Layer

  On a wired LAN, 802.3 standards use the carrier sense multiple access with collision detection (CSMA/CD) mechanism to control wired media access of different devices. The CSMA/CD mechanism requires that all terminals should detect packets of each other. However, WLANs provide only limited wireless signal coverage, so some terminals may fail to detect the packets of each other. 802.11 standards use the carrier sense multiple access with collision avoidance (CSMA/CA) mechanism to overcome the deficiency in the CSMA/CD mechanism.

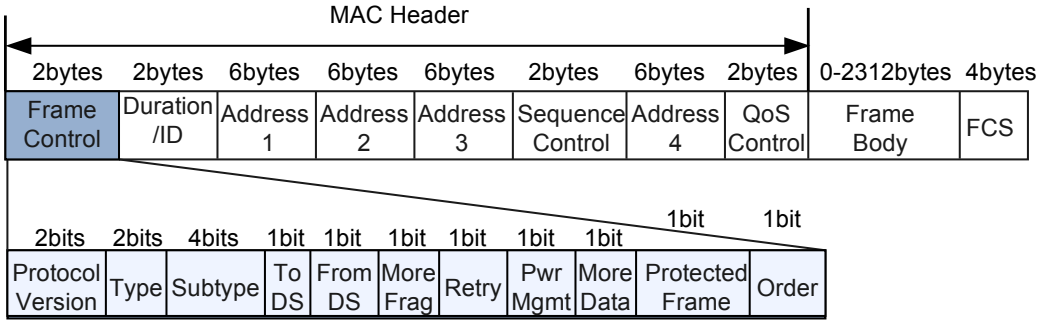
  NOTE

  For CSMA/CA principles, see **8.3.2.1 WMM**.

802.11 MAC Frame Format

An 802.11 MAC frame consists of a MAC header, frame body, and frame check sequence (FCS). The settings of attribute fields in the MAC header determine the frame type. **Figure 4-3** shows the 802.11 MAC frame format.

Figure 4-3 802.11 MAC frame format



An 802.11 MAC frame has a maximum length of 2348 bytes. The following describes the meanings of each field in an 802.11 MAC frame.

- Frame Control field: includes the following sub-fields:

- Protocol Version: indicates the MAC version of the frame. Currently, only MAC version 0 is supported.
- Type/Subtype: identifies the frame type, including data, control, and management frames.
  - Data frame: transmits data packets, including a special type of frame: Null frame. A Null frame has a zero-length frame body. A STA can send a Null frame to notify an AP of the changes in the power-saving state.

    NOTE

    802.11 supports the power-saving mode, allowing STAs to shut down antennas to save power when no data is transmitted.
  - Control frame: helps transmit data frames, releases and obtains channels, and acknowledges received data. Some common control frames include:
    - Acknowledgement (ACK) frame: After receiving a data frame, the receiving STA will send an ACK frame to the sending STA.
    - Request to Send (RTS) and Clear to Send (CTS) frames: provide a mechanism to reduce collisions for APs with hidden STAs. A STA sends an RTS frame before sending data frames. The STA that receives the RTS frame responds with a CTS frame. This mechanism is used to release a channel and enable a sending STA to obtain data transmission media.
  - Management frame: manages WLANs, including notifying network information, adding or removing STAs, and managing radio. Some common management frames include:
    - Beacon frame: is periodically sent by an AP to announce the WLAN presence and provide WLAN parameters (for example, the SSID, supported rate, and authentication type).
    - Association Request/Response frame: A STA sends an Association Request frame to an AP to request to join a WLAN. After receiving the Association Request frame, the AP sends an Association Response frame to the STA to accept or reject the association request.
    - Disassociation frame: is sent from a STA to terminate the association with an AP.
    - Authentication Request/Response frame: is used in link authentication between a STA and an AP for identity authentication.
    - Deauthentication frame: is sent from a STA to terminate link authentication with an AP.
    - Probe Request/Response frame: A STA or an AP sends a Probe Request frame to detect available WLANs. After another STA or AP receives the Probe Request frame, it needs to reply with a Probe Response frame that carries all parameters specified in a Beacon frame.
- To DS and From DS: indicates whether a data frame is destined for a distribution system (or an AP). If the two fields are set to 1, the data frame is transmitted between APs.
- More Frag: indicates whether a packet is divided into multiple fragments for transmission.
- Retry: indicates whether a frame needs to be retransmitted. This field helps eliminate duplicate frames.

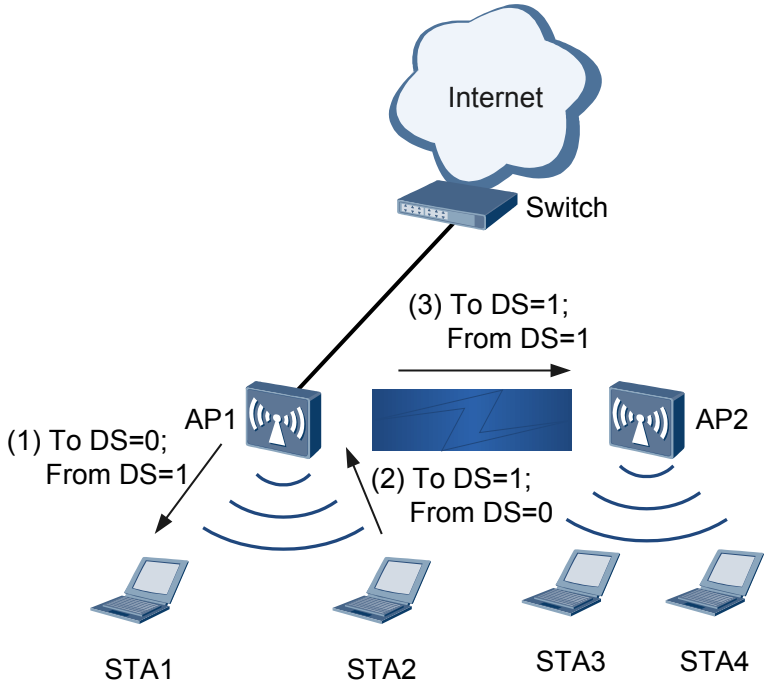
  - Pwr Mgmt: indicates the power management mode of a STA after the completion of a frame exchange, including Active and Sleep modes.
  - More Data: indicates that an AP transmits buffered packets to a STA in power-saving mode.
  - Protected Frame: indicates whether a frame is encrypted.
  - Order: indicates whether a frame is transmitted in order.
- Duration/ID field: provides the following functions according to its values.
  - Indicates the duration in which a STA can occupy a channel. This field is used for CSMA/CA.
  - Identifies an MAC frame transmitted during Contention-Free Period (CFP). The value of this field is fixed as 32768, indicating that a STA keeps occupying a channel and other STAs cannot use the channel.
  - Specifies the Association ID (AID) of a PS-Poll frame, which identifies the BSS to which a STA belongs. A STA may work in active or sleep mode. When a STA works in sleep mode, an AP buffers data frames destined for the STA. When the STA transitions from the sleep mode to the active mode, the STA sends a PS-Poll frame to request the buffered data frames. After receiving the PS-Poll frame, the AP delivers the requested data frames to the STA based on the AID in the PS-Poll frame.
- Address field: indicates MAC addresses. An 802.11 frame can have up to four address fields. The four address fields vary according to the To DS/From DS sub-field in the Frame Control field. For example, the values of the four address fields are different when a frame is sent from a STA to an AP and when a frame is sent from an AP to a STA. **Table 4-2** describes the rules for filling in the four address fields.

Table 4-2 Rules for filling in the four address fields

To DS	From DS	Address 1	Address 2	Address 3	Address 4	Description
0	0	Destination address	Source address	BSSID	Unused	The frame is a management or control frame, for example, a Beacon frame sent by an AP.
0	1	Destination address	BSSID	Source address	Unused	AP1 sends the frame to STA1 as shown in (1) in **Figure 4-4**.

To DS	From DS	Address 1	Address 2	Address 3	Address 4	Description
1	0	BSSID	Source address	Destination address	Unused	STA2 sends the frame to AP1 as shown in (2) in **Figure 4-4**.
1	1	BSSID of the destination AP	BSSID of the source AP	Destination address	Source address	AP1 sends the frame to AP2 as shown in (3) in **Figure 4-4**.

Figure 4-4 WLAN networking



- Sequence Control field: is used to eliminate duplicate frames and reassemble fragments. It includes two sub-fields:
  - Fragment Number: is used to reassemble fragments.
  - Sequence Number: is used to eliminate duplicate frames. When a device receives an 802.11 MAC frame, the device discards the frame if its Sequence Number field value is the same as a previous frame.

- QoS Control field: exists only in a data frame to implement 802.11e-compliant WLAN QoS.
- Frame Body field: transmits payload from higher layers. It is also called the data field. In 802.11 standards, the transmitted payload is also called a MAC service data unit (MSDU).
- Frame Check Sequence (FCS) field: checks the integrity of received frames. The FCS field is similar to the cyclic redundancy check (CRC) field in an Ethernet packet.

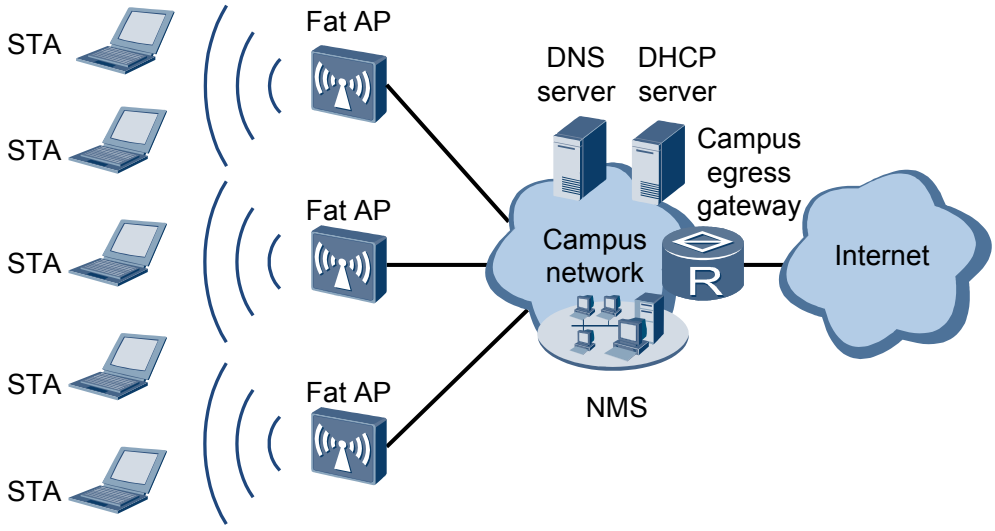
4.2.3 WLAN Architecture

A WLAN has the wired side and wireless side. On the wired side, an AP connects to the Internet using Ethernet. On the wireless side, a STA communicates with an AP using 802.11. The WLAN architecture on the wireless side includes the autonomous architecture.

Autonomous Architecture

In autonomous architecture, Fat APs implement wireless access without requiring an AC, as shown in **Figure 4-5**.

Figure 4-5 WLAN autonomous architecture



The autonomous architecture was widely used in early stage of WLAN construction. Fat APs have powerful functions and can work independently of ACs; however, Fat APs have complex structure and are difficult to manage in a centralized manner. When an enterprise has a large number of APs deployed, AP configuration and software upgrade bring large workload and high costs. Therefore, the autonomous architecture is gradually replaced by the centralized architecture.

In autonomous architecture, STAs associate with a Fat AP to access a WLAN. For details, see **4.2.4 STA Access**.

4.2.4 STA Access

STA access includes three phases: scanning, link authentication, and association.

Scanning

A STA can actively or passively scan wireless networks.

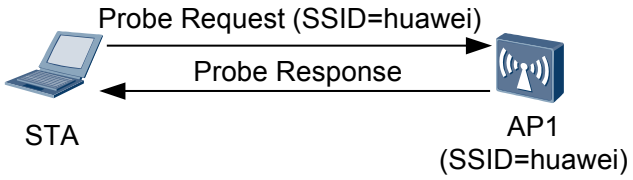
Active Scanning

In active scanning, a STA periodically searches for surrounding wireless networks. The STA can send two types of Probe Request frames: containing SSID and not containing SSID.

- The STA sends a Probe Request frame containing an SSID in each channel to search for the AP with the same SSID. Only the AP with the same SSID will respond to the STA. For example, in **Figure 4-6**, the STA sends a Probe Request frame containing SSID huawei to search for an AP with SSID huawei.

  This method applies to the scenario where a STA actively scans wireless networks to access a specified wireless network.

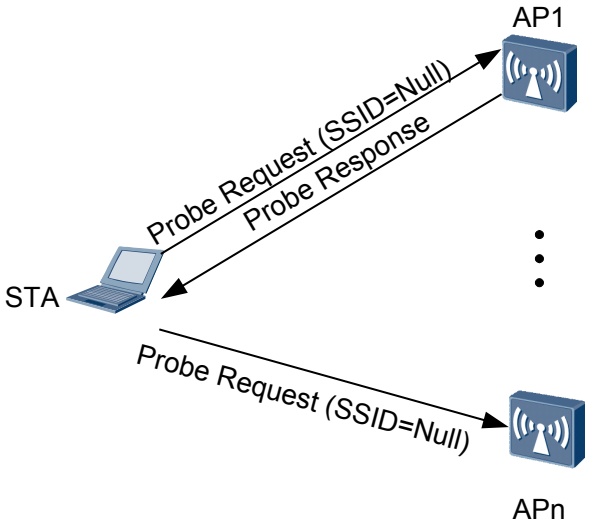
  Figure 4-6 Active scanning by sending a Probe Request frame containing an SSID

- The STA periodically broadcasts a Probe Request frame that does not contain an SSID in the supported channels as shown in **Figure 4-7**. The APs return Probe Response frames to notify the STA of the wireless services they can provide.

  This method applies to the scenario where a STA actively scans wireless networks to determine whether wireless services are available.

  Figure 4-7 Active scanning by sending a Probe Request frame containing no SSID

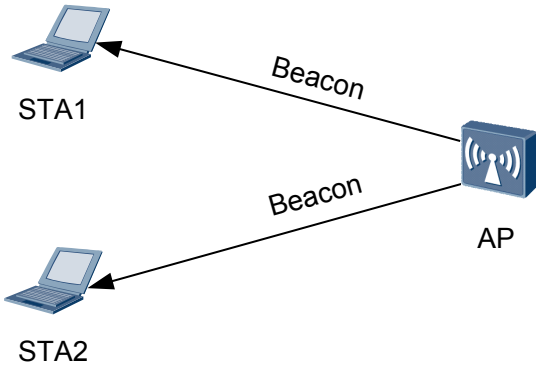
  

Passive Scanning

In **Figure 4-8**, a STA listens on the Beacon frames that an AP periodically sends in each channel to obtain AP information. A Beacon frame contains information including the SSID and supported rate.

To save power of a STA, enable the STA to passively scan wireless networks. In most cases, VoIP terminals passively scan wireless networks.

Figure 4-8 Passive scanning process

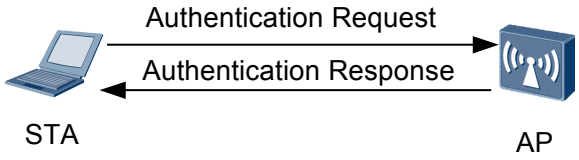


Link Authentication

To ensure wireless link security, an AP needs to authenticate STAs that attempt to access the AP. IEEE 802.11 defines two authentication modes: open system authentication and shared key authentication.

- Open system authentication: indicates no authentication. STAs are successfully authenticated as long as the AP to be associated supports this mode, as shown in **Figure 4-9**.

  Figure 4-9 Open system authentication

- Shared key authentication: requires that the STA and AP have the same shared key preconfigured. The AP checks whether the STA has the same shared key to determine whether the STA can be authenticated. If the STA has the same shared key as the AP, the STA can be authenticated. Otherwise, the STA cannot be authenticated.

Figure 4-10 Shared key authentication

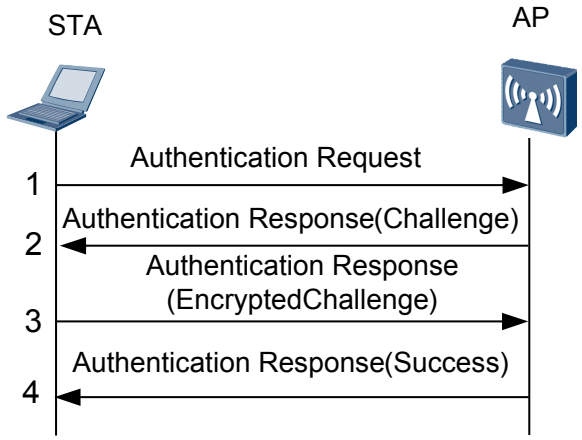


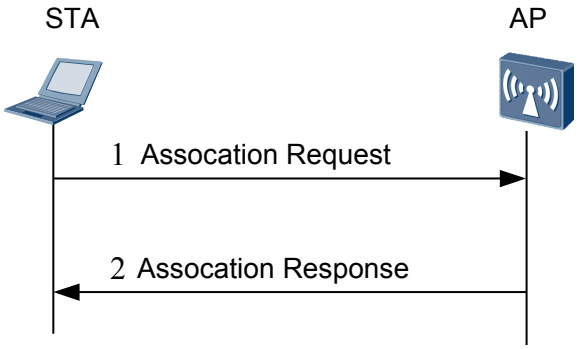
Figure 4-10 shows the shared key authentication process:

1. The STA sends an Authentication Request packet to the AP.
2. The AP generates a challenge and sends it to the STA.
3. The STA uses the preconfigured key to encrypt the challenge and sends it to the AP.
4. The AP uses the preconfigured key to decrypt the encrypted challenge and compares the decrypted challenge with the challenge sent to the STA. If the two challenges are the same, the STA can be authenticated. Otherwise, the STA cannot be authenticated.

Association

Client association refers to link negotiation. After link authentication is complete, a STA initiates link negotiation using Association packets, as shown in Figure 4-11.

Figure 4-11 STA association



1. The STA sends an Association Request packet to the AP. The Association Request packet carries the STA's parameters and the parameters that the STA selects according to the service configuration, including the transmission rate, channel, QoS capabilities, access authentication algorithm, and encryption algorithm.
2. The AP determines whether to authenticate the STA according to the received Association Request packet and replies with an Association Response packet.

NOTE

The STA determines whether it needs to be authenticated according to the received Association Response packet:

- If the STA does not need to be authenticated, the STA can access the wireless network.
- If the STA needs to be authenticated, the STA initiates user access authentication. After being authenticated, the STA can access the wireless network. For details about user access authentication, see NAC Configuration in *Huawei Wireless Access Points Configuration - Configuration Guide - Security*.

4.3 Applications

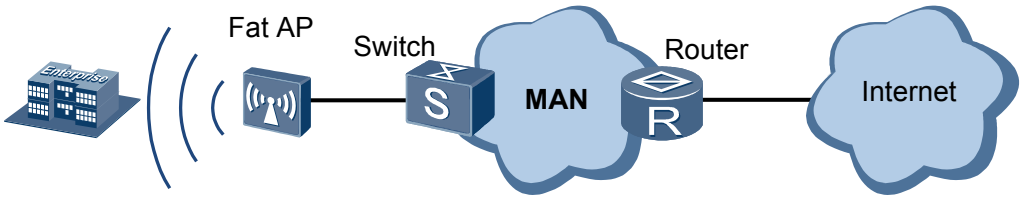
This section describes application scenarios of basic WLAN services.

4.3.1 SOHO WLAN Networking Application

The SOHO WLAN solution applies to independent small-scale networks, for example, small-scale enterprises, stores, cafe bars, SOHO offices, or enterprise branches where WLAN services are deployed independently.

Most of SOHO WLAN networks have no independent authentication server or NMS device and use the autonomous architecture (Fat AP). In **Figure 4-12**, a Fat AP is deployed on the SOHO WLAN.

Figure 4-12 SOHO WLAN networking



4.4 Configuration Task Summary

After basic WLAN service configurations are complete, STAs can access the wireless network.

WLAN basic functions can be implemented only when the following tasks are complete:

Tasks 1 and 3 are mandatory, and you need to complete the them one by one.

1. **4.6.1 Configuring AP System Parameters**: You can configure AP system parameters to identify an AP and ensure that radio parameters (channel and power) of an AP comply with local laws and regulations.
2. **4.6.2 (Optional) Managing APs**: You can configure management APs, including configuring alarm thresholds and log suppression, and disabling radios or VAPs as scheduled, which facilitates AP management.
3. **4.6.3 Configuring the WLAN Service VAP**: You can configure different VAPs for APs to provide differentiated WLAN services for users.

4.5 Default Configuration

This section provides the default WLAN service configuration.

Table 4-3 Default WLAN service configuration

Parameter	Default Setting
Country code	CN (China)

4.6 Configuring WLAN Service

You can configure the WLAN service to enable users to easily access a wireless network and move around within the coverage of the wireless network.

4.6.1 Configuring AP System Parameters

You can configure AP system parameters to identify an AP and ensure that radio parameters (channel and power) of an AP that associates with the AP comply with local laws and regulations.

Pre-Configuration Tasks

Before configuring AP system parameters, complete the following task:

- **1.4 Configuring User Login**

Configuration Process

The configuration tasks are mandatory and can be performed in any sequence. The AP function takes effect only when all configuration tasks are completed.

4.6.1.1 Configuring Country Codes

Context

A country code identifies the country to which AP radios belong. Different countries support different AP radio attributes, including the transmit power and supported channels.

NOTE

- When configuring an AP for the first time, you must configure the correct country code. The country code must comply with local laws and regulations.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan global country-code country-code
```

A global country code is configured for the AP.

By default, the global country code of a fat AP is CN.

NOTE

For details about country codes, see **wlan global country-code**.

Changing a country code will delete related VAPs.

----End

4.6.1.2 Checking the Configuration

Procedure

- Run the **display wlan global** command to check AP system parameters.

----End

4.6.2 (Optional) Managing APs

You can configure management APs, including configuring alarm thresholds and log suppression, and disabling radios or VAPs as scheduled, which facilitates AP management.

Pre-Configuration Tasks

Before configuring management APs, complete the following tasks:

- **1.4 Configuring User Login**

Configuration Process

The configuration tasks are mandatory and can be performed in any sequence.

4.6.2.1 Configuring Alarm Thresholds on an AP

Context

You can configure alarm thresholds on an AP to monitor the AP in real time. When the configured thresholds are exceeded, the AP generates alarms or logs.

The default alarm thresholds are recommended.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
high-temperature threshold value
```

The high temperature alarm threshold is configured.

By default, the high temperature alarm threshold on an AP is 50°C.

NOTE

The AP5010SN-GN and AP5010DN-AGN do not support this command.

Step 4 Run:

```
low-temperature threshold value
```

The low temperature alarm threshold is configured.

By default, the low temperature alarm threshold on an AP is -10°C.

NOTE

The AP5010SN-GN and AP5010DN-AGN do not support this command.

----End

4.6.2.2 Configuring Log Suppression on APs

Context

If a STA keeps attempting to connect to an AP because of signal interference or instability, the AP processes a large number of duplicate login and logoff logs in a short period, causing a huge waste of resources.

To address this problem, enable log suppression.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
access-user syslog-restrain enable
```

Log suppression is enabled on APs.

By default, log suppression is enabled on an AP.

Step 3 (Optional) Run:

```
access-user syslog-restrain period period
```

The log suppression period is set.

By default, the log suppression period on an AP is 300s.

----End

4.6.2.3 Checking the Configuration

Procedure

- Run the **display ap** command to check AP information.
- Run the **display optical-info ap-id** *ap-id* command to check optical module information on an AP.

----End

4.6.3 Configuring the WLAN Service VAP

When an AP is working properly, you can configure service virtual access points (VAPs) on the AP to provide differentiated WLAN services for users.

Pre-configuration Tasks

Before configuring the WLAN service VAP, complete the following task:

- **4.6.1 Configuring AP System Parameters**
- Configuring a DHCP server to allocate IP addresses to STAs

  NOTE

  For details on how to configure a DHCP server, see **3.8 DHCP Configuration**. To use a DHCP server to assign IP addresses to STAs, configure the fat AP as the DHCP server or use an independent DHCP server.

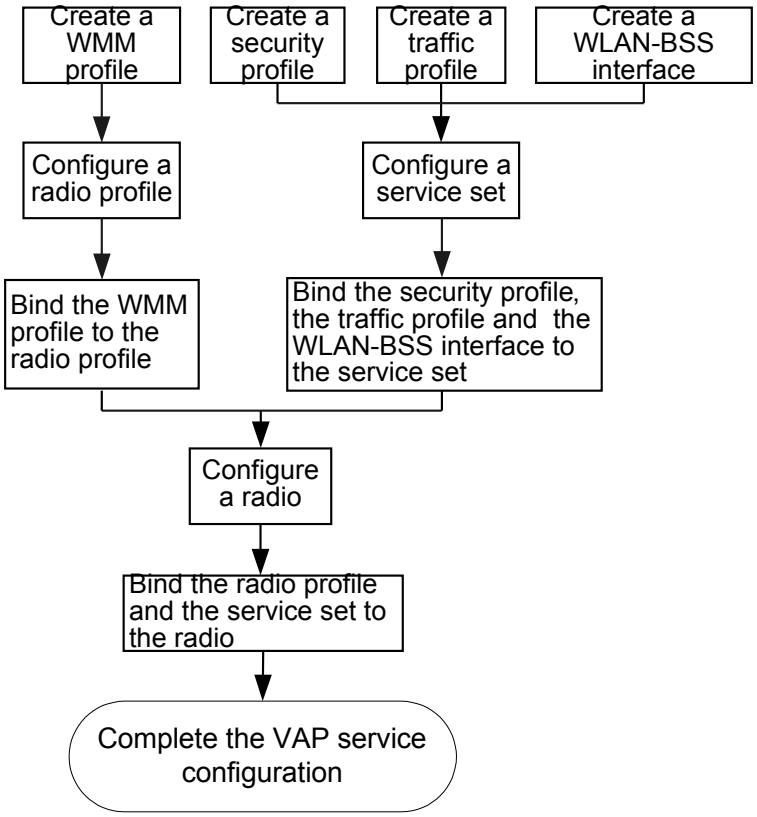
  - When an enterprise branch has no independent DHCP server, configure an fat AP as the DHCP server.
  - An independent DHCP server applies to large WLANs of large- and medium-sized campus networks.

Configuration Process

When a user discovers a WLAN and connects to the WLAN, the user connects to a VAP. A VAP is a functional entity on an AP. You can create different VAPs on an AP to provide wireless access services for different users so that these users can obtain different network resources. A VAP is also the binding relationship between an AP, a radio, and a service set.

Figure 4-13 shows the process of configuring a VAP. Learn about the configuration process before configuring a VAP.

Figure 4-13 Configuring a VAP



4.6.3.1 Creating a WMM Profile

Context

802.11 provides services of the same quality for all applications. Different applications, however, have different requirements for wireless networks. 802.11 cannot provide differentiated services for different applications.

To provide differentiated services for different applications, the Wi-Fi Alliance defines the Wi-Fi Multimedia (WMM) standard, which classifies data packets into four access categories (ACs) in descending order of priorities, that is, AC-voice (AC-VO), AC-video (AC-VI), AC-best effort (AC-BE), and AC-background (AC-BK). This standard ensures that high-priority packets preempt channels.

A WMM profile is created to implement the WMM protocol. After a WMM profile is created, packets with higher AP or STA priority preempt a wireless channel first, ensuring better quality for voice and video services on WLANs.

NOTE

For details on how to configure parameters in a WMM profile, see **8.3.6 Configuring WMM**.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
wmm-profile { id profile-id | name profile-name } *
```

A WMM profile is created and the WMM profile view is displayed.

By default, the WMM profile named **wmmf** exists in the system.

NOTE

When creating a WMM profile, pay attention to the following:

- After a WMM profile is created, the profile retains the default settings. The default settings are recommended. For details on how to configure a WMM profile, see **8.3.6 Configuring WMM**.
- The profile name is mandatory when you create a WMM profile.

----End

4.6.3.2 Configuring a Radio Profile

Context

A radio profile defines the following parameters: radio type, radio rate, channel mode, radio power mode, packet loss threshold, error packet threshold, collision rate threshold, packet fragmentation threshold, Request To Send/Clear To Send (RTS/CTS) threshold, maximum number of retransmission attempts for long/short frames, whether short preamble is supported, delivery traffic indication message (DTIM) interval, Beacon frame interval, and WMM profile name or ID. If a radio is bound to a radio profile, the radio inherits all the parameters defined in the radio profile.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
radio-profile { id profile-id | name profile-name } *
```

A radio profile is created and the radio profile view is displayed.

By default, the radio profile named **radiof** exists in the system.

NOTE

When creating a radio profile, pay attention to the following:

- After a radio profile is created, the profile retains the default settings.
- The profile name is mandatory when you create a radio profile.

Step 4 (Optional) Configure optional parameters in the radio profile.

Procedure	Command	Description
Configure the channel mode.	**channel-mode** { **auto** | **fixed** } By default, the channel mode is automatic mode. **NOTE** When the channel working mode of a radio changes from automatic mode to fixed mode, the channel in automatic mode replaces the manually configured channel to ensure that the radio works in the optimal channel environment.	An AP supports two channel modes: ● Automatic mode: An AP selects a channel for a radio based on the WLAN radio environment, so you do not need to specify channels for radios.It is recommended that you configure the radio calibration function for automatic selection of optimal channels and fix the channel through commands. For details, see **5.7 Configuring Radio Calibration**. You can also manually specify the channel based on network planning, preventing channel interferences. ● Fixed mode: A channel is manually configured for a radio to avoid frequent channel adjustment (this may cause intermittent service interruption).

Procedure	Command	Description
Configure the power mode.	**power-mode** { **auto** | **fixed** } By default, the power mode is automatic mode.	An AP supports two power modes: ● Automatic mode: The AP selects the transmit power for a radio based on the WLAN radio environment. ● Fixed mode: The transmit power is manually configured for a radio.
Configure the radio type.	**radio-type** { **80211a** | **80211an** | **80211gn** | **80211b** | **80211bg** | **80211bgn** | **80211g** | **80211n** } By default, the radio type is 802.11bgn.	Different radios have different radio types: ● The radio type of a 2.4-GHz radio can be 802.11b, 802.11bg, 802.11bgn, 802.11g, 802.11n, or 802.11gn. ● The radio type of a 5-GHz radio can be 802.11a, 802.11n, or 802.11an.
Set the rate mode to automatic mode and configure the maximum rate.	**rate auto max-rate rate-value** { **rate_1** | **rate_2** | **rate_5_5** | **rate_6** | **rate_9** | **rate_11** | **rate_12** | **rate_18** | **rate_24** | **rate_36** | **rate_48** | **rate_54** }	If you configure the maximum rate for a radio but the radio does not support the configured maximum rate, the configuration fails. For example, if a maximum rate of 54 Mbit/s is configured for an 802.11b radio, the configuration fails because the radio does not support the rate of 54 Mbit/s.
Configure the interval at which an AP sends Beacon frames.	**beacon-interval** *beacon-interval* By default, the interval for sending Beacon frames is 100 ms.	An AP broadcasts Beacon frames at intervals to notify STAs of an existing 802.11 network.

Procedure	Command	Description
Configure the DTIM interval.	**dtim-interval** *dtim-interval* By default, the DTIM interval is 1.	The DTIM interval specifies how many Beacon frames are sent before the Beacon frame that contains the DTIM. An AP sends a Beacon fame to wake a STA in power-saving mode, indicating that the saved broadcast and multicast frames will be transmitted to the STA. ● A short DTIM interval helps transmit data in a timely manner, but the STA is waken frequently, causing high power consumption. ● A long DTIM interval lengthens the dormancy time of a STA and saves power, but degrades the transmission capability of the STA.

Procedure	Command	Description
Configure an AP to support the short preamble.	**short-preamble** { **enable** | **disable** } By default, an AP supports the short preamble.	The preamble is a section of bits in the header of a data frame. It synchronizes signals transmitted between the sender and receiver and can be a short or long preamble. ● A short preamble ensures better network synchronization performance and is recommended. ● A long preamble is usually used for compatibility with earlier network adapters of clients.

Procedure		Command	Description
Configure the packet fragmentation threshold.		**fragmentation-threshold** *fragmentation-threshold* By default, the packet fragmentation threshold is 2346 bytes.	If an 802.11 MAC frame exceeds the packet fragmentation threshold, the frame needs to be fragmented. ● When the packet fragmentation threshold is too small, packets are fragmented into smaller frames. These frames are transmitted at a high extra cost, resulting in low channel efficiency. ● When the packet fragmentation threshold is too large, long packets are not fragmented, increasing the transmission time and error probability. If an error occurs, packets are retransmitted. This wastes the channel bandwidth. ● A large threshold is recommended.
Configure the collision rate threshold, packet loss threshold, and error packet threshold.	Configure the collision rate threshold.	**conflict-rate-threshold** *conflict-rate-threshold* By default, the collision rate threshold is 60%.	This configuration helps determine whether the radio environment is good. When the collision rate, packet loss ratio, or error packet ratio of a radio reaches the threshold, the system considers that the radio environment deteriorates. When this occurs, the system needs to improve the radio environment.
	Configure the packet loss threshold and error packet threshold.	**per-threshold** *per-threshold* By default, the packet loss threshold and error packet threshold is 30%.	

Procedure	Command	Description
Enable beamforming.	**beamforming enable** By default, beamforming is disabled.	Beamforming can enhance signals at a particular angle (for target users), attenuate signals at another angle (for non-target users or obstacles), and extend the radio coverage area. **NOTE** AP6x10SN/DN series except AP6310SN-GN supports beamforming.

Procedure		Command	Description
Configure the RTS-CTS operation mode.		**rts-cts-mode** { **cts-to-self** | **disable** | **rts-cts** } By default, the RTS-CTS operation mode is cts-to-self.	The RTS/CTS handshake mechanism prevents data transmission failures caused by channel conflicts. If STAs perform RTS/CTS handshakes before sending data, RTS frames consume high channel bandwidth. The default RTS-CTS operation mode is recommended. ● If the RTS/CTS handshake mechanism is not used, there may be hidden STAs. If base stations A and C simultaneously send information to base station B because base station C does not know that base station A is sending information to base station B, signal conflict occurs. As a result, signals fail to be sent to base station B. ● The RTS/CTS handshake mechanism reduces the transmission rate and even causes the network delay. **NOTE** To reduce the network delay, disable RTS-CTS.
Configure the RTS mechanism.	Configure the RTS threshold.	**rts-cts-threshold** *rts-cts-threshold* By default, the RTS threshold is 2347 bytes.	If STAs perform RTS/CTS handshakes before sending data, many RTS frames consume high channel bandwidth. To prevent

Procedure		Command	Description
	Configure the maximum number of retransmission attempts for frames smaller than or equal to the RTS threshold.	**short-retry** *retry-number* By default, the maximum number of retransmission attempts for frames smaller than or equal to the RTS threshold is 7.	this problem, set the RTS threshold and maximum number of retransmission attempts for long/short frames. The RTS threshold specifies the length of frames to be sent. When the length of frames to be sent by a STA is smaller than the RTS threshold, no RST/CTS handshake is performed. The default RTS threshold is recommended. **NOTE** This configuration is applicable only when the RTS-CTS operation mode is rts-cts.
	Configure the maximum number of retransmission attempts for frames longer than the RTS threshold.	**long-retry** *retry-number* By default, the maximum number of retransmission attempts for frames longer than the RTS threshold is 4.	
Configure 802.11n.	Configure the guard interval (GI) mode.	**80211n guard-interval-mode** { **short** | **normal** } By default, the normal GI is used.	There are two types of GI: short GI and normal GI. When configuring 802.11n, you can configure the normal GI in 802.11a/g or short GI in 802.11n. The short GI reduces the extra cost and improves the transmission rate.
	Enable the MAC Protocol Data Unit (MPDU) aggregation function.	**80211n a-mpdu enable** By default, the MPDU aggregation function is enabled.	An 802.11 packet is sent as an MPDU, requiring channel competition and backoff and consuming channel resources. The 802.11n MPDU aggregation function aggregates multiple MPDUs into an aggregate MAC Protocol Data Unit (A-MPDU), so that N MPDUs can be transmitted through

Procedure		Command	Description
	Configure the maximum length of an A-MPDU.	**80211n a-mpdu max-length-exponent** *length-capability* By default, the maximum length of an A-MPDU is 65535 bytes.	one channel competition and backoff. This function saves the channel resources to be consumed for sending N-1 MPDUs. The MPDU aggregation function improves channel efficiency and 802.11 network performance.

----End

4.6.3.3 Binding a WMM Profile to a Radio Profile

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
radio-profile { id profile-id | name profile-name } *
```

The radio profile view is displayed.

Step 4 Run:

```
wmm-profile { id profile-id | name profile-name }
```

A WMM profile is bound to the radio profile.

By default, the WMM profile named **wmmf** is bound to the radio profile named **radiof**.

NOTE

A radio profile can be applied to a radio only after a WMM profile is bound to the radio profile.

----End

4.6.3.4 Creating a Security Profile

Context

As WLAN technology uses radio signals to transmit service data, service data can easily be intercepted or tampered by attackers when being transmitted on the open wireless channels. Security is critical to WLANs. You can create a security profile to configure security policies, which protect privacy of users and ensure data transmission security on WLANs.

A security profile provides four WLAN security policies: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, and WLAN Authentication and Privacy Infrastructure (WAPI). Each security policy has a series of security mechanisms, including the link authentication mechanism used to establish a wireless link, user authentication mechanism used when users attempt to connect to a wireless network, and data encryption mechanism used during data transmission.

If no security policy is configured during the creation of a security profile, the default authentication mode (open system authentication) is used. When a user searches for a wireless network, the user can connect to the wireless network without being authenticated.

For details on how to configure security policies, see **6 Configuration Guide - WLAN Security**.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
security-profile { id profile-id | name profile-name } *
```

A security profile is created and the security profile view is displayed.

By default, the security profile named **secf** exists in the system.

NOTE

After a security profile is created, the profile retains the default settings.

The profile name is mandatory when you create a security profile.

----End

4.6.3.5 Creating a Traffic Profile

Context

You can create a traffic profile to customize priority mapping and traffic policing functions for a WLAN.

- Priority mapping: If Wi-Fi Multimedia (WMM) is enabled on both a STA and an AP, the STA sends packets carrying the priority. To ensure end-to-end QoS and retain the priorities of packets during transmission, configure the device to map priorities of different packets.
- Traffic policing: To protect network resources, limit the rate of packets sent by a STA.

For details on how to configure parameters in a traffic profile, see **8.3.7 Configuring Priority Mapping** and **8.3.8 Configuring Traffic Policing**.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
traffic-profile (WLAN view) { id profile-id | name profile-name } *
```

A traffic profile is created.

By default, the traffic profile named **traf** exists in the system.

NOTE

After a traffic profile is created, the profile retains the default settings.

The profile name is mandatory when you create a traffic profile.

----End

4.6.3.6 Configuring a WLAN-BSS Interface

Context

When an AP receives 802.11 radio packets, it uses a WLAN-BSS interface to send the packets to the WLAN service module. The WLAN-BSS interface is configured with parameters such as the interface priority and authentication mode.

A WLAN-BSS interface is a virtual Layer 2 interface. Similar to a hybrid Layer 2 Ethernet interface, a WLAN-BSS interface has Layer 2 attributes and supports multiple Layer 2 protocols.

After creating and configuring a WLAN-BSS interface, bind a service set to the interface.

Procedure

- Configure a VLAN for a WLAN-BSS interface.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface wlan-bss *wlan-bss-number*

     A WLAN-BSS interface is created.
  3. Run:
     port hybrid pvid vlan *vlan-id*

     The default VLAN ID of a hybrid interface is configured.

     By default, no VLAN ID is configured for any WLAN-BSS interface.
  4. Run:
     port hybrid untagged vlan *vlan-id*

     The hybrid interface is added to a VLAN. Frames of the VLANs pass through the hybrid interface in untagged mode.

     By default, a hybrid interface is added to VLAN1 in untagged mode.

----End

4.6.3.7 Configuring a WLAN Service Set

Context

The administrator needs to deliver service parameters to an AP so that the AP can provide network access service for wireless users. A service set is a group of service parameters, including the SSID, whether to hide the SSID, maximum number of access users, and user association timeout period.

After configuring a service set, bind the service set to an AP radio. Then all the service parameters in the service set are applied to a VAP. Subsequently, the AP provides differentiated wireless services for users based on these service parameters.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
wlan

The WLAN view is displayed.

Step 3 Run:
service-set { **name** *service-set-name* | **id** *service-set-id* } *

A service set is created.

The service set name is mandatory when you create a service set.

Step 4 Configure mandatory parameters for the service set.

Procedure	Command	Description
Configure the SSID.	**ssid** *ssid*	By default, no SSID is set for a service set.

Step 5 Configure optional parameters for the service set.

NOTE

Only basic parameters are listed. Other parameters are configured in corresponding features.

Procedure		Command	Description
Set the maximum number of access users for the service set.		**max-user-number** *max-user-number*	By default, the maximum number of access users in a service set is 64.
Configure the user association timeout period.		**association-timeout** *association-timeout*	By default, the user association timeout period is 5 minutes.
Configure the AP to hide the SSID in a Beacon frame.		**ssid-hide** By default, the SSID is not hidden in a Beacon frame.	When creating a WLAN, configure an AP to hide the SSID of the WLAN to ensure security. Only the users that learn about the SSID can connect to the WLAN.
Configure dynamic ARP detection.	Enable dynamic ARP detection.	**dai enable** By default, dynamic ARP detection is disabled.	Dynamic ARP detection prevents man in the middle attacks, protects data of authorized user from being intercepted by unauthorized users during transmission, and protects an AP against CPU attacks.
	Set the ARP attack alarm threshold.	**arp-attack threshold** *threshold-value* By default, the ARP attack alarm threshold is 15.	

Procedure	Command	Description
Enable DHCP snooping on an AP.	**dhcp snooping** By default, DHCP snooping is disabled on an AP.	After DHCP snooping is enabled, if a STA that associates with an AP obtains an IP address through DHCP, the AP generates a dynamic binding table based on the STA IP information to prevent DHCP attacks (such as bogus DHCP server attacks and DHCP server DoS attacks). To check STA's IP address on the AP, enable DHCP snooping. **NOTE** If an STA associates with a device functioning as the DHCP server, and the STA works as an AP to connect other STAs, the STA cannot obtain an IP address. To prevent this problem, you are advised to disbale the DHCP probe function.
Enable IP source guard on an AP.	**ip source guard enable** By default, IP source guard is disabled on an AP.	IP source guard checks IP packets against the binding table to defend against source IP address spoofing attacks. **NOTE** IP source guard takes effect only when both the **dhcp snooping** and **ip source guard enable** commands are executed. If an offline STA goes online again on the AP enabled with DHCP snooping, you may not view the IP address of the STA. To solve this problem, enable IP source guard.

Procedure		Command	Description
Configure an AP to insert the Option 82 field in DHCP packets sent from a STA.	Enable an AP to insert the Option 82 field in DHCP packets sent from a STA.	**dhcp option82 insert enable** By default, an AP is disabled from inserting the Option 82 field in DHCP packets sent from a STA.	A STA obtains an IP address through DHCP after going online. When the DHCP Request packet sent by the STA reaches an AP, the AP inserts the Option 82 field in the packet to send the AP's MAC address or SSID to the DHCP server. According to the Option 82 field, the DHCP server can determine the AP through which the STA goes online.
	Configure the format of the remote-ID in the Option 82 field inserted in DHCP packets sent from a STA.	**dhcp option82 remote-id format** { **ap-mac** | **ap-mac-ssid** } The default format of remote-id in Option 82 carried in DHCP packets sent by STAs is **ap-mac**.	
Enable a specified VAP.		**service-mode enable**	By default, a VAP is enabled.
Enable the function of converting IPv4 multicast packets to IPv4 unicast packets.		**igmp-mode snooping** By default, the function of converting IPv4 multicast packets to IPv4 unicast packets is disabled.	After the function is enabled, an AP listens on Report and Leave packets to maintain multicast-to-unicast entries. When sending multicast packets to the client, the AP converts the multicast packets to unicast packets based on the multicast-to-unicast entries to improve multicast stream transmission efficiency.
Configure the type for a service set.		**type (service set view)**	By default, the type of a service set is service.

----End

4.6.3.8 Binding a Security Profile, a Traffic Profile, and an WLAN-BSS Interface to a Service Set

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
service-set { name service-set-name | id service-set-id } *
```

The service set view is displayed.

Step 4 Run:

```
security-profile { name profile-name | id profile-id }
```

A security profile is bound to the service set.

By default, no security profile is bound to a service set.

Step 5 Run:

```
traffic-profile { name profile-name | id profile-id }
```

A traffic profile is bound to the service set.

By default, no traffic profile is bound to a service set.

Step 6 Run:

```
wlan-bss wlan-bss-number
```

A WLAN-BSS interface is bound to the service set.

By default, no WLAN-BSS is bound to a service set.

NOTE

Each WLAN-BSS interface can be bound only to one service set.

----End

4.6.3.9 Configuring a Radio

Context

You can configure a radio to configure radio parameters on an AP radio module, including the antenna gain, power, channel, and number of available antennas.

After a VAP is created, the VAP inherits all the parameters configured in the radio bound to the VAP.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

interface wlan-radio *wlan-radio-number*

The radio view is displayed.

NOTE

If *wlan-radio-number* is set to 0/0/0, the 2.4-GHz radio interface view is displayed; if *wlan-radio-number* is set to 0/0/1, the 5-GHz radio interface view is displayed.

All types of APs support 2.4 GHz and 5 GHz radio interfaces except that the AP5010SN-GN, AP6010SN-GN, AP6310SN-GN, and AP7110SN-GN support only the 2.4-GHz radio interface.

Step 3 (Optional) Run:

radio enable

The radio is enabled.

By default, the radio is enabled.

Step 4 (Optional) Run:

available-antenna-number { **all** | *available-antenna-number* }

The number of available antennas on a radio is set. Excess antennas will then be shut down to save power.

By default, all antennas on a radio are available.

NOTE

The value of *available-antenna-number* must be equal to or smaller than the number of antennas on a radio.

Step 5 (Optional) Run:

power-level *power-level*

The power level of the radio is specified.

By default, the power level of a radio is 0, indicating full power. The actual power is determined by an AP type.

In automatic power mode, the AP can automatically adjust the radio power level based on the radio environment.

The power reduces by 1 dBm each time the AP power level increases by 1.

Step 6 (Optional) Run:

channel { **20mhz** | **40mhz-minus** | **40mhz-plus** } *channel*

A channel is configured for the radio.

By default, the bandwidth of a radio channel is 20 MHz.

To avoid signal interference, ensure that adjacent APs work in non-overlapping channels.

NOTE

40mhz-minus and **40mhz-plus** take effect only when the radio type is 802.11n.

Different countries support different wireless channels, You can run the **display ap configurable channel** command to check the channels supported by all the APs .

Step 7 (Optional) Run:

users-traffic-scheduler enable

The multi-user traffic scheduling function is enabled for the radio.

By default, the multi-user traffic scheduling function is disabled.

Step 8 (Optional) Run:

80211n mcs *mcs-value*

The modulation coding scheme (MCS) value is configured for the 802.11n radio.

By default, when one spatial stream exists, the MCS value is 7. When two spatial streams exist, the MCS value is 15. When there are three spatial streams, the MCS value is 23.

A larger MCS value indicates a higher transmission rate.

NOTE

This command takes effect only when the radio type is set to 802.11a/n, 802.11b/g/n, 802.11g/n, or 802.11n using the **radio-type** command.

Step 9 (Optional) Run:

multicast rate { **rate_1** | **rate_2** | **rate_5_5** | **rate_6** | **rate_9** | **rate_11** | **rate_12** | **rate_18** | **rate_24** | **rate_36** | **rate_48** | **rate_54** }

The rate is configured for wireless multicast packets of the radio.

NOTE

If no radio profile is bound to the radio, the multicast rate cannot be configured.

By default, the rate of wireless multicast packets is 11 Mbit/s for a 80211b, 80211bg, 80211bgn, or 80211n radio and 6 Mbit/s for radios of other types.

If you configure the maximum rate for a radio but the radio does not support the configured maximum rate, the configuration fails.

Step 10 (Optional) Run:

multicast mcs *mcs-value*

The MCS value is set for wireless multicast packets of the 802.11n radio.

NOTE

If no radio profile is bound to the radio, the MCS value of the radio packets cannot be configured.

By default, when there is one spatial stream, the MCS value is 7; when there are two spatial streams, the MCS value is 15; when there are three spatial streams, the MCS value is 23.

The MCS value and rate of multicast packets cannot be configured simultaneously.

----End

4.6.3.10 Binding a Radio Profile to a Wlan-Radio interface

Context

After a radio profile is bound to a radio, parameters defined in the radio profile are applied to the radio.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface wlan-radio wlan-radio-number
```

The radio interface view is displayed.

Step 3 Run:

```
radio-profile { id profile-id | name profile-name }
```

A radio profile is bound to the radio.

----End

4.6.3.11 Configuring a VAP and Delivering the VAP to an AP

Context

A VAP is a functional entity on an AP. You can create a VAP on a radio by binding a service set to the radio.

When a VAP is delivered to an AP, the service set parameters in the VAP are delivered to the AP. The AP then provides services for users based on the service set parameters.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface wlan-radio wlan-radio-number
```

The radio interface view is displayed.

Step 3 Run:

```
service-set { name service-set-name | id service-set-id } [ wlan wlan-id ]
```

A service set is bound to the VAP.

NOTE

Each service set can be bound only to one wlan-radio interface.

----End

4.6.3.12 (Optional) Configuring Channel Switching Without Service Interruption

Pre-Configuration Tasks

Before configuring channel switching without service interruption, complete the following task:

- Configuring basic WLAN services (For details, see **4 Configuration Guide - WLAN Service**.)

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
radio-profile { id profile-id | name profile-name } *
```

The specified radio profile view is displayed.

Step 4 Run:

```
channel-switch announcement enable
```

The AP is enabled to send an announcement after the channel is switched.

By default, the AP cannot send an announcement when the channel is switched.

Step 5 Run:

```
channel-switch mode continue-transmitting
```

Data transmission from the STA is configured to continue on the current channel when the channel is switched.

By default, data transmission from STAs continues on the current channel when the channel is switched.

NOTE

When the AP channel needs to be switched, the AP instructs the STA to switch the channel after a fixed number of Beacon intervals so that the STA and AP switch the channel simultaneously. This prevents the STA from reconnecting to the AP.

----End

4.6.3.13 Checking the Configuration

Procedure

- Run the **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check information about all WMM profiles or a specified WMM profile.
- Run the **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check information about all radio profiles or a specified radio profile.
- Run the **display binding radio-profile** { **id** *profile-id* | **name** *profile-name* } command to check the binding between an AP radio and a specified radio profile.
- Run the **display interface wlan-bss** [*wlan-bss-number*] command to check the running status and statistics about a specified WLAN-BSS interface.

- Run the **display actual channel-power interface** *interface* command to check the channel and power of a radio.
- Run the **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [**detail**] } command to check information about all security profiles or a specified security profile.
- Run the **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check information about all traffic profiles or a specified traffic profile.
- Run the **display radio config interface** *interface* command to check the configuration of a radio.
- Run the **display service-set** { **all** | **id** *service-set-id* | **name** *service-set-name* | **ssid** *ssid* } command to check information about all service sets or a specified service set.
- Run the **display vap** { **all** | **service-set** [**id** *service-set-id* | **name** *service-set-name*] } command to check VAP information.

----End

4.7 Maintaining WLAN Service

Maintaining WLAN Service includes monitoring APs, monitoring STAs and displaying neighbor information.

4.7.1 Monitoring APs

Context

To monitor AP running status after the basic WLAN service configuration is complete, run the following commands in any view.

Procedure

- Run the **display uncontrol ap** { **all** | **bssid** *bssid* } command to check unauthorized APs.
- Run the **display actual channel-power interface** *interface* command to check the channel and power of a specified radio.
- Run the **display ap around-ssid-list** command to check the neighbor SSID of a specified AP.

----End

4.7.2 Monitoring STAs

Context

After STAs successfully associate with the AP, you can run the following commands in any view to monitor the STA running status.

Procedure

- Run the **display statistics ssid** *ssid-name* **ap** *ap-id* **radio** *radio-id* command to check statistics about packets carrying a specified SSID on a specified AP radio.
- Run the **display statistics mac interface** *interface* command to check statistics about the MAC layer of a specified AP radio.
- Run the **display station assoc-info** { **sta** *mac-address* | **interface** *interface* [**service-set** *service-set-id*] } command to check access information about associated STAs.
- Run the **display station assoc-num** [**service-set** *service-set-id*] command to check the number of STAs in a specified service set or on a specified AP.
- Run the **display station statistics** [**sta** *mac-address*] command to check statistics on a specified STA, including the number of packets or bytes sent and received by the STA and rate of the STA. If an AP is specified, this command displays the number of STAs that associate with, disassociate from, and re-associate with the AP.
- Run the **display station status sta** *mac-address* command to check the status of a specified STA, including the SSID of the WLAN to which the STA connects, online duration, uplink signal noise ratio, and uplink receiving power of the STA.
- Run the **display statistics sta** *mac-address* command to check statistics about online STAs.

----End

4.7.3 Displaying Neighbor Information

Context

You can view neighbor information on a specified AP radio to learn about the AP location and neighbor relationship, helping locate unauthorized APs and plan the WLAN.

Procedure

- Run the **display neighbor interface** *wlan-radio-num* command to check neighbor information on a specified AP radio.

----End

4.7.4 Disabling Radios or VAPs as Scheduled

Context

In actual WLAN applications, the network administrator wants to disable radios or WLAN services in a specified period, ensuring security and reducing power consumption. You can disable the specified radio or VAP as scheduled.

This configuration is applicable to enterprises that want to disable WLAN services in a specified period for security or at midnight when the user service traffic volume is low.

Procedure

- Disable radios as scheduled.

1. Run:
   system-view

   The system view is displayed.
2. Run:
   wlan

   The WLAN view is displayed.
3. Run:
   auto-off service radio interface *wlan-radio* **start-time** *start-time* **end-time** *end-time*

   Radios are disabled as scheduled.

   By default, radios are not disabled as scheduled.

- Disable VAPs as scheduled.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     wlan

     The WLAN view is displayed.
  3. Run:
     auto-off service ess service-set id { { *start-id* [**to** *end-id*] } &<1-10> | **all** } **start-time** *start-time* **end-time** *end-time*

     VAPs are disabled as scheduled.

     By default, VAPs are not disabled as scheduled.

     NOTE
     The service set must be configured before this command is executed. For details, see **4.6.3.7 Configuring a WLAN Service Set**.

----End

4.8 Configuration Examples

This section provides WLAN service configuration examples, including networking requirements, configuration roadmap, and configuration procedure.

4.8.1 Example for Configuring the WLAN Service on a Small-Scale Network

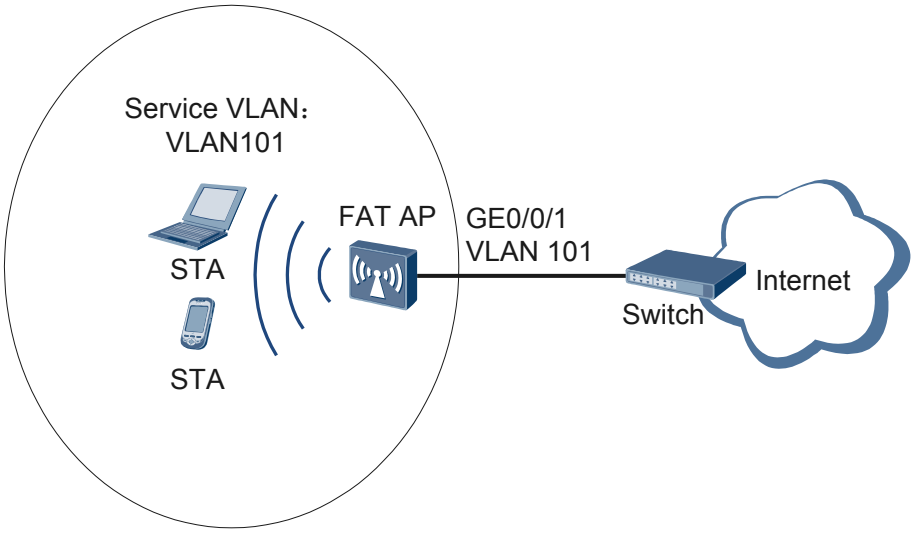
Networking Requirements

As shown in **Figure 4-14**, a Fat AP accesses the Internet through wired connections and connects to STAs wirelessly. An enterprise branch needs to deploy WLAN services for mobile office so that branch users can access the enterprise internal network from anywhere at any time.

The following requirements must be met:

- A WLAN named **test** is available.
- Branch users are assigned IP addresses on 192.168.11.0/24.

Figure 4-14 WLAN service configuration networking on a small-scale network



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the AP and upstream device to implement Layer 2 interconnection.
2. Configure the AP as a DHCP server to assign IP addresses to STAs from an IP address pool of an interface.
3. Configure AP system parameters, including the country code.
4. Configure a VAP so that STAs can access the WLAN.
   a. Configure a WMM profile and radio profile on the AP, retain the default settings of the WMM profile and radio profile, bind the WMM profile to the radio profile to enable STAs to communicate with the AP.
   b. Configure a WLAN-BSS interface so that radio packets can be sent to the WLAN service module after reaching the AP.
   c. Configure a security profile and traffic profile on the AP, retain the default settings of the security profile and traffic profile, configure a service set, bind the WLAN-BSS interface, security profile, and traffic profile to apply security policies and QoS policies to STAs.
   d. Configure a VAP and deliver VAP parameters to the AP so that STAs can access the Internet through the WLAN.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
```

```
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 6 Verify the configuration.

After the configuration is complete, run the **display vap service-set name test** command. The command output shows that the VAP has been created.

```
[AP] display vap service-set name test
  All VAP Information(Total-1):
  SS: Service-set     BP: Bridge-profile
  ------------------------------------------------------------------------
  Radio ID  SS ID  BP ID  WLAN ID  BSSID           Type
  0         1      -      1        DCD2-FC21-5D40  service
  ------------------------------------------------------------------------
  Total: 1
```

STAs discover the WLAN with SSID **test** and attempt to associate with the WLAN. You can run the **display station assoc-info interface wlan-radio0/0/0 service-set 1** command on the AP. The command output shows that the STAs associate with the WLAN **test**.

```
[AP] display station assoc-info interface wlan-radio0/0/0 service-set 1
  ------------------------------------------------------------------------------
  STA MAC          AP-ID   RADIO-ID  SS-ID   SSID
  ------------------------------------------------------------------------------
  14cf-9208-9abf   0       0         1        test
  ------------------------------------------------------------------------------
  Total stations: 1
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
```

```
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

4.9 FAQ

This section describes the FAQ of WLAN basic service.

4.9.1 What Are the Differences Between 802.11a/b/g/n Standards?

The following tables lists the differences between 802.11a/b/g/n standards in frequency band, compatibility, theoretical rate, and actual rate.

Protocol	Frequency Band	Compatibility	Theoretical Rate	Actual Rate
802.11a	5 GHz	NA	54 Mbit/s	About 22 Mbit/s
802.11b	2.4 GHz	NA	11 Mbit/s	About 5 Mbit/s
802.11g	2.4 GHz	Compatible with 802.11b	54 Mbit/s	About 22 Mbit/s
802.11n	2.4 GHz, 5 GHz	Compatible with 802.11a/b/g	300 Mbit/s (two spatial flows)	About 80 to 220 Mbit/s

4.9.2 What Are WLAN Reliability Features?

- WLAN service protection mechanisms: IP source guard (IPSG), DHCP snooping, statically configured MAC-IP table, and dynamic ARP inspection (DAI)
  - IPSG: This function defends against IP packet attacks by filtering out packets with forged IP addresses.
  - DHCP snooping: MAC-IP entries are dynamically generated and MAC-IP entries are reported to the AP. DHCP snooping protects WLAN servers and clients against attacks from ARP, IP, or DHCP packets with forged IP and MAC addresses.
  - Statically configured MAC-IP table: Only administrators can configure static IP addresses. Users using static IP addresses can connect to the network only after their MAC addresses are bound to the static IP addresses by administrators. Packets whose

MAC addresses and IP addresses do not match are considered as invalid packets and are discarded.

- DAI: It is an ARP security technology that intercepts ARP packets, discards ARP packets that do not match the DHCP snooping binding table, and records ARP attack logs. DAI can also limit the rate of ARP packets. DAI protects a device from ARP snooping attacks and prevents errors in the ARP cache table.

4.9.3 What Are the Differences Between HT20 and HT40, How Is the 11n 40 MHz Channel Is Partitioned, and What Are the Meanings of Plus and Minus?

The channel bandwidth in HT20 mode is 20 MHz, and the channel bandwidth in HT40 mode is 40 MHz. Two neighboring 20 MHz channels are bundled to form a 40 MHz channel. One channel functions as the main channel, and the other as the auxiliary channel. The main channel sends Beacon packets and data packets, and the auxiliary channel sends other packets. When the HT40 mode is used in the 2.4 GHz frequency band, there is only one non-overlapping channel. Therefore, you are not advised to use the HT40 mode in the 2.4 GHz frequency band.

Two neighboring 20 MHz channels can be bundled into a 40 MHz channel. If the center frequency of the main 20 MHz channel is higher than that of the auxiliary channel, 40MHz-plus is displayed; otherwise, 40MHz-minus is displayed. For example, if the center frequency 149 and the center frequency 153 reside on two 20 MHz channels, 149plus indicates that the two 20 MHz channels are bundled to form a 40 MHz channel.

4.9.4 What Is the Working Process of 802.11n Short GI?

When the radio chip sends data in OFDM modulation mode, it divides a frame into different data blocks to send. To ensure data transmission reliability, the guard interval (GI) is used between the data blocks to ensure that the receive end correctly parses each data block. During spatial propagation, the delay will occur on wireless signals at the receive end because of multipath. If subsequent data blocks are transmitted fast, these data blocks will interfere with the original data block. The GI is used to avoid such interference. The common GI is 800 us, whereas the short GI defined in the 802.11n standard is 400 us, which increases the physical connection rate by 11%.

4.9.5 Is the WLAN Rate the Upstream or Downstream Rate?

WLAN rate refers to the wireless rate of data transmissions between APs and STAs or between bridges and downstream nodes. Devices on both ends work in half-duplex mode, that is, they can only receive or send data at a time. The WLAN rate is the sum of upstream and downstream rates. Common users mainly use Internet access services to browse web pages, most of which is downstream traffic. In this case, the WLAN rate refers to the downstream rate.

4.9.6 What Are the Physical Rate, Theoretical Rate, and Actual Rate in the 802.11 Standard?

1. The WLAN physical rate is the physical layer rate of a radio interface, that is, the physical layer rate at which a radio interface keeps sending data. For example, the 802.11b physical rate is 11 Mbit/s and the 802.11g physical rate is 54 Mbit/s.
2. What is the relationship between the user theoretical rate and physical rate? The physical rate indicates only the performance of a radio interface, but users only care about how much bandwidth and rate they can use. The following uses the 802.11b standard as an example and assumes that a user packet is 1500 bytes. After a 32-byte header is prepended to the packet, the packet is longer than an Ethernet data frame. The checksum bits in 802.11b and Ethernet are both 4 bytes. The longest data frames (1536 bytes) are transmitted at the rate of 11 Mbit/s. The transmission time is [1536 (bytes) x 8 (bit)]/11 Mbit/s = 1117 microseconds.

   On the WLAN, a link code and PLCP header (exclusively used by WLAN) are prepended to a data frame. The transmission time of the link code and PLCP header is 192 microseconds. In addition to the interframe gap, a random period (delay offset) is required during the transmission of data frames on WLANs. In 802.11b, the average delay offset is 360 microseconds.

   On the WLAN, an ACK frame is received from the remote end each time a data frame is sent to confirm successful communication. The next data frame is sent only after the ACK frame is received. The total transmission time is 213 microseconds.

   The transmission time of a 1500-byte data frame includes the waiting time and ACK transmission time, equaling 1882 microseconds.

   1117 + 192 + 360 + 213 = 1882

   In this case, the theoretical maximum UDP throughput for 1500-byte data frames is 7.1 Mbit/s.
3. The preceding calculation result is based on the UDP model and 1500-byte frames. The actual usage scenarios are much complex than the preceding scenario. Additionally, the number of STAs also greatly affects AP performance. Therefore, the actual user rate is usually tested. In most cases, the actual rate of 802.11b can reach about 4.7 Mbit/s.

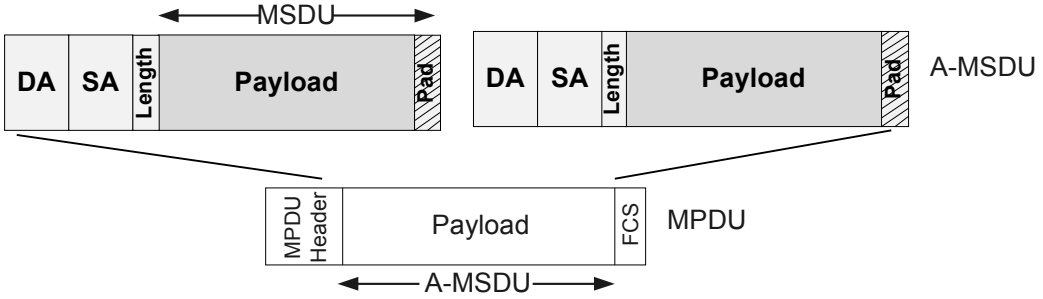
4.9.7 What Are the Implementations of 802.11n Frame Aggregation Technologies, MSDU and MPDU?

MSDU is short for MAC service data unit.

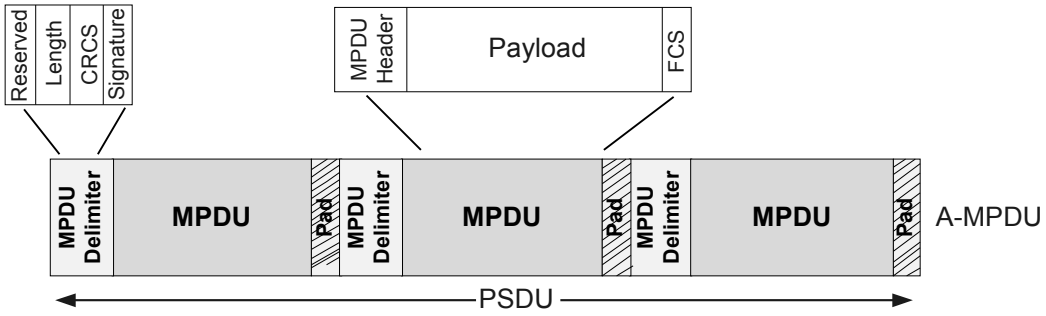
MPDU is short for MAC protocol data unit.

In wireless network security, an MSDU is an Ethernet packet. After integrity check MIC, framing, encryption, serial number assignment, CRC checksum, and MAC header are added to an MSDU, the MSDU becomes an MPDU. An MPDU is a data frame encapsulated using 802.11.

The A-MSDU technology aggregates multiple MSDUs into a large payload. Typically, when an AP or a STA receives an MSDU from the protocol stack, it tags the MSDU with an Ethernet header, called the A-MSDU subframe. The A-MSDU technology encapsulates multiple A-MSDU subframes into an MPDU, which is called an A_MPDU subframe, in accordance with the 802.11 protocol, as shown in the following figure:



The A-MPDU technology aggregates several A_MPDU subframes encapsulated in accordance with the 802.11 protocol. Sending several MPDUs at a time reduces the PLCP preamble and header required to send each 802.11 packet, increasing the system throughput, as shown in the following figure.



4.10 References

This section lists references of WLAN basic service.

The following table lists the references.

Document	Description	Remarks
RFC 5415	Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification	-
RFC 5416	Control and Provisioning of Wireless Access Points Protocol Binding for IEEE 802.11	-
IEEE 802.11	WLAN communication standard	-
IEEE 802.1x	Standard for Port-based Network Access Control	-

5 Configuration Guide - Radio Resource Management

About This Chapter

Radio resource management enables a WLAN to adapt to changes in the radio environment by dynamically adjusting radio resources. This improves service quality for wireless users.

5.10 Maintaining Radio Resource Management

Maintaining radio resource management includes displaying and clearing radio calibration statistics.

5.11 Configuration Examples

This section provides radio resource management configuration examples. Each configuration example includes networking requirements, configuration roadmap, and configuration procedure.

5.12 FAQ

This section provides answers to frequently asked questions about use of the radio resource management.

5.13 References

This section lists documentation related to radio resource management.

5.1 Introduction to Radio Resource Management

This section describes the definition, background, and functions of radio resource management.

Definition

Radio resource management enables APs to check the surrounding radio environment, dynamically adjust working channels and transmit power, and evenly distribute access users. This function helps reduce radio signal interference, adjust radio coverage, and enable a wireless network to quickly adapt to changes in the radio environment. With the radio resource management function, the wireless network can provide high service quality for wireless users and maintain an optimal radio resource utilization.

Purpose

WLAN technology uses radio signals (such as 2.4 GHz or 5 GHz radio waves) as transmission medium. Radio waves will attenuate when they are transmitted over air, degrading service quality for wireless users. Radio resource management enables a WLAN to adapt to changes in the radio environment by dynamically adjusting radio resources. This improves service quality for wireless users.

5.2 Principles

This section describes the implementation of radio resource management.

5.2.1 Radio Calibration

Overview

On a WLAN, operating status of APs is affected by the radio environment. For example, adjacent APs using the same working channel interfere with each other, and a large-power AP can interfere with adjacent APs if they work on overlapping channels. The radio calibration function can dynamically adjust channels and power of APs to ensure that the APs work at the optimal performance.

- Channel adjustment

  On a WLAN, adjacent APs must work on non-overlapping channels to avoid radio interference. For example, the 2.4 GHz frequency band is divided into 14 overlapping 20 MHz channels, as shown in **Figure 5-1**.

  NOTE

  For channels supported in different countries, see the *Country Code & Channel Compliance Table*. You can search and obtain this table at *http://support.huawei.com/enterprise*.

Figure 5-1 Channels in the 2.4 GHz frequency band

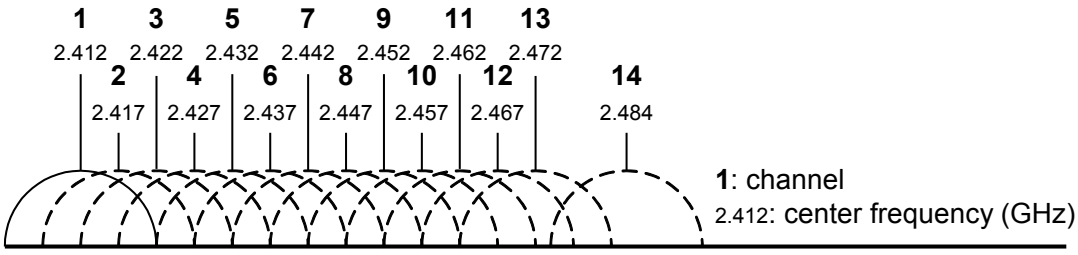
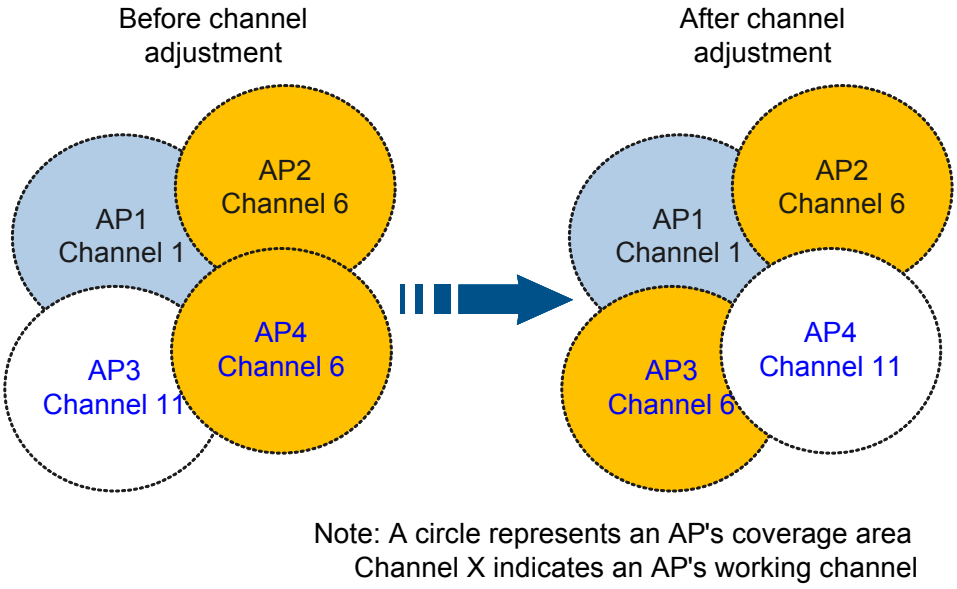


Figure 5-2 shows the channel distribution before and after channel adjustment. Before channel adjustment, both AP2 and AP4 use channel 6. After channel adjustment, AP4 uses channel 11 so that it does not interfere with AP2.

After channel adjustment, each AP is allocated an optimal channel to minimize or avoid adjacent-channel or co-channel interference, ensuring reliable data transmission on the network.

Figure 5-2 Channel adjustment



In addition to optimizing radio performance, channel adjustment can also be used for dynamic frequency selection (DFS). In some regions, radar systems work in the 5 GHz frequency band, which interfere with radio signals of APs working in the 5 GHz frequency band. The DFS function enables APs to automatically switch to other channels when they detect interference on their current working channels.

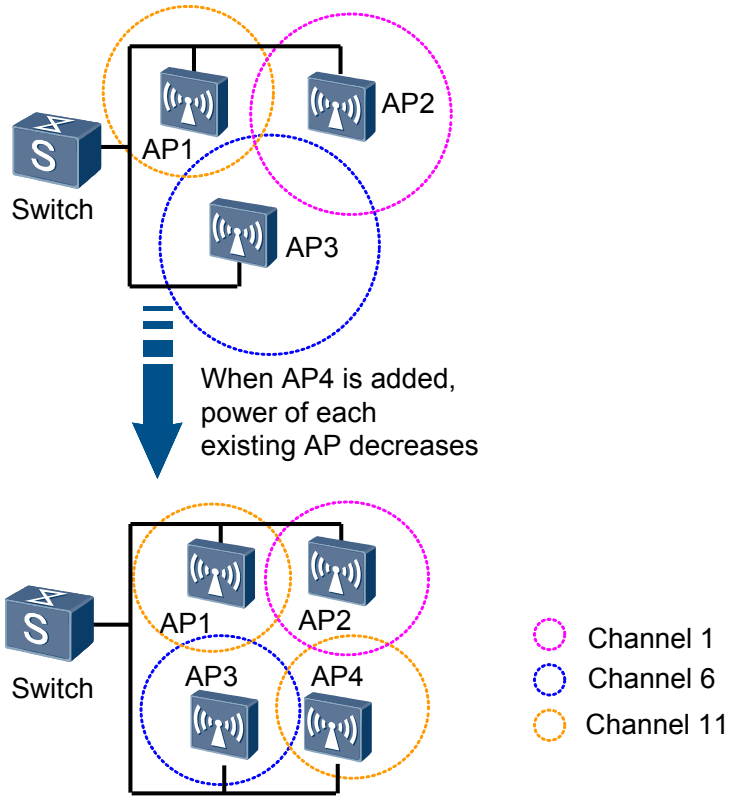
- Power adjustment

  An AP's transmit power determines its radio coverage area. APs with higher power have larger coverage areas. A traditional method to control the radio power is to set the transmit power to the maximum value to maximize the radio coverage area. However, a high transmit power may cause interference to other wireless devices. Therefore, an optimal power is required to balance the coverage area and signal quality.

The power adjustment function helps dynamically allocate proper power to APs according to the real-time radio environment.

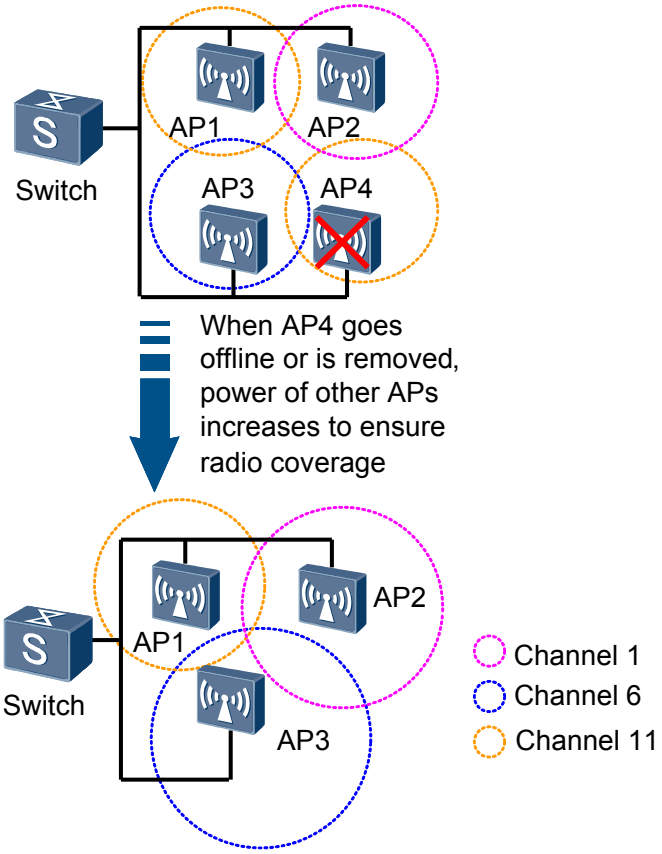
- When an AP is added to the network, the transmit power of neighboring APs decreases. As shown in **Figure 5-3**, the area of the circle around an AP represents the AP's transmit power and coverage area. When AP4 is added to the network, transmit power of each AP decreases automatically.

Figure 5-3 Transmit power of APs decreases



- When an AP goes offline or fails, power of neighboring APs increases, as shown in **Figure 5-4**.

Figure 5-4 Transmit power of APs increases



Implementation

Radio calibration is implemented as follows:

1. After radio calibration is enabled, the AP periodically implements neighbor probing.
2. The AP periodically implements neighbor probing.
3. The AC executes radio calibration algorithms to adjust AP power and working channels.

   The radio calibration algorithm includes the Dynamic Channel Allocation (DCA) algorithm and Transmit Power Control (TPC) algorithm.

Background Neighbor Probing

During global or partial radio calibration, an AP needs to listen on Beacon frames on each channel until all channels are probed. The probing process takes a long time and may cause service interruption.

If background neighbor probing is enabled before radio calibration, an AP determines whether to switch to another channel for neighbor probing every 300s based on the service traffic volume and threshold of user quantity. If the channel switching condition is met (the number of users or traffic on the channel does not exceed the threshold), the AP switches to the new channel. The AP then listens on Beacon frames on the new channel and saves the probing result. After 300 ms, the AP switches back to the original channel.

5.2.2 5G-Prior Access

When an AP and STA support both 5 GHz and 2.4 GHz frequency bands, the AP can request the STA to associate with the 5 GHz radio first.

Most STAs support both 5 GHz and 2.4 GHz frequency bands and they usually associate with the 2.4 GHz radio by default when connecting to the Internet. To connect to the 5 GHz radio, users must manually select the 5 GHz radio. When the 2.4 GHz frequency band has many users or severe interference, the 5 GHz frequency band can provide better access service for wireless users. The 5G-prior access function enable STAs to preferentially associate with the 5 GHz radio.

NOTE

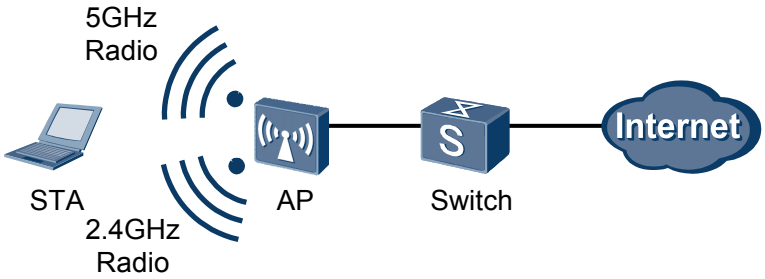
To implement the 5G-prior access function, an AP must have the same SSID and security policy on the 5 GHz and 2.4 GHz radios.

5G-prior access is implemented as follows:

As shown in **Figure 5-5**, when the AP receives a Probe Request frame from the STA, it checks the radio receiving the Probe Request frame. If the Probe Request frame is received by the 2.4 GHz radio, the AP does not return a Probe Response frame. If the Probe Request frame is received by the 5 GHz, the AP returns a Probe Response frame. Then the STA associates with the 5 GHz radio.

If only the 2.4 GHz radio receives 25 Probe Request frames continuously but the 5 GHz radio does not receive any Probe Request frame, the AP returns a Probe Response frame through the 2.4 GHz radio. Then the STA associates with the 2.4 GHz radio.

Figure 5-5 5G-prior access



5.3 Configuration Tasks Summary

This section describes the configuration task and logic of radio resource management.

Table 5-1 describes the radio resource management configuration tasks.

Table 5-1 Radio resource management configuration task summary

Configuration Task	Configuration	Description
Interference Detection	WLAN wireless channels are often affected by the radio environment, and the service quality is therefore degraded. If interference detection is configured, an monitoring AP can learn the radio environment in real time and report alarms in a timely manner. Interference detection can detect AP co-channel interference, AP adjacent-channel interference, and STA interference. ● AP co-channel interference: Two APs working in the same frequency band interfere with each other. For example, on a large-scale WLAN (a university campus network), different APs often use the same channel. When there are overlapping areas among these APs, co-channel interference exists, degrading network performance. ● AP adjacent-channel interference: Two APs with different center frequencies have overlapping areas, resulting in adjacent-channel interference. When APs are placed too close to each other or have strong signals, producing more noise and degrading network performance. ● STA interference: If there are many STAs	**5.5 Configuring Interference Detection**

Configuration Task	Configuration	Description
	that are managed by other APs around an AP, services of the STAs managed by the local AP may be affected.	
Background Neighbor Probing	Background neighbor probing helps you learn status of all channels on the WLAN network. If background neighbor probing is enabled, an AP determines whether to switch to another channel for neighbor probing every 10s based on the service traffic volume and threshold of user quantity. If the channel switching condition is met (the number of users or traffic on the channel does not exceed the threshold), the AP switches to the new channel. The AP then listens on Beacon frames on the new channel and saves the probing result. After 60 ms, the AP switches back to the original channel.	**5.6 Configuring Background Neighbor Probing**

Configuration Task	Configuration	Description
Radio Calibration	On a WLAN, operating status of APs is affected by the radio environment. For example, if adjacent APs work on overlapping channels, a large-power AP can interfere with adjacent APs. The radio calibration function can dynamically adjust channels and power of APs to ensure that the APs work at the optimal performance. The device uses global radio calibration and partial radio calibration as required. ● Global radio calibration: The AC dynamically allocates channels and power to all the APs. Generally, this calibration mode is used on a newly deployed WLAN. ● Partial radio calibration: The AC dynamically allocates channels and power to radios bound to specified radio profiles. Generally, this calibration mode is used in a scenario when a deployed WLAN needs to be maintained or optimized.	**5.7 Configuring Radio Calibration**

Configuration Task	Configuration	Description
5G-Prior or Normal Access	5G-prior is implemented on dual-band APs. When an AP and STA support both 5 GHz and 2.4 GHz frequency bands, the AP can request the STA to associate with the 5 GHz radio first. When the 2.4 GHz frequency band has many users or severe interference, the 5 GHz frequency band can provide better access service for wireless users. The 5G-prior access function enable STAs to preferentially associate with the 5 GHz radio.	**5.8 Configuring 5G-Prior or Normal Access**

5.4 Default Configuration

This section provides the default radio resource management configuration.

Table 5-2 Default radio resource management configuration

Parameter	Default Setting
Channel mode	Automatic mode
Power mode	Automatic mode
Radio calibration	Enabled
5G-Prior or Normal Access	Enabled
Interference detection	Disabled
Restriction of access from weak-signal STAs	Disabled
Restriction of access from low-rate STAs	Disabled
AP signal-strength-based power adjustment	Disabled

5.5 Configuring Interference Detection

After interference detection is configured, an alarm message is generated when the AP detects that co-channel interference, adjacent-channel interference, or STA interference exceeds the alarm threshold.

Pre-configuration Tasks

Before configuring interference detection, complete the following task:

- **Configuring WLAN Service**

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
radio-profile { id profile-id | name profile-name } *
```

The radio profile view is displayed.

Step 4 Run:

```
interference detect enable
```

Interference detection is enabled.

By default, interference detection is disabled.

Step 5 (Optional) Configure interference detection thresholds.

- Run:

  ```
  set ap common-frequency interference threshold threshold-value
  ```

  The alarm threshold for co-channel interference is set.

  By default, the alarm threshold for co-channel interference is 50%.

- Run:

  ```
  set ap adjacent-frequency interference threshold threshold-value
  ```

  The alarm threshold for adjacent-channel interference is set.

  By default, the alarm threshold for adjacent-channel interference is 50%.

- Run:

  ```
  set station interference threshold threshold-value
  ```

  The alarm threshold for STA interference is set.

  By default, the alarm threshold for STA interference is 32.

----End

Checking the Configuration

- Run the **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check the interference detection configuration.

5.6 Configuring Background Neighbor Probing

Background neighbor probing helps you learn status of all channels on the WLAN network.

Context

NOTE

Enabling background neighbor probing on APs may cause service interruption when Thinkpad x220 laptops use Windows7 operating system to connect to WLANs. You need to manually connect Thinkpad x220 laptops to WLANs.

Pre-configuration Tasks

Before configuring background neighbor probing, complete the following task:

- **Configuring Basic WLAN Services**

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
radio-profile { id profile-id | name profile-name } *
```

The radio profile view is displayed.

Step 4 Run:

```
background scanning enable
```

Background neighbor probing is enabled on APs.

By default, background neighbor probing is disabled on an AP.

Step 5 (Optional) Run:

```
channel scan-time time
```

The period during which the AP scans channels is configured.

The default period during which an AP scans channels is 60 ms.

This command applies to the WIDS, background neighbor probing, and terminal positioning functions.

Step 6 (Optional) Run:

```
channel scan-frequency time
```

The interval at which the AP scans channels is configured.

The default interval at which an AP scans channels is 10s.

This command applies to the WIDS, background neighbor probing, and terminal positioning functions.

Step 7 Run either of the following commands to configure the channel switching threshold for background neighbor probing.

- If background neighbor probing is based on the service volume,

  run the **background scanning service-threshold** *service-threshold-value* command to configure the service threshold for background neighbor probing.

  By default, the service threshold for background neighbor probing is 20%.

- If background neighbor probing is based on the user quantity,

  run the **background scanning client-threshold** *client-threshold-value* command to configure the user threshold for background neighbor probing.

  By default, the user threshold for background neighbor probing is 10.

----End

Verify the configuration.

- Run the **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check the background neighbor probing status in a specified radio profile.

5.7 Configuring Radio Calibration

Radio calibration can dynamically adjust channels and power of APs to ensure that the APs work at the optimal performance.

Context

NOTICE

- When radio calibration automatically triggers power adjustment, an alarm (WRFM_1.3.6.1.4.1.2011.6.139.3.24.1.19 hwRadioPowerChangedNotify) indicating that the radio power changes may be generated.

There are three radio calibration modes:

- Auto mode: The device implements radio calibration at certain intervals (the interval is specified by **interval** and the default interval is 60 minutes).

NOTE

In auto mode, the device continuously detects neighbors and updates neighbor information. When a radio calibration interval is reached, global radio calibration is triggered.

The auto mode applies to coverage hole compensation, coverage hole compensation reversal, and partial radio calibration.

- Manual mode: Radio calibration is not automatically implemented by the device but manually triggered through the **calibrate manual startup** command.
- Schedule mode: The device triggers radio calibration at the time specified by the parameter **time**.

The three modes cannot be configured simultaneously. You can choose any of the modes as required. **Schedule** mode is recommended, which can be specified using the **calibrate enable schedule time** *time-value* command. You can configure the device to perform radio calibration in off-peak hours, for example, between 00:00 am and 06:00 am.

NOTE

Global radio calibration is implemented on all APs.

Pre-configuration Tasks

Before configuring radio calibration, complete the following tasks:

- **Configuring Basic WLAN Services**
- Configuring the channel mode and power mode in a radio profile to auto for APs (for details, see **4.6.3.2 Configuring a Radio Profile**)

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
calibrate enable { auto [ interval interval-value ] | manual | schedule time time-value }
```

The radio calibration mode is configured.

The default radio calibration mode is **manual**.

Step 4 (Optional) Run:

```
calibrate policy { rogue-ap | load }
```

The radio calibration policy is created.

By default, no radio calibration policy is created. Radio calibration policies can be used together. You can run the command multiple times to configure different radio calibration policies according to service requirements.

Step 5 (Optional) Run:

calibrate sensitivity { **low** | **medium** | **high** }

The radio calibration sensitivity is set for the device.

By default, the radio calibration sensitivity of the device is set to **medium**.

Step 6 (Optional) Run:

calibrate { **2.4g** | **5g** } **20mhz channel-set** *channel-value*

The calibration channel set is configured.

If no calibration channel is configured, the device implements radio calibration on calibration channels that correspond to the global country code.

NOTE

When configuring a radio calibration set, avoid using radar channels.

Step 7 (Optional) Run:

scan { **2.4g** | **5g** } **20mhz channel-set** *channel-value*

The probe channel set is configured.

If no probe channel is configured, the device probes global calibration channels. If no global calibration channel is configured, the device probes calibration channels that correspond to the global country code.

Step 8 Run:

radio-profile { **id** *profile-id* | **name** *profile-name* }*

The radio profile view is displayed.

Step 9 (Optional) Run:

calibrate scan-cycle *scan-cycle-value*

The channel probe interval is set for radio calibration.

By default, the channel probe interval for radio calibration is 60s.

Step 10 (Optional) Run:

radio-type { **80211gn** | **80211b** | **80211bg** | **80211bgn** | **80211g** | **80211n** }

The radio profile type is configured.

By default, the radio type is 802.11b/g/n.

If the probe channels or calibration channels work at 5 GHz radio, you must specify the type of the radio calibration profile as 802.11a, 802.11n, or 802.11an.

Step 11 (Optional) Run:

calibrate-interval *calibrate-interval*

The radio calibration interval is set in the radio profile.

By default, the radio calibration interval is 720 minutes.

Step 12 Run:

calibrate enable

Radio calibration is enabled.

By default, radio calibration is enabled.

Step 13 Run:

```
quit
```

Return to the WLAN view.

----End

Check the Configuration

- Run the **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check the channel probe interval for radio calibration and radio calibration status in a specified radio profile.
- Run the **display radio config interface** *interface* command to check the radio calibration interval and radio calibration status on a specified AP radio interface.

Follow-up Procedure

To manually trigger radio calibration, set the radio calibration mode to **manual** and run the **calibrate manual startup** command. The device implements radio calibration only after the **calibrate manual startup** command is executed. Before the next radio calibration is triggered, the channel and power remain unchanged.

5.8 Configuring 5G-Prior or Normal Access

5G-prior access is enabled by default. That is, the AP requests STAs to preferentially associate with 5 GHz radios by default.

Pre-configuration Tasks

Before configuring 5G-prior or normal access, complete the following tasks:

- **Configuring WLAN Service**
- Ensuring that an AP supports both 5 GHz and 2.4 GHz frequency bands and has the same SSID and security policy on the 5 GHz and 2.4 GHz radios

NOTE

If STAs are configured to preferentially access the 5 GHz radio, ensure that the 5 GHz radio power is larger than the 2.4 GHz radio power on the AP to provide good access effect.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
access priority { 5g | normal }
```

The STA access mode is set to 5G prior or normal.

By default, the STA access mode is set to 5G prior.

----End

Checking the Configuration

- Run the **display ap** command to check the STA radio access mode.

5.9 Restricting Access from Weak-Signal or Low-Rate STAs

You can restrict access from weak-signal or low-rate STAs to prevent these STAs from accessing the WLAN.

Context

In the case of good WLAN signal coverage, you can restrict WLAN access from weak-signal or low-rate STAs at the edge of the coverage area.

NOTE

This function takes effect only for the new STAs that need to access a WLAN but not for the existing STAs that have connected to the WLAN.

Pre-configuration Tasks

Before restricting access from weak-signal or low-rate STAs, complete the following task:

- **Configuring WLAN Service**

Procedure

- Restrict access from weak-signal STAs.
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     wlan
     ```
     The WLAN view is displayed.
  3. Run:
     ```
     radio-profile { id profile-id | name profile-name } *
     ```
     The radio profile view is displayed.
  4. Run:
     ```
     sta-access-limit signal-strength enable
     ```
     Restriction of access from weak-signal STAs is enabled.

     By default, restriction of access from weak-signal STAs is disabled.
  5. Run:
     ```
     sta-access-limit signal-strength threshold threshold-value
     ```

The lower threshold for the STA signal strength is set.

By default, the lower threshold for the STA signal strength is -80 dBm.

- Restrict access from low-rate STAs.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     wlan

     The WLAN view is displayed.
  3. Run:
     radio-profile { **id** *profile-id* | **name** *profile-name* } *

     The radio profile view is displayed.
  4. Run:
     sta-access-limit rate enable

     Restriction of access from low-rate STAs is enabled.

     By default, restriction of access from low-rate STAs is disabled.
  5. Run:
     sta-access-limit rate rate-value { **rate_1** | **rate_2** | **rate_5_5** | **rate_6** | **rate_9** | **rate_11** | **rate_12** | **rate_18** | **rate_22** | **rate_24** | **rate_33** | **rate_36** | **rate_48** | **rate_54** }

     The lower threshold for the STA access rate is set.

     By default, the lower threshold for the STA access rate is 11 Mbit/s.

----End

Checking the Configuration

- Run the **display radio-profile** { **id** *profile-id* | **name** *profile-name* } command to check the configuration of restriction of access from weak-signal or low-rate STAs.

5.10 Maintaining Radio Resource Management

Maintaining radio resource management includes displaying and clearing radio calibration statistics.

5.10.1 Displaying Radio Calibration Statistics

Context

During radio calibration, run the following command to view radio calibration statistics.

Procedure

- Run the **display statistics calibrate interface** *wlan-radio-num* command to check radio calibration statistics.

----End

5.10.2 Clearing Radio Calibration Statistics

Context

Before re-collecting radio calibration statistics, run the **reset statistics calibrate** command to clear the existing statistics.

NOTICE

Radio calibration statistics cannot be restored after they are cleared. Confirm your operation before running the command.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface wlan-radio wlan-radio-number
```

The radio interface view is displayed.

Step 3 Run:

```
reset statistics calibrate
```

Clear radio calibration statistics.

----End

5.11 Configuration Examples

This section provides radio resource management configuration examples. Each configuration example includes networking requirements, configuration roadmap, and configuration procedure.

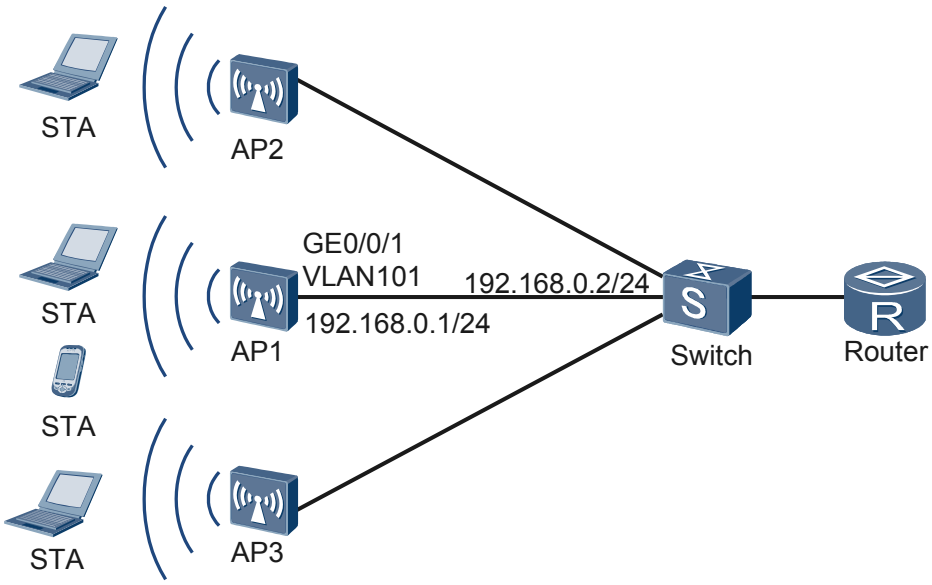
5.11.1 Example for Configuring Radio Calibration for APs

Networking Requirements

As shown in **Figure 5-6**, a WLAN containing three APs (AP1, AP2, and AP3) is deployed on the campus network. The three APs interfere with each other, so the WLAN network performance is low.

Users expect that three APs can automatically adjust their channels and power to reduce interference and achieve optimal WLAN performance.

Figure 5-6 Networking for configuring radio calibration for APs



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic WLAN services to ensure that users can access the Internet through WLAN.
2. Configure radio calibration for APs to enable the APs to adjust channels and power so that the APs work at optimal performance.

Procedure

Step 1 Configure AP1 to communicate with the upstream device.

NOTE

Configure AP1's uplink interface to transparently transmit packets of service VLANs and communicate with the upstream network device.

Add AP1's uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP1
[AP1] vlan batch 101
[AP1] interface gigabitethernet 0/0/1
[AP1-GigabitEthernet0/0/1] port link-type trunk
```

```
[AP1-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP1-GigabitEthernet0/0/1] quit
```

Configure a default route with the next hop address 192.168.0.2 on AP1.

```
[AP1] ip route-static 0.0.0.0 0 192.168.0.2
```

Step 2 Configure AP1 as a DHCP server to allocate IP addresses to STAs.

Configure the DHCP server to allocate IP addresses to STAs from the IP address pool on VLANIF 101.

```
[AP1] dhcp enable
[AP1] interface vlanif 101
[AP1-Vlanif101] ip address 192.168.0.1 24
[AP1-Vlanif101] dhcp select interface
[AP1-Vlanif101] dhcp server excluded-ip-address 192.168.0.2
[AP1-Vlanif101] quit
```

Step 3 Configure system parameters for AP1.

Configure the country code for AP1.

```
[AP1] wlan global country-code cn
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP1] wlan
[AP1-wlan-view] wmm-profile name wmm id 1
[AP1-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio**, set the radio type to 802.11an, and bind the WMM profile **wmm** to the radio profile.

```
[AP1-wlan-view] radio-profile name radio id 1
[AP1-wlan-radio-prof-radio] wmm-profile name wmm
[AP1-wlan-radio-prof-radio] radio-type 80211an
Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP1-wlan-radio-prof-radio] quit
[AP1-wlan-view] quit
```

Create the WLAN-BSS interface 1.

```
[AP1] interface wlan-bss 1
[AP1-Wlan-Bss1] port hybrid pvid vlan 101
[AP1-Wlan-Bss1] port hybrid untagged vlan 101
[AP1-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP1] wlan
[AP1-wlan-view] security-profile name security id 1
[AP1-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP1-wlan-view] traffic-profile name traffic id 1
[AP1-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP1-wlan-view] service-set name test id 1
[AP1-wlan-service-set-test] ssid test
```

```
[AP1-wlan-service-set-test] wlan-bss 1
[AP1-wlan-service-set-test] security-profile name security
[AP1-wlan-service-set-test] traffic-profile name traffic
[AP1-wlan-service-set-test] quit
[AP1-wlan-view] quit
```

Step 5 Configure a VAP.

```
[AP1] interface Wlan-Radio0/0/1
[AP1-Wlan-Radio0/0/1] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP1-Wlan-Radio0/0/1] service-set name test
[AP1-Wlan-Radio0/0/1] quit
```

Step 6 Configure radio calibration.

Set the radio calibration mode to **schedule**, configure the device to start radio calibration at 3:00 a.m. every day, and set the radio calibration policy to **load**.

```
[AP1-wlan-view] calibrate enable schedule time 03:00:00
[AP1-wlan-view] calibrate policy load
```

Enable radio calibration in the radio profile view. By default, radio calibration is enabled in the radio profile view.

Step 7 Verify the configuration.

STAs discover the WLAN with the SSID **test** and attempt to associate with the WLAN. You can run the **display station assoc-info interface wlan-radio0/0/1 service-set 1** command on AP1. The command output shows that the STAs associate with the WLAN **test**.

```
[AP1-wlan-view] display station assoc-info interface wlan-radio0/0/1 service-set 1
  ------------------------------------------------------------------------------
  STA MAC          AP-ID   RADIO-ID  SS-ID   SSID
  ------------------------------------------------------------------------------
  14cf-9208-9abf   1       1         1        test
  ------------------------------------------------------------------------------
  Total stations: 1
```

You can run the **display statistics calibrate interface wlan-radio0/0/1** command on AP1 to check radio calibration statistics on AP1.

```
[AP1-wlan-view] display statistics calibrate interface wlan-radio0/0/1
  ------------------------------------------------------------------------
   Signal environment deterioration :1
   Power calibration                :1
   Channel calibration              :0
  ------------------------------------------------------------------------
```

NOTE

The procedure for configuring radio calibration on AP2 and AP3 is similar to that on AP1 and is not provided here.

----End

Configuration Files

- Configuration file of AP1

```
#
 sysname AP1
#
vlan batch 101
#
dhcp enable
```

```
#
interface Vlanif101
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
 dhcp server excluded-ip-address 192.168.0.2
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
ip route-static 0.0.0.0 0 192.168.0.2
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 calibrate enable schedule time 03:00:00
 calibrate policy load
 radio-profile name radio id 1
  radio-type 80211an
  wmm-profile id 1
#
interface Wlan-Radio0/0/1
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

5.12 FAQ

This section provides answers to frequently asked questions about use of the radio resource management.

5.12.1 Where Are Interference Sources in WLAN and How Is the Interference Strength?

Two frequency bands are available on WLANs: 2.4 GHz and 5 GHz.

The 2.4 GHz frequency band is the Industrial, Scientific, and Medical (ISM) open frequency band. Interference sources in the 2.4 GHz frequency band include cordless phones, baby monitors, microwave ovens, wireless cameras, bluetooth devices, infrared sensors, and fluorescent light ballasts.

Compared with 2.4 GHz frequency band, 5 GHz frequency band has fewer interference sources and more devices begin to use the 5 GHz frequency band, such as cordless phones, radars, wireless sensors, and digital satellites.

In most cases, microwave ovens work at the frequency band ranging from 2.4 to 2.5 GHz, which overlaps the 2.4 GHz frequency band used by WLAN devices. In addition, the power of microwave ovens ranges between 800 W and 2000 W, which is much higher than the transmit

power of APs and STAs. Even though interference shielding is performed, microwave ovens still have severe interference on WLAN devices. Microwave ovens greatly reduce the throughput of WLAN devices if they are within a distance shorter than 8 meters around WLAN devices.

The power of cordless phones is about 3 W, which is higher than the AP's transmit power. According to the test analysis on the interference caused by cordless phones on WLAN devices, when the distance between cordless phones and APs (or STAs) is within 1 meter, interference increases significantly. When the distance is shorter than 0.5 meter, WLAN devices are even offline and the cordless phone voice is not clear. Therefore, you are advised to deploy cordless phones more than 2 meters away from APs or STAs.

The transmit power of wireless cameras ranges from 500 to 1000 MW. In indoor scenarios, wireless cameras may affect the WLAN network but have lighter interference than microwave ovens and cordless phones. Therefore, you are advised to deploy wireless cameras far away from WLAN devices during WLAN planning.

Bluetooth devices use the frequency hopping spread spectrum (FHSS) technology and 1 MHz channel bandwidth. If a bluetooth device is sending data at the frequency band overlapping with a WLAN channel that is being monitored by a WLAN device, the WLAN device selects a random backoff period. During this period, the bluetooth device changes to work at a non-overlapping channel, allowing the WLAN device to send data. Therefore, bluetooth devices have small interference on WLAN devices. This interference can be ignored during WLAN planning.

5.13 References

This section lists documentation related to radio resource management.

The following table lists the reference for this feature.

Document	Description	Remarks
IEEE 802.11k	Radio Resource Measurement of Wireless LANs	-

6 Configuration Guide - WLAN Security

About This Chapter

As wireless local area network (WLAN) technology uses radio signals to transmit service data, service data can easily be intercepted or tampered by attackers when being transmitted on the open wireless channels. WLAN security can be configured to protect WLAN networks against attacks and secure information and services of authorized users.

This section lists references of WLAN security.

6.1 Introduction to WLAN Security

This section describes the definition and Purpose of WLAN Security.

Definition

WLAN security involves the following:

- Perimeter security: An 802.11 network is subject to threats from unauthorized APs and users, ad-hoc networks, and denial of service (DoS) attacks. A wireless intrusion detection system (WIDS) can detect unauthorized users and APs. A wireless intrusion prevention system (WIPS) can protect an enterprise network against unauthorized access from wireless networks.
- User access security: Link authentication, access authentication, and data encryption are used to ensure validity and security of user access on wireless networks.
- Service security: This feature protects service data of authorized user from being intercepted by unauthorized users during transmission.

Purpose

WLAN networks are easy to deploy and expand, flexible, and cost-effective. As WLAN technology uses radio signals to transmit service data, service data can easily be intercepted or tampered by attackers when being transmitted on the open wireless channels. Security has become a major factor that hinders WLAN technology development.

WLAN technology can provide the following mechanisms to guarantee data security for wireless users:

- WIDS and WIPS mechanisms that detect and defend against intrusion from unauthorized users
- Security policies for wireless users, including link authentication, access authentication, and data encryption
- Security mechanisms for wireless services, such as user isolation

6.2 Perimeter Security Principles

This section describes the implementation of WIDS and WIPS.

6.2.1 Wireless Intrusion Detection

Monitor APs can be configured on a network to prevent intrusion to the network. When configured with the intrusion detection function, monitor APs periodically listen on wireless signals. The AP can obtain information about wireless devices and take countermeasures on unauthorized devices.

Before configuring intrusion detection on an AP, configure the working mode of the AP.

An AP supports three working modes: access mode, monitor mode, and hybrid mode:

- Access mode: If background neighbor probing is not enabled on an AP, the AP only transmits data of wireless users and does not monitor wireless users on the network. If background neighbor probing is enabled, the AP can not only transmit data of wireless users but also scan wireless devices and listen on all 802.11 frames on wireless channels.
- Monitor mode: An AP scans wireless devices on the network and listens on all 802.11 frames on wireless channels. In this mode, all WLAN services on the AP are disabled and the AP cannot transmit data of wireless users.
- Hybrid mode: An AP can monitor wireless devices while transmitting data of wireless users.

  NOTE

  An AP can implement the WIDS or WIPS function only when it works in monitoring or hybrid mode.

Intrusion detection consists of two phases: wireless device identification and rogue device identification.

Wireless Device Identification

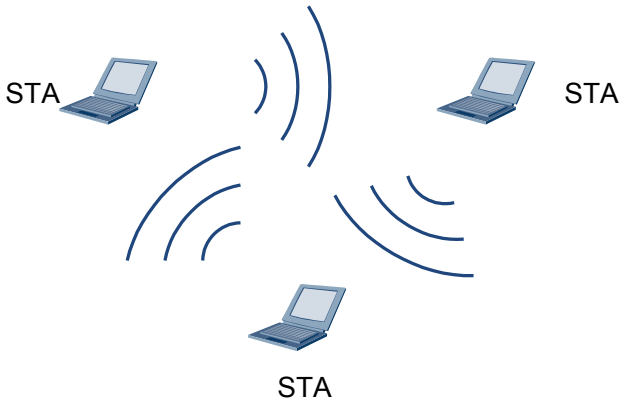
An AP working in monitoring or hybrid mode can identify types of neighboring wireless devices according to detected 802.11 frames. The wireless device identification process is as follows:

1. The AP working mode is set to monitoring or hybrid.
2. The AP listens on frames sent from neighboring wireless devices to collect information about wireless devices. The AP determines frame types and device types according to MAC headers in received 802.11 MAC frames. For details about the 802.11 MAC frame format, see **4.2.2 802.11 Standards**.

   An AP can identify the following device types: AP, STA, wireless bridge, and ad-hoc device.

   - Wireless bridge: an AP provides wireless distribution system (WDS) service. For details about WDS, see WDS Configuration.
   - Ad-hoc device: a device on an ad-hoc network. An ad-hoc network is a temporary wireless network composed of several devices with wireless network adapters, as shown in **Figure 6-1**.

   Figure 6-1 Ad-hoc network

An AP identifies device types in the following way:

- When receiving a Probe Request, Association Request or Reassociation Request frame, the AP determines whether the sender is an ad-hoc device or STA according to the network type specified in the Frame Body field of the 802.11 MAC frame.
  - Ad-hoc: The network type is independent basic service set (IBSS).
  - STA: The network type is basic service set (BSS).
- When receiving a Beacon, Probe Response, Association Response, or Reassociation Response frame, the AP determines whether the sender is an ad-hoc device or AP according to the network type specified in the Frame Body field of the 802.11 MAC frame.
  - Ad-hoc: The network type is IBSS.
  - AP: The network type is BSS.
- The AP listens on all 802.11 data frames and checks the DS fields of the data frames to determine whether the sender is an ad-hoc device, wireless bridge, STA, or AP.
  - Ad-hoc device: In the Frame Control field of the 802.11 MAC header, both the To DS and From DS fields are 0.
  - Wireless bridge: In the Frame Control field of the 802.11 MAC header, both the To DS and From DS fields are 1.
  - STA: In the Frame Control field of the 802.11 MAC header, the To DS field is 1 and the From DS field is 0.
  - AP: In the Frame Control field of the 802.11 MAC header, the To DS field is 0 and the From DS field is 1.

Rogue Device Identification

- Interference AP: an AP that works on the same channel or adjacent channels with the monitor AP.
- Rogue AP: an AP not on the SSID whitelist
- Rogue STA: a STA that does not go online on the local AP
- Rogue bridge: a WDS device not managed by the local AP
- Rogue Ad hoc device: all Ad hoc devices detected

NOTE

An AP can take a countermeasure on rogue devices to prevent them from accessing the network. For details about the countermeasure, see **6.2.2 Wireless Intrusion Prevention**

6.2.2 Wireless Intrusion Prevention

An AC can prevent wireless intrusion of three types of unauthorized devices:

- Rogue AP

  The monitoring AP uses the rogue AP's identity information to broadcast a Deauthentication frame. After STAs that associate with the rogue AP receive the Deauthentication frame, they disassociate from the rogue AP. This countermeasure prevents STAs from associating with rogue APs.

NOTE

- Deauthentication frames are used to terminate established wireless links. Either an AP or a STA can send a Deauthentication frame to terminate the current link.
- Currently, an AP supports only countermeasure on rogue APs that have the same SSIDs.

- Unauthorized STA

  The monitoring AP uses the unauthorized STA's identity information to unicast a Deauthentication frame. After the AP with which the unauthorized STA associates receives the Deauthentication frame, the AP disassociates from the unauthorized STA. This countermeasure prevents APs from associating with unauthorized STAs.

- Ad hoc device

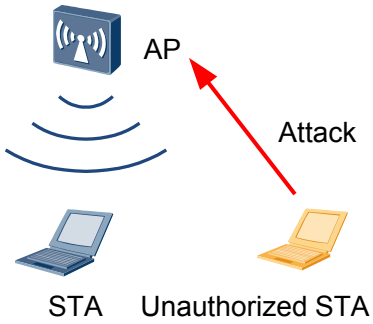
  The monitoring AP uses the ad hoc device's identity information (BSSID and MAC address of the device) to unicast a Deauthentication frame. After the STAs that associate with the ad hoc device receive the Deauthentication frame, the STAs disassociate from the ad hoc device. This countermeasure prevents STAs from associating with ad hoc devices.

6.2.3 Attack Detection

On small- and medium-scale WLANs, the attack detection function can be enabled to detect flooding attacks, weak initialization vector (IV), and spoofing attacks. This function enables an AP to add attackers to the dynamic blacklist and send alarms to alert administrators.

Flooding Attack Detection

Figure 6-2 Flooding attack



In **Figure 6-2**, the AP receives a large number of management packets or empty data packets that have the same type and source MAC address within a short period. This is a flooding attack. As a result, the system is busy processing these attack packets and cannot process packets from authorized STAs.

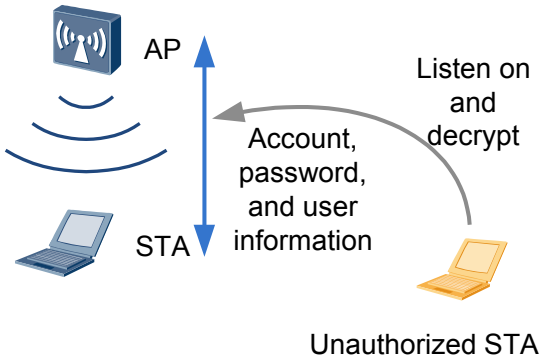
Flooding attack detection allows an AP to keep monitoring the traffic volume of each STA to prevent flooding attacks. When the traffic of a STA exceeds the allowed threshold (for example, the AP receives more than 100 packets from a STA within 1 second), the AP considers that the STA will flood packets and reports an alarm. If a dynamic blacklist is configured, the AP adds the detected attack device to the dynamic blacklist. Before the dynamic blacklist ages, the AP discards all the packets from the attack device to prevent the network from a flooding attack.

An AP can detect flooding attacks of the following packets:

- Authentication Request
- Deauthentication
- Association Request
- Disassociation
- Reassociation Request
- Probe Request
- Action
- EAPOL Start
- EAPOL-Logoff
- 802.11 Null
- 802.11 Null QoS

Weak IV Detection

Figure 6-3 Weak IV

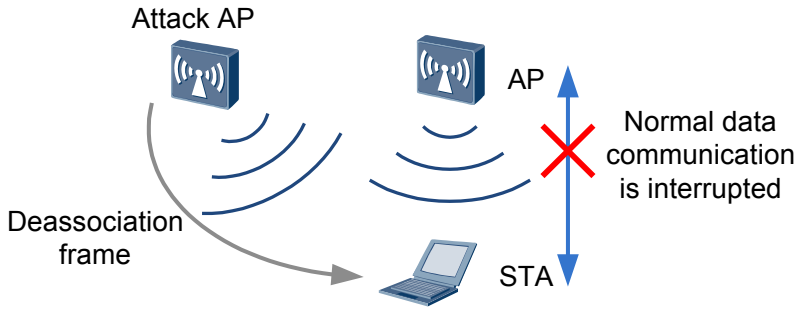


In **Figure 6-3**, when WEP encryption is used, a STA uses a 3-byte IV and a fixed shared key to encrypt each packet to be sent so that the same shared key generates different encryption effects. If the STA uses the weak IV (the first byte of the IV ranges from 3 to 15 and the second byte is 255), attackers can easily decrypt the shared key and access network resources because the IV of the packet sent by the STA is sent in plain text as one part of the header.

Weak IV detection identifies the IV of each WEP packet to prevent attackers from decrypting the shared key. When the AP detects a packet carrying the weak IV, the AP sends an alarm so that users can use other security policies to prevent STAs from using the weak IV for encryption.

Spoofing Attack Detection

Figure 6-4 Spoofing attack



In **Figure 6-4**, an attacker (a rogue AP or malicious user) forges an authorized user to send spoofing attack packets to STAs, which then fail to go online. This is a spoofing attack, which is also called man-in-the-middle attack. Spoofing attack packets includes broadcast Disassociation packets and Deauthentication packets.

After the spoofing attack detection function is enabled, an AP checks whether the source MAC address of a packet is its MAC address when receiving either of the two types of packets. If so, the WLAN is under the spoofing attack of Disassociation or Deauthentication packets.

6.2.4 Defense Against Brute Force Attacks on PSK

The brute force method is to search for a password by trying to use all possible password combinations. This method is also called the exhaustive attack method. For example, a 4-digit password that contains only digits may have a maximum of 10,000 combinations. The password can be decrypted after a maximum of 10,000 attempts. In theory, the brute force method can decrypt any password. The only problem is how to shorten the time used to decrypt a password. When a WLAN uses WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key as the security policy, attackers can use the brute force method to decrypt the password.

Defense against brute force attacks on PSK can prolong the time used to decrypt passwords to improve password security. An AP checks whether the number of key negotiation attempts during WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key authentication exceeds the configured threshold. If so, the AP considers that a user is using the brute force method to decrypt the password. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist, discards all the packets of the user until the dynamic blacklist entry ages.

6.3 User Access Security Principles

This section describes the implementation of WLAN security policy, STA whitelist and blacklist.

6.3.1 Security Policy

Four WLAN security policies are available: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, WLAN Authentication and Privacy Infrastructure (WAPI). Each security policy has a series of security mechanisms, including the link authentication mechanism

used to establish a wireless link, user authentication mechanism used when users attempt to connect to a wireless network, and data encryption mechanism used during data transmission.

6.3.1.1 WEP

Wired Equivalent Privacy (WEP), defined in IEEE 802.11, is used to protect data of authorized users from tampering during transmission on a WLAN. The WEP protocol uses the RC4 algorithm that encrypts data using a 64-bit, 128-bit, or 152-bit encryption key. An encryption key contains a 24-bit initialization vector (IV) generated by the system, so the length of key configured on the WLAN server and client is 40-bit, 104-bit, or 128-bit. WEP uses a static encryption key. That is, all STAs associating with the same SSID use the same key to connect to the wireless network.

A WEP security policy defines a link authentication mechanism and a data encryption mechanism.

Link authentication mechanisms include open system authentication and shared key authentication. For details about link authentication, see "Link Authentication" in **4.2.4 STA Access**.

- If open system authentication is used, data is not encrypted during link authentication. After a user goes online, service data can be encrypted by WEP or not, depending on the configuration.
- If shared key authentication is used, the WLAN client and server complete key negotiation during link authentication. After a user goes online, service data is encrypted using the negotiated key.

6.3.1.2 WPA/WPA2

WEP shared key authentication uses the RC4 symmetric stream cipher to encrypt data. This authentication method requires the same static key pre-configured on the server and client. Both the encryption mechanism and encryption algorithm can bring security risks to the network. The Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) to overcome WEP defects before more secure policies are provided in 802.11i. WPA still uses the RC4 algorithm, but it uses an 802.1x authentication framework and supports Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) and EAP-Transport Layer Security (EAP-TLS) authentication, and defines the Temporal Key Integrity Protocol (TKIP) encryption algorithm. Later, 802.11i defined WPA2. Different from WPA, WPA2 uses a more secure encryption algorithm: Counter Mode with CBC-MAC Protocol (CCMP).

Both WPA and WPA2 support 802.1X authentication and TKIP/CCMP encryption algorithm, ensuring better compatibility. The two protocols provide almost the same security level and their difference lies in the protocol packet format.

The WPA/WPA2 security policy involves four phases: link authentication, access authentication, key negotiation, and data encryption.

Link Authentication

Link authentication can be completed in open system authentication or shared key authentication mode. For details, see "Link Authentication" in **4.2.4 STA Access**.

WPA and WPA2 support only open system authentication.

Access Authentication

WPA and WPA2 have an enterprise edition and a personal edition.

- WPA/WPA2 enterprise edition (WPA/WPA2-802.1X authentication): uses a RADIUS server and the EAP protocol for authentication. Users provide authentication information, including the user name and password, and are authenticated by an authentication server (generally a RADIUS server).

  Large-scale enterprise networks usually use the WPA/WPA2 enterprise edition.

  NOTE

  For details about 802.1X authentication, see 802.1X Authentication in the *Configuration Guide - Security*.

  WPA/WPA2 implements 802.1X authentication using EAP-TLS and EAP-PEAP. **Figure 6-5** and **Figure 6-6** show EAP-TLS 802.1X authentication and EAP-PEAP 802.1X authentication processes.

  Figure 6-5 EAP-TLS 802.1X authentication

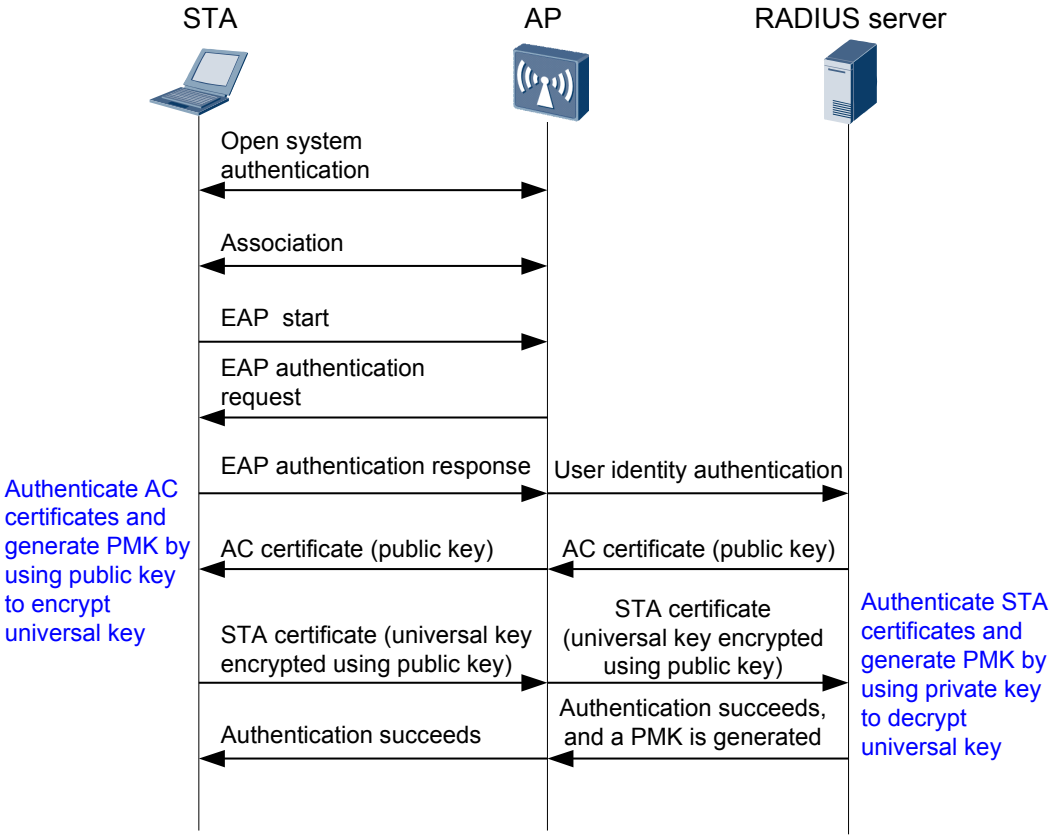
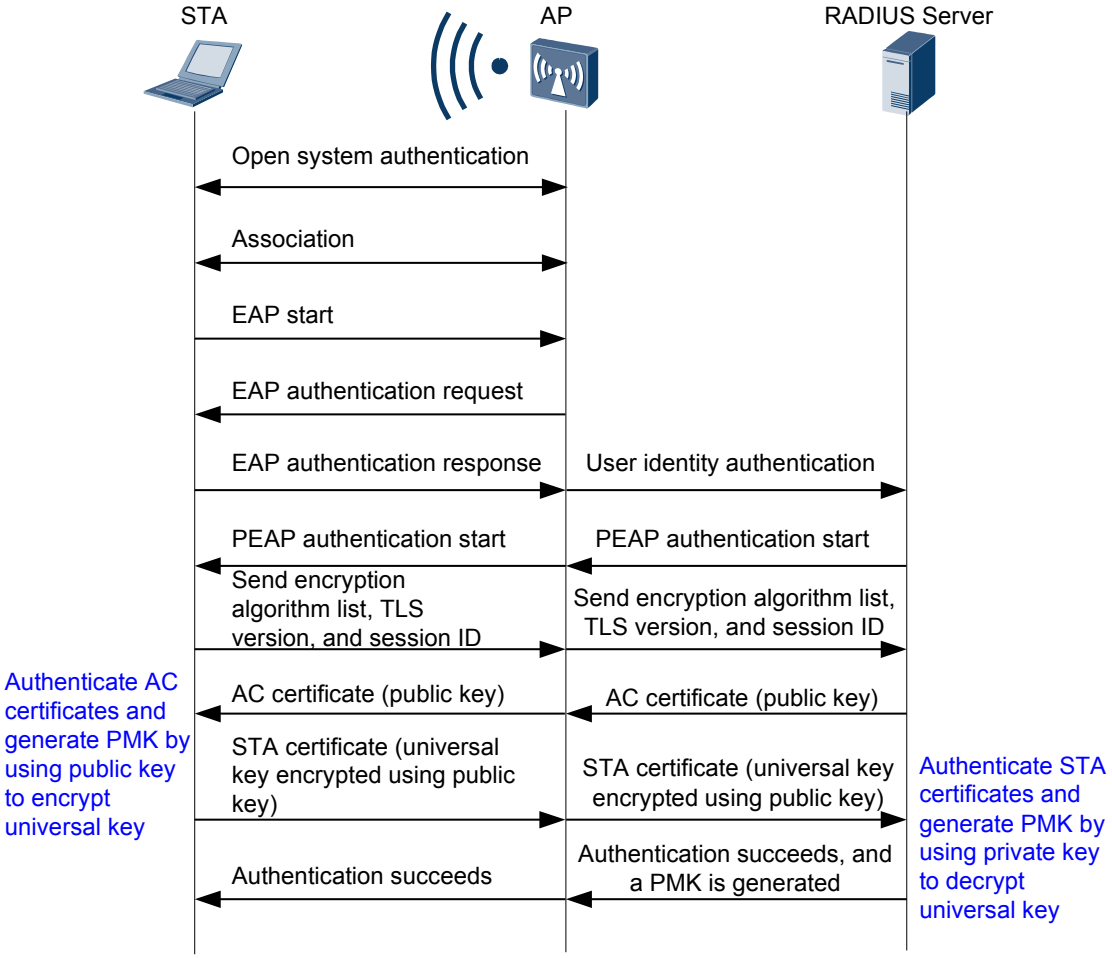


Figure 6-6 EAP-PEAP 802.1X authentication



- WPA/WPA2 personal edition: A dedicated authentication server is expensive and difficult to maintain for small- and medium-scale enterprises and individual users. The WPA/WPA2 personal edition provides a simplified authentication mode: pre-shared key (WPA/WPA2-PSK) authentication. This mode does not require a dedicated authentication server. Users only need to set a pre-shared key on each WLAN node (including WLAN server, wireless router, and wireless network adapter). A WLAN client can access the WLAN if its pre-shared key is the same as that configured on the WLAN server. The pre-shared key is not used for encryption; therefore, it will not bring security risks like the 802.11 shared key authentication.

802.1X authentication can be used to authenticate wireless and wired users, whereas PSK authentication is specific to wireless users.

PSK authentication requires that a STA and an AP be configured with the same pre-shared key. The STA and AP authenticate each other through key negotiation. During key negotiation, the STA and AP use their pre-shared keys to decrypt the message sent from each other. If the messages are successfully decrypted, the STA and AP have the same pre-shared key. If they use the same pre-shared key, PSK authentication is successful; otherwise, PSK authentication fails.

Key Negotiation

802.11i defines two key hierarchies: pairwise key hierarchy and group key hierarchy. The pairwise key hierarchy protects unicast data exchanged between STAs and APs. The group key hierarchy protects broadcast or multicast data exchanged between STAs and APs.

During key negotiation, a STA and an AP use the pairwise master key (PMK) to generate a pairwise transient key (PTK) and a group temporal key (GTK). The PTK is used to encrypt unicast packets, and the GTK is used to encrypt multicast and broadcast packets.

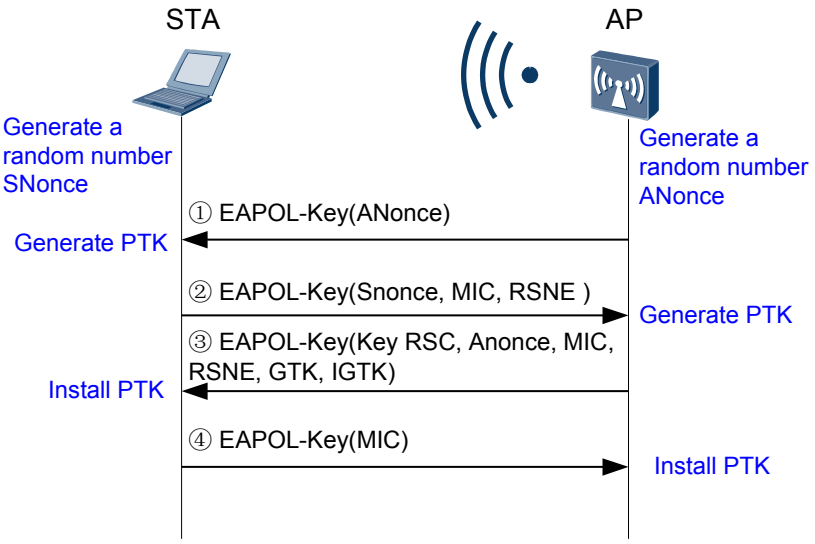
- In 802.1X authentication, a PMK is generated in the process shown in **Figure 6-5**.
- In PSK authentication, the method to generate a PMK varies according to the method to set the pre-shared key (configured using a command):
  - If the pre-shared key is a hexadecimal numeral string, it is used as the PMK.
  - If the pre-shared key is a character string, the PMK is calculated using the hash algorithm based on pre-shared key and service set identifier (SSID).

Key negotiation consists of unicast key negotiation and multicast key negotiation.

- Unicast key negotiation

  Key negotiation is completed through a four-way handshake between a STA and an AP, during which the STA and AP send EAPOL-Key frames to exchange information, as shown in **Figure 6-7**.

Figure 6-7 Unicast key negotiation



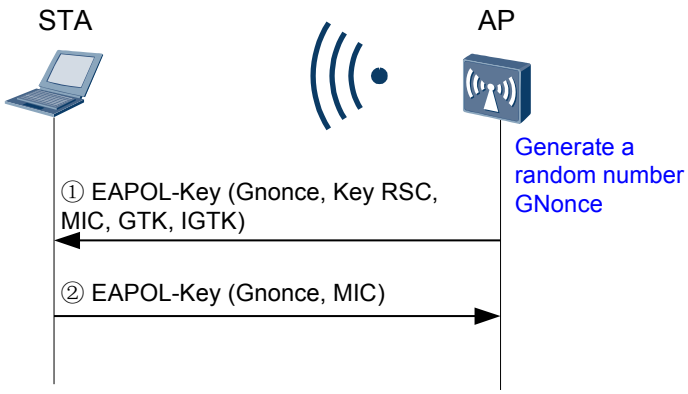
1. The AP sends an EAPOL-Key frame with a random value (ANonce) to the STA.
2. The STA calculates the PTK using MAC addresses of its own and the AP, PMK, ANonce, and SNonce, and sends an EAPOL-Key frame to the AP. The EAPOL-Key frame carries the SNonce, robust security network (RSN) information element, and message integrity code (MIC) of the EAPOL-Key frame. The AP calculates the PTK using the MAC addresses of its own and the STA, PMK, ANonce, and SNonce, and validates the MIC to determine whether STA's PMK is the same as its own PMK.

3. The AP sends an EAPOL-Key frame to the STA to request the STA to install the PTK. The EAPOL-Key frame carries the ANonce, RSN information element, MIC, and encrypted GTK.
4. The STA sends an EAPOL-Key frame to the AP to notify the AP that the PTK has been installed and will be used. The AP installs the PTK after receiving the EAPOL-Key frame.

- Multicast key negotiation

  Multicast key negotiation is completed through a two-way handshake. The two-way handshake begins after the STA and AP generate and install a PTK through a four-way handshake. **Figure 6-8** shows the two-way handshake process.

  Figure 6-8 Multicast key negotiation



1. The AP calculates the GTK, uses the unicast key to encrypt the GTK, and sends an EAPOL-Key frame to the STA.
2. After the STA receives the EAPOL-Key frame, it validates the MIC, decrypts the GTK, installs the GTK, and sends an EAPOL-Key ACK frame to the AP. After the AP receives the EAPOL-Key ACK frame, it validates the MIC and installs the GTK.

Data Encryption

WPA and WPA2 support TKIP and CCMP encryption algorithms.

- TKIP

  Unlike WEP that uses a static shared key, TKIP uses a dynamic key negotiation and management mechanism. Each user obtains an independent key through dynamic negotiation. The key of a user is calculated using the PTK generated in key negotiation, MAC address of the sender, and packet sequence number. This mechanism helps defend against attacks to WEP.

  TKIP uses MICs to ensure integrity of frames received on the receiver and validity of data sent by the sender and receiver. This mechanism protects information integrity. A MIC is calculated using the MIC key generated during key negotiation, destination MAC address, source MAC address, and data frame.

- CCMP

Different from WEP and TKIP that use a stream cipher algorithm, CCMP uses an Advanced Encryption Standard (AES) block cipher. The block cipher algorithm overcomes defects of the RC4 algorithm and provides a higher security.

6.3.1.3 WAPI

WLAN Authentication and Privacy Infrastructure (WAPI) is a Chinese national standard for WLANs, which was developed based on IEEE 802.11. WAPI provides higher security than WEP and WPA and consists of the following:

- WLAN Authentication Infrastructure (WAI): authenticates user identities and manages keys.
- WLAN Privacy Infrastructure (WPI): protects data transmitted on WLANs and provides the encryption, data verification, and anti-replay functions.

WAPI uses the elliptic curve cryptography (ECC) algorithm based on the public key cryptography and the block key algorithm based on the symmetric-key cryptography. The ECC algorithm is used for digital certificate authentication and key negotiation between wireless devices. The block key algorithm is used to encrypt and decrypt data transmitted between wireless devices. The two algorithms implement identity authentication, link authentication, access control, and user information encryption.

WAPI has the following advantages:

- Bidirectional identity authentication

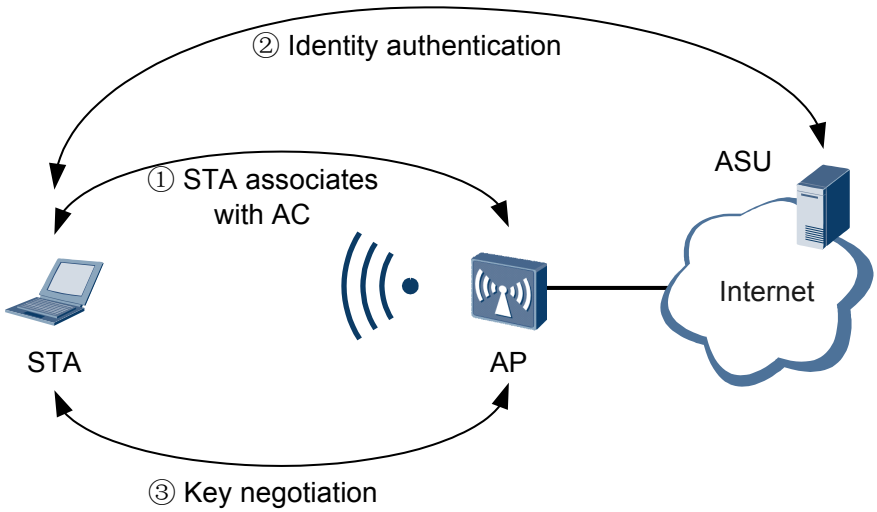
  Bidirectional identity authentication prevents access from unauthorized STAs and protects a WLAN against attacks from unauthorized WLAN devices. Other security policies only enable WLAN devices to authenticate STAs and do not provide a mechanism to authenticate WLAN devices.
- Digital certificate as identity information

  A WAPI system has an independent certificate server. STAs and WLAN devices use digital certificates to prove their identities, improving network security. When a STA requests to join or leave a network, the administrator only needs to issue a certificate to the STA or revoke the certificate of the STA.
- Well-developed authentication protocol

  WAPI uses digital certificates to identify STAs and wireless devices. During identity authentication, the elliptic curve digital signature algorithm is used to verify a digital certificate. In addition, the secure message hash algorithm is used to ensure message integrity, preventing attackers from tampering or forging information transmitted during identity authentication. In other security policies, the message integrity check mechanism is ineffective and cannot prevent attackers from tampering or forging authentication success messages.

As shown in **Figure 6-9**, WAPI involves identity authentication and key negotiation, which begin after a STA associates with an AP.

Figure 6-9 WAPI networking



Identity Authentication

WAPI provides two identity authentication modes: certificate-based mode (WAPI-CERT) and pre-shared key-based mode (WAPI-PSK).

- WAPI-CERT: A STA and an AP authenticate each other's certificate. The certificates must be loaded on the STA and AP and verified by an authentication service unit (ASU). After certificate authentication is complete, the STA and AP use the temporal public key and private key to generate a base key (BK) for key negotiation.

  The WAPI-CERT mode is applicable to large-scale enterprise networks or carrier networks that can deploy and maintain an expensive certificate system.

Figure 6-10 WAPI certificate authentication

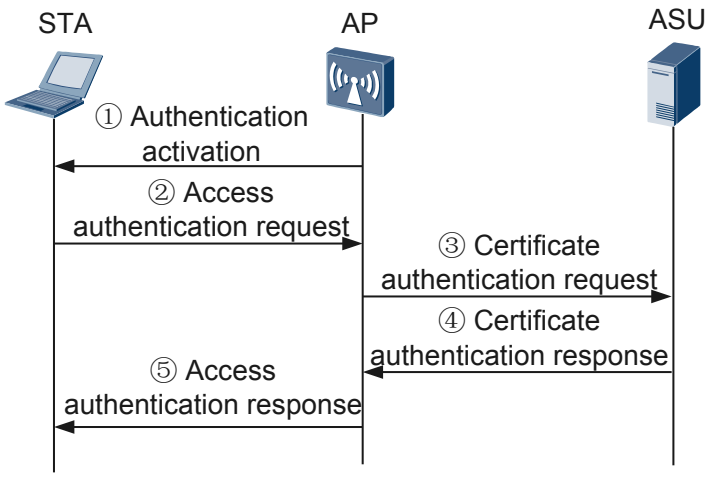


Figure 6-10 shows the WAPI certificate authentication process.

1. Authentication activation: When a STA requests to associate or re-associate with an AP, the AP checks whether the user is a WAPI user. If the user is a WAPI user, the AP sends an authentication activation packet to trigger the certificate authentication process.
2. Access authentication request: The STA sends an access authentication request carrying the STA's certificate and system time to the AP. The system time is the access authentication request time.
3. Certificate authentication request: When the AP receives the access authentication request, it records the access authentication request time and sends a certificate authentication request to the ASU. The certificate authentication request carries the STA's certificate, access authentication request time, AP's certificate, and signature generated using the AP's private key and the preceding information.
4. Certificate authentication response: When the ASU receives the certificate authentication request, it authenticates the AP's signature and certificate. If the AP's signature and certificate are invalid, the authentication fails. If they are valid, the ASU authenticates the STA's certificate. After the authentication is complete, the ASU constructs a certificate authentication response with the STA's certificate authentication result, AP's certificate authentication result, and signature generated using the authentication results, and sends the certificate authentication response to the AP.
5. Access authentication response: When the AP receives the certificate authentication response, it checks the signature to obtain the STA's certificate authentication result, and controls access of the STA based on the certificate authentication result. The AP then forwards the certificate authentication response to the STA. The STA checks the signature generated by the ASU to obtain the AP's certificate authentication result, and determines whether to associate with the AP based on the result. If the certificate authentication succeeds, the AP accepts the access request. If the certificate authentication fails, the AP disassociates the STA from the network.

- WAPI-PSK: The STA and AP have the same pre-shared key configured before authentication. The pre-shared key is converted into a BK during authentication.

  The WAPI-PSK mode does not require an expensive certificate system, so it is applicable to individual users or small-scale enterprise networks.

Key Negotiation

After the AP is authenticated by the ASU, the AP initiates key negotiation with the STA. Key negotiation consists of unicast key negotiation and multicast key negotiation.

- Unicast key negotiation

  The STA and AP use the unicast encryption key and unicast integrity key obtained through unicast key negotiation to ensure security of unicast data exchanged between them. During unicast key negotiation, the STA and AP use the KD-HMAC-SHA256 algorithm to calculate a unicast session key (USK) based on the BK. In addition to the USK, the STA and AP also negotiate the encryption key and identity key used to generate the multicast key.

Figure 6-11 WAPI unicast key negotiation

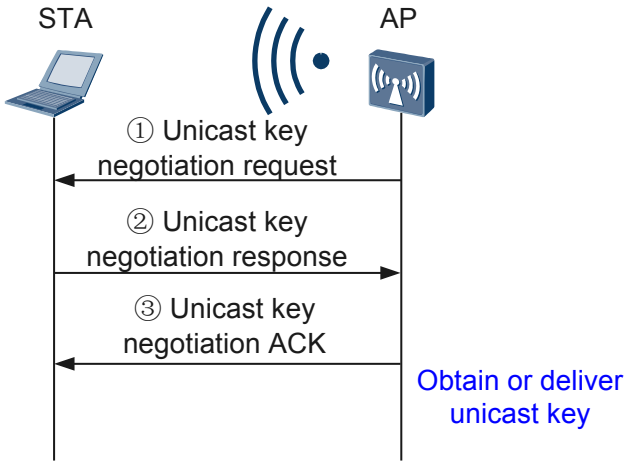


Figure 6-11 shows the unicast key negotiation process.

1. Unicast key negotiation request

   After a BK is generated, the AP sends a unicast key negotiation request packet to the STA.

2. Unicast key negotiation response

   After the STA receives the unicast key negotiation request packet, it performs the following steps:

   a. Checks whether this negotiation process is triggered to update the unicast key.
      - If so, the STA proceeds to step b.
      - If not, the STA proceeds to step c.

      NOTE

      WAPI allows the STA to directly send a unicast key negotiation response to the AP to initiate a unicast key update.

   b. Checks whether the challenge of the AP is the same as the challenge that is obtained in last unicast key negotiation and saved locally. If the two challenges are different, the STA drops the unicast key negotiation request packet.

   c. Generates a random challenge, and then uses the KD-HMAC-SHA256 algorithm to calculate a USK and the AP's challenge used for the next unicast key negotiation based on the BK, AP's challenge, and STA's challenge.

   d. Uses the message authentication key and HMAC-SHA256 algorithm to calculate a message authentication code, and sends it to the AP with a unicast key negotiation response packet.

3. Unicast key negotiation ACK

   After the AP receives the unicast key negotiation response packet, it performs the following steps:

   a. Checks whether the AP's challenge is correct. If the AP's challenge is incorrect, the AP drops the unicast key negotiation response packet.

   b. Uses the KD-HMAC-SHA256 algorithm to calculate a USK and the AP's challenge used for the next unicast key negotiation based on the BK, AP's

challenge, STA's challenge. The AP then calculates the local message authentication code using the message authentication key and HMAC-SHA256 algorithm, and compares the local message authentication code with that in the received unicast key negotiation response packet. If the two message authentication codes are different, the AP drops the unicast key negotiation response packet.

c. Checks the WAPI information element in the response packet if this is the first unicast key negotiation after the BK is generated. If the network type is BSS, the AP checks whether the WAPI information element in the response packet is the same as that in the association request packet it received before. If they are different, the AP sends a Deauthentication frame to disassociate the STA. If the network type is IBSS (ad-hoc network), the AP checks whether the unicast key algorithm supports the information element in the response packet. If not, the AP sends a Deauthentication frame to disassociate the STA.

d. Uses the message authentication key and HMAC-SHA256 algorithm to calculate a message authentication code, and sends it to the STA with a unicast key negotiation ACK packet.

- Multicast key negotiation

  The AP uses the multicast encryption key and multicast integrity key derived from the multicast master key (MMK) to encrypt broadcast or multicast data it sends, and sends a multicast key advertisement packet to the STA. The STA obtains the multicast encryption key and multicast integrity key from the multicast key advertisement packet to decrypt the broadcast or multicast data it receives.

  Multicast key negotiation is performed after unicast key negotiation is complete. The AP advertises the multicast keys to the STA in this process.

Figure 6-12 WAPI multicast key negotiation

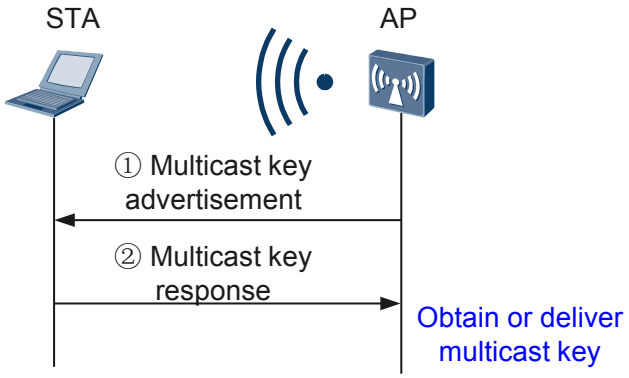


Figure 6-12 shows the multicast key negotiation process.

1. Multicast key advertisement

   The AP uses the random number algorithm to calculate a MMK, encrypts the MMK using the negotiated unicast key, and sends an advertisement packet to notify the STA of the MMK.

2. Multicast key response

   After the STA receives the multicast key advertisement packet, it performs the following steps:

a. Calculates the checksum using the message authentication key identified by the unicast key identifier, and compares the checksum with the message authentication code. If the checksum is different from the message authentication code, the STA drops the multicast key advertisement packet.

b. Checks whether the key advertisement identifier is increasing. If not, the STA drops the multicast key advertisement packet.

c. Decrypts the multicast key to obtain the 16-byte master key and uses the KD-HMAC-SHA256 algorithm to extend it to 32 bytes. The first 16 bytes indicate the encryption key, and the last 16 bytes indicate the integrity key.

d. Saves the key advertisement identifier and sends a multicast key response packet to the AP.

After the AP receives the multicast key response packet, it performs the following steps:

a. Calculates the checksum using the message authentication key identified by the unicast key identifier, and compares the checksum with the message authentication code. If the checksum is different from the message authentication code, the AP drops the multicast key response packet.

b. Compares fields (such as key advertisement identifier) in the multicast key response packet with corresponding fields in the multicast key advertisement packet it has sent. If all the fields are the same, the multicast key negotiation is successful. Otherwise, the AP drops the multicast key response packet.

Key Update

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. To enhance security, WAPI provides time-based and packet-based key updates mechanisms:

- Time-based key update: The unicast and multicast keys of a STA have an aging time (configured using a command). When the aging time of the current unicast or multicast key expires, the STA and AP negotiate a new unicast or multicast key.
- Packet-based key update: When the number of packets encrypted using a unicast or multicast key reaches a specified value (configured using a command), the STA and AP negotiate a new unicast or multicast key.

6.3.2 STA Blacklist and Whitelist

On a WLAN, blacklist or whitelist can be configured to filter access from STAs based on specified rules. The blacklist or whitelist allows authorized STAs to connect to the WLAN and rejects access from unauthorized STAs.

- Whitelist

  A whitelist contains MAC addresses of STAs that are allowed to connect to a WLAN. After the whitelist function is enabled, only the STAs in the whitelist can connect to the WLAN, and access from other STAs is rejected.

- Blacklist

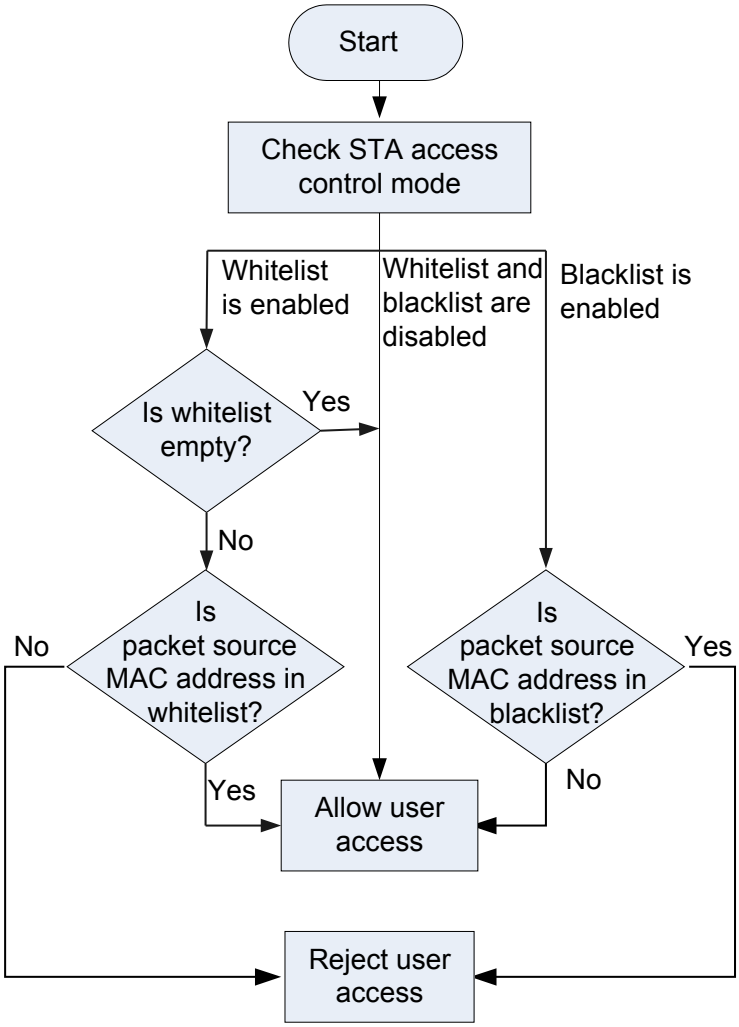
A blacklist contains MAC addresses of STAs that are not allowed to connect to a WLAN. After the blacklist function is enabled, STAs in the blacklist cannot connect to the WLAN, and other STAs can connect to the WLAN.

NOTE

If the STA whitelist or blacklist function is enabled but the whitelist or blacklist is empty, all STAs can connect to the WLAN.

Figure 6-13 shows how STA blacklist and whitelist work.

Figure 6-13 STA blacklist and whitelist working process



6.4 Service Security Principles

This section describes the implementation of user isolation and terminal type identification.

6.4.1 User Isolation

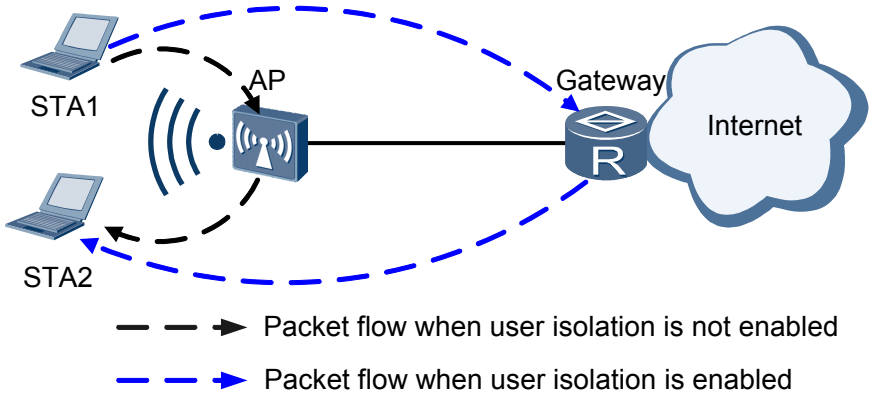
In public places (such as airports and cafes), carriers' networks, medium- and large-sized enterprises, and financial organizations, users may need to connect to the Internet wirelessly. In these scenarios, user isolation can ensure security of data transmitted between users. User isolation can be implemented based on VAPs or user groups.

VAP-based User Isolation

In VAP-based user isolation mode, Layer 2 packets cannot be transmitted between WLAN users associating with the same VAP. All user traffic must be forwarded by the gateway, and all WLAN users communicate through the gateway.

As shown in **Figure 6-14**, STA1 and STA2 associate with the same VAP. Before user isolation is enabled, Layer 2 packets can be forwarded between STA1 and STA2. After user isolation is enabled, Layer 2 packets cannot be forwarded between STA1 and STA2.

Figure 6-14 VAP-based user isolation



User Group-based User Isolation

WLAN users need to be dynamically authorized to limit the network resources users can access after they go online. A RADIUS server controls user authority based on user groups. After a user is authenticated, the RADIUS server delivers a user group for the user to the AP. User groups can be associated with different ACL rules to control authorization information for different types of users. User group-based user isolation can isolate users within a user group or between different user groups to protect security of service data.

After intra-group user isolation is configured in a user group, users in the user group cannot communicate with each other.

After inter-group isolation is configured in a user group, users in the user group cannot communicate with users in other user groups.

6.5 Applications

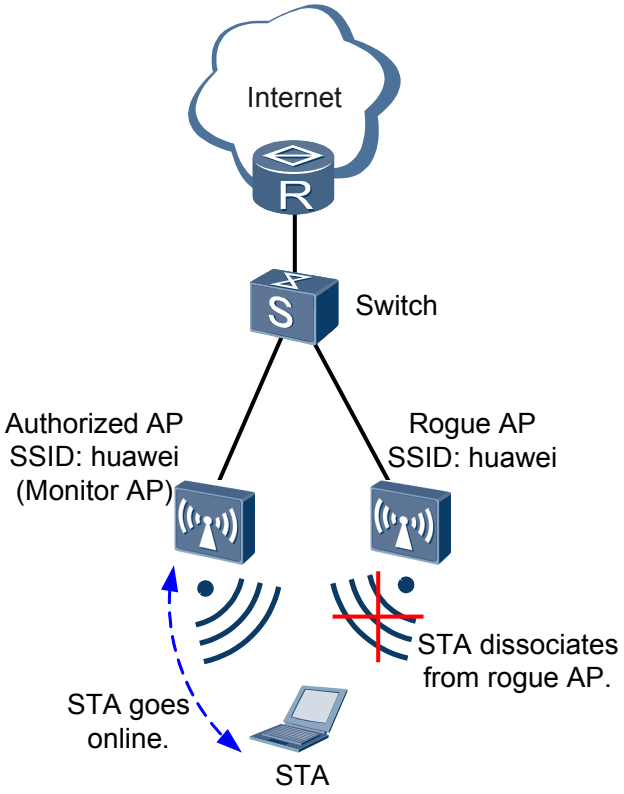
This section describes application scenarios of WLAN security.

6.5.1 WIDS/WIPS

Configuring WIDS and WIPS Against Rogue Devices

As shown in **Figure 6-15**, an employee connects to a rogue fat AP from the campus network or uses simulation software to simulate a fat AP and deceive users into connecting to the corresponding SSID. After WIDS and WIPS are configured, the AP identifies the rogue AP. The monitor AP then uses the rogue AP's identity information to broadcast a Deauthentication frame. After STAs associating with the rogue AP receive the Deauthentication frame, they disassociate from the rogue AP. This countermeasure prevents STAs from associating with the rogue AP.

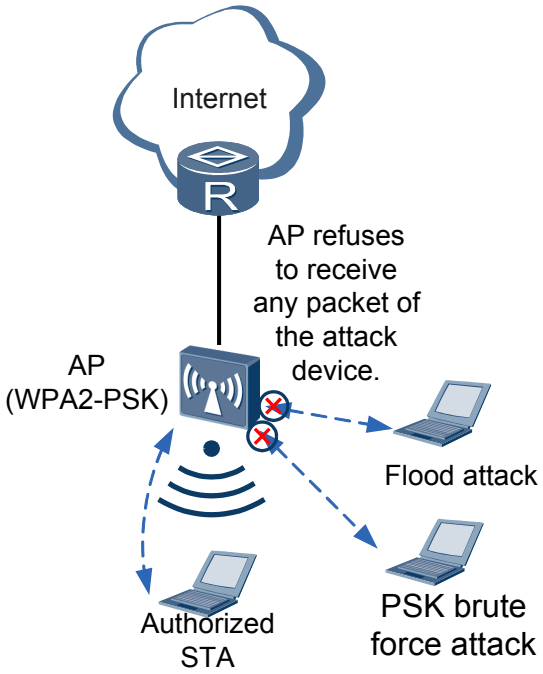
Figure 6-15 Configuring WIDS and WIPS against rogue devices



Configuring WIDS and WIPS Against Attack Devices

As shown in **Figure 6-16**, the campus wireless network uses the WPA2-PSK authentication mode. Attackers use terminals to initiate flood attacks to the wireless network and attempts to use the brute force method to decrypt the password. After detecting the attack device, the AP adds the attack device to the dynamic blacklist and does not process any packet of the device to prevent attacks.

Figure 6-16 Configuring WIDS and WIPS against attack devices



6.5.2 Security Policy

Commonly Used Security Policy for Households and SOHO Networks

Households and SOHO networks do not require high security. They usually use the WPA/WPA2 personal edition and do not require an authentication server.

Commonly Used Security for Enterprise Networks

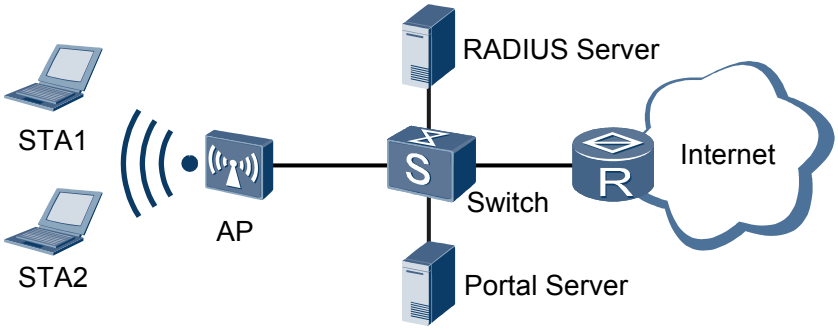
Enterprise networks require high security. They usually use the 802.1X-based WPA/WPA2 enterprise edition and deploy an authentication server.

Commonly Used Security Policy for Carrier Networks

Besides WEP, WPA/WPA2, and WAPI that are specific to wireless users, carriers can combine WLAN security policies with port authentication to enhance security of wireless users. Port authentication methods include 802.1X authentication, MAC address authentication, and Portal authentication. For details about the authentication methods, see NAC in the *Feature description - Security*.

As shown in **Figure 6-17**, a carrier WLAN network usually uses WEP (no authentication, no encryption) and Portal authentication. When a STA attempts to connect to wireless network, the AP pushes the Portal authentication web page to the user. The user must enter the user name and password on the displayed web page. If the user is successfully authenticated by the RADIUS server, the user can connect to the Internet wirelessly.

Figure 6-17 WEP+Portal authentication

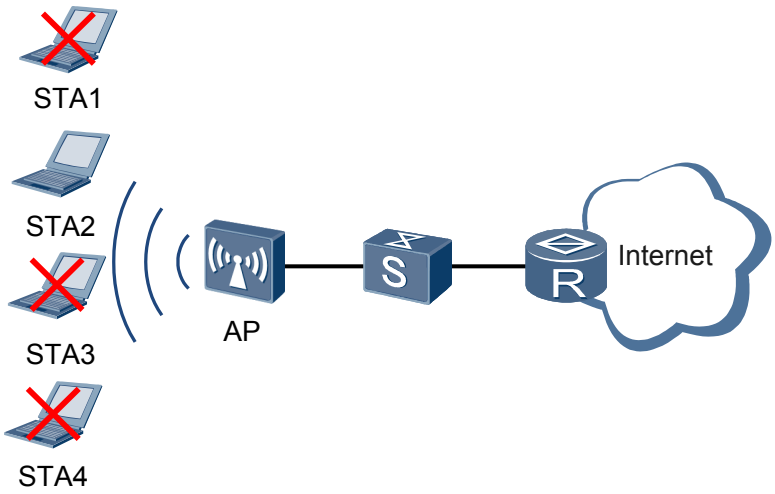


6.5.3 STA Blacklist and Whitelist

STA Whitelist

As shown in **Figure 6-18**, visiting employees often bring their laptops in an AP's coverage area on a campus network. If only STAs of a few local employees are allowed to connect to the wireless network, the enterprise can configure the whitelist function on the AP and add MAC addresses of these STAs to the whitelist. In this example, STA2 is added to the whitelist. Then only STA2 can connect to the wireless network, and STAs not in the whitelist (STA1, STA3, and STA4 in **Figure 6-18**) cannot connect to the wireless network through the AP.

Figure 6-18 STA whitelist application

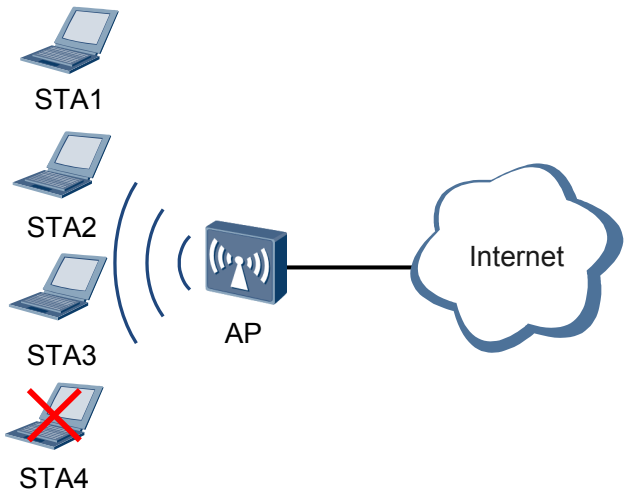


STA Blacklist

As shown in **Figure 6-19**, many STAs of local employees exist in an AP's coverage area on a campus network. Guests or visiting employees sometimes bring their laptops to this AP's coverage area. If only STAs of guests or visiting employees are not allowed to connect to the wireless network, the enterprise can configure the blacklist function on the AP and add MAC addresses of these STAs to the blacklist. In this example, STA4 is added to the blacklist. Then

STA4 cannot connect to the wireless network through the AP, and other STAs (STA1, STA2, and STA3 in **Figure 6-19**) can connect to the wireless network.

Figure 6-19 STA blacklist application



6.6 Default Configuration

This section describes the default configuration of the WLAN security features.

Table 6-1 Default WLAN security configuration

Parameter	Default Setting
AP working mode	Normal mode
WIDS/WIPS	Disabled
Attack detection	Disabled
Dynamic blacklist	Disabled
Security policy	WEP
WEP security policy	Open system authentication+non-encryption
WPA security policy	802.1x+PEAP authentication+TKIP encryption
WPA2 security policy	802.1x+PEAP authentication+CCMP encryption
WAPI security policy	WAPI-CERT authentication+WPI encryption
WAPI USK/MSK update mode	Time-based update

Parameter	Default Setting
WAPI USK/MSK update parameters	● The default update interval is 86400 seconds. ● The default number of update packets is 10. ● The default number of retransmissions of a key negotiation packet is 3.
STA blacklist and whitelist	Disabled

6.7 Configuring WLAN Security

As wireless local area network (WLAN) technology uses radio signals to transmit service data, service data can easily be intercepted or tampered by attackers when being transmitted on the open wireless channels. WLAN security can be configured to protect WLAN networks against attacks and secure information and services of authorized users.

6.7.1 Configuring WIDS and WIPS

You can configure WIDS and WIPS to detect and defend against intrusion from unauthorized devices on WLAN networks and enable the AC to detect attacks and add devices initiating the attacks to the dynamic blacklist, ensuring security of authorized users.

Pre-configuration Tasks

Before configuring WIDS and WIPS, complete the following task:

- **4 Configuration Guide - WLAN Service**

Configuration Procedure

The device supports the configuration of detection and defense against intrusion from unauthorized devices, attack detection, and dynamic blacklist.

- Configuration of detection and defense against intrusion from unauthorized devices:
  1. **6.7.1.1 Configuring WIDS for an AP**
  2. **6.7.1.2 Configuring WIPS for an AP**
- Configuration of attack detection and dynamic blacklist:
  1. **6.7.1.3 Configuring the AP Attack Detection Function**
  2. **6.7.1.4 Configuring the Dynamic Blacklist Function**

The configuration procedure is as follows:

6.7.1.1 Configuring WIDS for an AP

Context

There are security risks from unauthorized devices on WLAN networks, so administrators deploy monitoring APs to monitor the WLAN networks. After the AP working mode is set to monitoring or hybrid, the AP monitors wireless devices. The AP can identify unauthorized devices.

An AP periodically detects wireless device information, including added and modified device information in detection intervals. After several detection intervals, all the wireless device information saved in the AP may be different from rogue device information. You can set the interval for synchronizing all the wireless device information and rogue device information. After the synchronization interval is reached, synchronization starts. If information about a rogue device is not displayed in all the wireless device information, the rogue device is removed. Then the AP deletes information about the rogue device and adds it to historical records of rogue devices.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface wlan-radio wlan-radio-number
```

The radio interface view is displayed.

Step 3 Run:

```
work-mode { hybrid | monitor }
```

The AP working mode is set to hybrid or monitoring.

By default, radios work in normal mode and transmit only WLAN user data.

Step 4 Run:

```
device detect enable
```

WIDS is enabled for the AP.

By default, no AP is enabled with WIDS.

NOTE

To change the working mode of a WIDS-enabled AP to normal, run the **undo device detect enable** command to disable WIDS first. Then run the **work-mode normal** command to change the working mode to normal.

The configured WIDS or WIPS takes effect only after a service set is bound to a radio interface.

Step 5 Run:

```
wlan
```

The WLAN view is displayed.

Step 6 (Optional) Run:

ssid-whitelist ssid *ssid-name*

The SSID whitelist is configured.

By default, no SSID whitelist is configured.

Step 7 (Optional) Run:

radio-profile { **id** *profile-id* | **name** *profile-name* } *

The radio profile view is displayed.

Step 8 (Optional) Run:

channel scan-time *time*

The period during which the AP scans channels is configured.

The default period during which an AP scans channels is 60 ms.

The channel scan period applies to background neighbor probing and WIDS applications.

Step 9 (Optional) Run:

channel scan-frequency *time*

The interval at which the AP scans channels is configured.

The default interval at which an AP scans channels is 10s.

The channel scan interval applies to background neighbor probing and WIDS applications.

Step 10 (Optional) Run:

device report-duration *duration*

The interval at which the AP updates wireless device information is set.

By default, an AP updates wireless device information at an interval of 300 seconds.

Step 11 (Optional) Run:

device synchronization-duration *duration*

The interval at which the AP synchronizes all wireless device information is set.

By default, an AP synchronizes all wireless device information at an interval of 360 minutes.

----End

6.7.1.2 Configuring WIPS for an AP

Context

A monitoring AP identifies unauthorized devices. You can configure the monitoring AP to defend against the unauthorized devices based on the configured WIPS mode. The monitoring AP periodically sends control frames to STAs to disconnect authorized STAs from unauthorized APs or disconnect unauthorized STAs.

Currently, WIPS can be used to defend against rogue APs. A monitoring AP uses the IP address of a rogue AP to broadcast Deauthentication frames to STAs, so that authorized STAs disconnect from the rogue AP.WIPS can also be used to defend against intrusion from unauthorized user terminals and ad-hoc devices. The monitoring AP sends unicast Deauthentication frames to disconnect the unauthorized devices.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface wlan-radio wlan-radio-number
```

The radio interface view is displayed.

Step 3 Run:

```
countermeasures enable
```

WIPS is enabled for the AP.

By default, WIPS is disabled.

Step 4 Run:

```
countermeasures mode rogue { all | ap spoof-ssid | client [ blacklist ] | adhoc }
```

The WIPS mode is set.

By default, no WIPS mode is set.

----End

6.7.1.3 Configuring the AP Attack Detection Function

Context

On small- and medium-scale WLANs, the attack detection function can be enabled to detect flooding attacks, weak initialization vector (IV), spoofing attacks, and brute force cracking of WPA/WPA2/WAPI preshared keys and WEP shared keys. This function enables an AP to add attackers to the dynamic blacklist and send alarms to alert administrators.

NOTE

After the dynamic blacklist function is enabled, the AP can add the detected attackers to the dynamic blacklist. For details, see **6.7.1.4 Configuring the Dynamic Blacklist Function**.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface wlan-radio wlan-radio-number
```

The radio interface view is displayed.

Step 3 Run:

```
attack detection enable { all | flood | weak-iv | spoof | wpa-psk | wpa2-psk | wapi-psk | wep-share-key }
```

Attack detection is enabled on the radio.

By default, attack detection is disabled on an AP radio.

Step 4 Configure attack detection parameters when enabling detection of flooding attacks and brute force cracking of WPA/WPA2/WAPI preshared keys and WEP shared keys.

1. Run:
   quit

   Return to the system view.
2. Run:
   wlan

   The WLAN view is displayed.
3. Run:
   attack detection flood interval *intvalue* **times** *timesvalue*

   The interval for flood attack detection and the maximum number of packets of the same type that an AP can receive within the interval are set.

   By default, the interval for flood attack detection is 60 seconds and an AP can receive a maximum of 300 packets of the same type within the interval.
4. Run:
   attack detection psk interval *intvalue* **times** *timesvalue*

   The interval for brute force preshared key cracking detection and the number of key negotiation attempts allowed within the interval are set.

   By default, the interval for brute force preshared key cracking detection is 60 seconds and an AP allows a maximum of 20 key negotiation attempts within the interval.

   The preshared keys in brute force cracking include those in WPA/WPA2-PSK, WAPI-PSK, and WEP-SK authentication modes.

----End

6.7.1.4 Configuring the Dynamic Blacklist Function

Context

The device support the attack detection function. When the device detects flooding attacks and brute force cracking of WPA/WPA2/WAPI preshared keys and WEP shared keys, the dynamic blacklist function can be configured. This function enables the AP to add attackers to the dynamic blacklist and reject any packets sent from the attackers until the dynamic blacklist entry ages.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
wlan

The WLAN view is displayed.

Step 3 Run:

```
dynamic-blacklist enable
```

The dynamic blacklist function is enabled.

By default, the dynamic blacklist function is disabled on an AP.

Step 4 Run:

```
dynamic-blacklist aging-duration duration
```

The aging time for the dynamic blacklist is set.

By default, the aging time for the dynamic blacklist is 600 seconds.

----End

6.7.1.5 Checking the Configuration

Context

After WIDS and WIPS are configured, you can check the WIDS and WIPS configuration and detected device information.

Procedure

- Run the **display radio config interface** *interface* command to check the configuration of a specified radio interface.
- Run the **display ap** command to check the configuration of a AP.
- Run the **display wlan ids detected** { **all** | [**interference** | **rogue**] **ap** | [**rogue**] **bridge** | [**rogue**] **client** | **adhoc** | **ssid** | **mac-address** *mac-address* } command to check information about wireless devices detected on the WLAN.
- Run the **display wlan ids rogue-history** { **all** | **ap** | **bridge** | **client** | **adhoc** | **ssid** | **mac-address** *mac-address* } command to check historical records of deleted rogue wireless devices.
- Run the **display wlan ids countermeasures device** { **all** | **ap** | **adhoc** | **client** | **ssid** | **mac-address** *mac-address* } command to check information about devices on which countermeasures are taken.
- Run the **display wlan ids attack-detected** { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** } command to check information about devices initiating attacks.
- Run the **display wlan ids attack-detected statistics** command to check the number of attack times.
- Run the **display wlan ids dynamic-blacklist** { **all** | **mac-address** *mac-address* } command to view devices added to the dynamic blacklist.

----End

6.7.2 Configuring a WLAN Security Policy

WLAN security policies include WEP, WPA, WPA2, and WAPI. You can deploy one of them.

Pre-configuration Tasks

Before configuring a WLAN security policy, complete the following task:

- **4 Configuration Guide - WLAN Service**

Configuration Procedure

Configure any one of the following security policies and check the configuration.

6.7.2.1 Configuring a WEP Security Policy

Context

The usage scenarios of a WEP security policy are as follows:

- Open system authentication+non-encryption+Portal authentication: applies to carrier networks and public places. The Portal protocol is used for access authentication and accounting.
- Shared-key authentication+WEP encryption: applies to personal WLANs where high security is not required. A shared key must be maintained.

For details about how to configure Portal authentication, see **Configuring Portal Authentication**.

Because a shared key is easy to be deciphered, the WEP security policy faces great security threats. Enterprise networks can use WEP shared-key authentication+WEP encryption, together with 802.1x authentication. An independent authentication server improves WLAN network security. For details about how to configure 802.1x authentication, see **Configuring 802.1x Authentication**.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
security-profile { id profile-id | name profile-name } *
```

The security profile view is displayed.

Step 4 Run:

```
security-policy wep
```

The WEP security policy is configured.

The default security policy is WEP.

By default, WEP uses open system authentication+non-encryption.

Step 5 Configure authentication and encryption modes.

- Configure open system authentication+non-encryption.

  Run:

  wep authentication-method open-system [**data-encrypt**]

  WEP open system authentication is configured.

  The parameter **data-encrypt** indicates open system authentication+WEP encryption. In this scenario, run the **wep key** and **wep default-key** command to configure a WEP shared key. The WEP shared key is used to generate an encryption key to encrypt WLAN data packets.

- Configure shared-key authentication+WEP encryption.

  NOTE

  In shared-key authentication mode, after a STA scans an SSID, if you double-click the SSID and enter the key, association may fail. This is because open system authentication is used when you double-click the SSID, which is inconsistent with the configured authentication method. To associate with an AP, manually create a WLAN network. You need to enter the SSID, identity authentication, and encryption mode, key, and key index configured on the AC.

  1. Run:

     wep authentication-method share-key

     WEP shared-key authentication is configured.

  2. Run:

     wep key { **wep-40** | **wep-104** | **wep-128** } { **pass-phrase** | **hex** } *key-id* **cipher** *cipher-key-value*

     The WEP shared key and key index are configured.

     By default, no shared key is configured.

  3. Run:

     wep default-key *key-id*

     The index of a shared key used in WEP is set.

     By default, the shared key with index as 0 is used.

     A maximum of four WEP keys can be configured, but only one WEP key can be used at a time.

----End

6.7.2.2 Configuring a WPA/WPA2 Security Policy

Context

Both WPA and WPA2 support 802.1X authentication and TKIP/CCMP encryption algorithm. The WPA and WPA2 protocols provide almost the same security level and their difference lies in the protocol packet format.

The usage scenarios of a WPA/WPA2 security policy are as follows:

- PSK+TKIP and PSK+CCMP: applies to personal and SOHO networks that do not require high security. No authentication server is required. If customers' devices support only WEP encryption, PSK+TKIP can be implemented without hardware upgrading, whereas PSK +CCMP can be implemented only by hardware upgrading.
- 802.1X+TKIP and 802.1X+CCMP: applies to networks requiring high security such as enterprise networks. An independent authentication server is required. If customers' devices

support only WEP encryption, 802.1X+TKIP can be implemented without hardware upgrading, whereas 802.1X+CCMP can be implemented only by hardware upgrading.

- WPA-WPA2 and TKIP-CCMP: User devices vary and support different authentication and encryption modes. This security policy supports simultaneous configuration of WPA and WPA2 on the AC so that multiple types of terminals can access the network, facilitating network management. If the security policy is set to WPA-WPA2, any terminal that supports WPA or WPA2 can be authenticated and access the WLAN; if the encryption mode is set to TKIP-CCMP, any authenticated terminal that supports TKIP or CCMP can implement service packet encryption.

For details about how to configure 802.1X authentication, see **Configuring 802.1x Authentication**. When a WLAN-BSS interface uses 802.1X authentication, configure the AP to function as an EAP relay.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
security-profile { id profile-id | name profile-name } *
```

The security profile view is displayed.

Step 4 Run:

```
security-policy { wpa | wpa2 | wpa-wpa2 }
```

The security policy is configured.

The default security policy is WEP.

- By default, WPA uses 802.1X authentication+TKIP encryption.
- By default, WPA2 uses 802.1X authentication+CCMP encryption.
- By default, WPA-WPA2 uses 802.1X authentication + TKIP-CCMP encryption.

After a security policy is specified, you can use the default authentication and encryption modes or configure the security and encryption modes in **Step 5**.

Step 5 Configure authentication and encryption modes.

- Configure 802.1X authentication+TKIP/CCMP/TKIP-CCMP encryption.

  Run:

  ```
  { wpa | wpa2 | wpa-wpa2 } authentication-method dot1x encryption-method { tkip | ccmp | tkip-ccmp }
  ```

  The 802.1X authentication protocol and encryption algorithm are configured for WPA/WPA2.

- Configure PSK authentication+TKIP/CCMP/TKIP-CCMP encryption.

  Run:

```
{ wpa | wpa2 | wpa-wpa2 } authentication-method psk { pass-phrase | hex }
cipher cipher-key encryption-method { tkip | ccmp | tkip-ccmp }
```

The pre-shared key and encryption algorithm are configured for WPA/WPA2.

----End

6.7.2.3 Configuring a WAPI Security Policy

Context

WAPI allows only robust security network association (RSNA), providing higher security than WEP, WPA, and WPA2.

The usage scenarios of a WAPI security policy are as follows:

- WAPI-CERT authentication+WPI encryption: applies to large-scale enterprise networks or carrier networks that can deploy and maintain an expensive certificate system.

  NOTE

  WAPI uses X.509 V3 certificates encoded in Base64 binary mode and saved in PEM format. The X.509 V3 certificate file name extension is .cer. Before importing certificate files for WAPI, ensure that the certificate files are saved on the root directory of the storage.

- WAPI-PSK authentication+WPI encryption: applies to personal networks and small-scale enterprise networks. No certificate system is required.

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends. To enhance security, WAPI provides the following key update mechanisms:

- Time-based key update: periodically updates a key.
- Packet-based key update: updates a key when the number of packets encrypted using the key reaches the specified value.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
security-profile { id profile-id | name profile-name } *
```

The security profile view is displayed.

Step 4 Run:

```
security-policy wapi
```

The security policy is configured.

The default security policy is WEP.

By default, WAPI uses WAPI-CERT authentication+WPI encryption.

Step 5 Configure authentication mode for WAPI.

- Set the authentication mode to WAPI-PSK, that is, pre-shard key authentication.

  Run:

  wapi authentication-method psk { **pass-phrase** | **hex** } **cipher** *cipher-key*

  Pre-shared key authentication and the authentication key are configured for WAPI.

- Set the authentication mode to WAPI-CERT, that is, certificate authentication.

  1. Run:

     wapi authentication-method certificate

     Certificate authentication is configured for WAPI.

  2. Run:

     wapi import certificate { **ap** | **asu** | **issuer** } **file-name** *file-name* [**password cipher** *password*]

     The AP certificate file, certificate of the AP certificate issuer, and ASU certificate file are imported.

  3. Run:

     wapi import private-key file-name *file-name* [**password** { **cipher** *cipher-password* | **simple** *simple-password* }]

     The AP private key file is imported.

  4. Run:

     wapi asu ip *ip-address*

     An IP address is configured for the ASU certificate server to which the AP sends certificate files.

  5. (Optional) Run:

     wapi cert-retrans-count *cert-count*

     The number of retransmissions of certificate authentication packets is set.

     The default number of retransmissions of certificate authentication packets is 3.

Step 6 (Optional) Run:

wapi { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-update-interval* }

The interval for updating a base key (BK) and the BK lifetime percentage are set.

By default, the interval for updating a BK is 43200s, and the BK lifetime percentage is 70%.

Step 7 (Optional) Run:

wapi sa-timeout *sa-time*

The timeout period of a security association (SA) is set.

The default timeout period of an SA is 60s.

If a STA is not authenticated within the timeout period, no SA is established and the STA cannot connect to the AC.

Step 8 (Optional) Run:

wapi { **usk** | **msk** } **key-update** { **disable** | **time-based** | **packet-based** | **timepacket-based** }

The USK or MSK update mode is set.

By default, USKs and MSKs are updated based on time.

Step 9 (Optional) Run:

```
wapi { usk-update-interval usk-interval | usk-update-packey usk-packet | usk-retrans-count usk-count }
```

The interval for updating a USK, number of packets that will trigger USK update, and number of retransmissions of USK negotiation packets are set.

By default, the interval for updating a USK is 86400s; the number of packets that will trigger USK update is 10; number of retransmissions of USK negotiation packets is 3.

Step 10 (Optional) Run:

```
wapi { msk-update-interval msk-interval | msk-update-packey msk-packet | msk-retrans-count msk-count }
```

The interval for updating an MSK, number of packets that will trigger MSK update, and number of retransmissions of MSK negotiation packets are set.

By default, the interval for updating an MSK is 86400s; the number of packets that will trigger MSK update is 10; number of retransmissions of MSK negotiation packets is 3.

----End

6.7.2.4 Checking the Configuration

Context

After a WLAN security policy is configured, check the configuration.

If a WAPI security policy is used, you can also view the certification content.

Procedure

- Run the **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [**detail**] } command to check the configuration of the WLAN security policy.
- Run the **display wapi certificate file-name** *file-name* command to check the certificate content.

----End

6.7.3 Configuring the STA Blacklist or Whitelist

STA blacklist and whitelist functions allow authorized STAs to connect to the WLAN and reject access from unauthorized STAs.

Pre-configuration Tasks

- **4 Configuration Guide - WLAN Service**

Configuration Procedure

Configure the blacklist or whitelist function for an AP or VAP and check the configuration.

6.7.3.1 Configuring a STA Whitelist

Context

A STA whitelist contains MAC addresses of STAs that are allowed to connect to a WLAN. When only a few STAs are allowed to connect to a WLAN, configure a STA whitelist and set the STA access control mode to whitelist for an AP or VAP.

You can configure a STA whitelist for all VAPs of an AP or for a specified VAP. If an AP and a VAP are configured with the blacklist or whitelist function, a STA can connect to the WLAN only when it is permitted by both the configuration on the AP and VAP.

NOTE

If a STA whitelist is empty, all STAs can connect to the WLAN to access network resources.

Procedure

- Configuring a STA whitelist for AP
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     wlan

     The WLAN view is displayed.
  3. Run:
     sta-whitelist *mac-address*

     The MAC address of a STA is added to the whitelist.

     By default, no MAC address is added to the STA whitelist.

     The device supports a maximum of 16 MAC addresses.
  4. Run:
     sta-access-mode whitelist

     The access control mode is set to the STA whitelist for the AP.

     By default, the STA access control mode is **disable**, indicating that STA access is not controlled by the blacklist or whitelist.
- Configuring a STA whitelist for a VAP
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     wlan

     The WLAN view is displayed.
  3. Run:
     sta-whitelist-profile { **name** *list-name* | **id** *list-id* } *

     A STA whitelist profile is created, and the STA whitelist profile view is displayed.

By default, no STA whitelist profile is created. A maximum of 16 STA whitelist profiles can be created.

4. Run:
   sta-mac *mac-address*

   The MAC address of a STA is added to the whitelist profile.

   A STA whitelist profile supports a maximum of 256 MAC addresses.
5. Run:
   quit

   Return to the WLAN view.
6. Run:
   service-set { **id** *profile-id* | **name** *profile-name* } *

   The service set view is displayed.
7. Run:
   sta-access-mode whitelist

   The access control mode is set to the STA whitelist for the VAP.

   By default, the STA access control mode is **disable**, indicating that STA access is not controlled by the blacklist or whitelist.
8. Run:
   sta-whitelist-profile { **name** *list-name* | **id** *list-id* }

   The service set is bound to the STA whitelist profile.

   By default, no service set is bound to a STA whitelist profile.

----End

6.7.3.2 Configuring a STA Blacklist

Context

A STA blacklist contains MAC addresses of STAs that are not allowed to connect to a WLAN. When only a few STAs are not allowed to connect to a WLAN, configure a STA blacklist and set the STA access control mode to blacklist for an AP or VAP.

You can configure a STA blacklist for all VAPs of an AP or for a specified VAP. If an AP and a VAP are configured with the blacklist or whitelist function, a STA can connect to the WLAN only when it is permitted by both the configuration on the AP and VAP.

Procedure

- Configuring a STA blacklist for the AP
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     wlan

The WLAN view is displayed.

3. Run:
   sta-blacklist *mac-address*

   The MAC address of a STA is added to the blacklist.

   By default, no MAC address is added to the STA blacklist.

   The device supports a maximum of 16 MAC addresses.

4. Run:
   sta-access-mode blacklist

   The access control mode is set to the STA blacklist for the AP.

   By default, the STA access control mode is **disable**, indicating that STA access is not controlled by the blacklist or whitelist.

- Configuring a STA blacklist for a VAP

1. Run:
   system-view

   The system view is displayed.

2. Run:
   wlan

   The WLAN view is displayed.

3. Run:
   sta-blacklist-profile { **name** *list-name* | **id** *list-id* } *

   A STA blacklist profile is created, and the STA blacklist profile view is displayed.

   By default, no STA blacklist profile is created. A maximum of 16 STA blacklist profiles can be created.

4. Run:
   sta-mac *mac-address*

   The MAC address of a STA is added to the blacklist profile.

   A STA blacklist profile supports a maximum of 256 MAC addresses.

5. Run:
   quit

   Return to the WLAN view.

6. Run:
   service-set { **id** *profile-id* | **name** *profile-name* } *

   The service set view is displayed.

7. Run:
   sta-access-mode blacklist

   The access control mode is set to the STA blacklist for the VAP.

   By default, the STA access control mode is **disable**, indicating that STA access is not controlled by the blacklist or whitelist.

8. Run:

   ```
   sta-blacklist-profile { name list-name | id list-id }
   ```

   The STA blacklist profile is bound to the service set.

   By default, no STA blacklist profile is bound to a service set.

----End

6.7.3.3 Checking the Configuration

Pre-configuration Tasks

After the blacklist or whitelist function is configured, you can check the STA access control mode of APs and the configured blacklist or whitelist.

Procedure

- Run the **display sta-access-mode** command to check the STA access control mode of a specified AP.
- Run the **display sta-whitelist** command to view the STA whitelist.
- Run the **display sta-whitelist-profile** { **name** *list-name* | **id** *list-id* | **all** } command to view whitelists in a STA whitelist profile.
- Run the **display sta-blacklist** command to view the STA blacklist.
- Run the **display sta-blacklist-profile** { **name** *list-name* | **id** *list-id* | **all** } command to view blacklists in a STA blacklist profile.

----End

6.7.4 Configuring User Isolation

The user isolation function prevents wireless users associated with the same VAP from forwarding Layer 2 packets to each other. These users cannot directly communicate, ensuring user data security and facilitating accounting management.

Context

In public places (such as airports and cafes), carrier networks, medium- and large-scale enterprises, and financial organizations, users may need to connect to the Internet wirelessly. If accurate and reliable user authentication is not performed, unauthorized users are able to use network resources, consuming bandwidth. This lowers the security and service quality of authorized users and brings unacceptable loss to wireless access service providers. Layer 2 isolation, together with security mechanisms defined in IEEE 802.11i, and RADIUS authentication/accounting mechanisms, can protect security for wireless users.

Pre-configuration Tasks

Before configuring user isolation, complete the following task:

- **Configuring WLAN basic services**

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
service-set { name service-set-name | id service-set-id } *
```

The service set view is displayed.

Step 4 Run:

```
user-isolate
```

User isolation is configured.

By default, user isolation is disabled.

Step 5 Run:

```
quit
```

Return to the WLAN view.

----End

Checking the Configuration

- Run the **display service-set** { **id** *service-set-id* | **name** *service-set-name* | **ssid** *ssid* } command to view the service set configuration to check whether user isolation is enabled.

6.7.5 Maintaining WLAN Security

Maintaining WLAN security includes displaying WLAN security information and clearing WLAN security information..

6.7.5.1 Displaying WLAN Security Configuration

Context

After WLAN security is configured, you can run the following display commands to check the WLAN security configuration.

Procedure

- Run the **display radio config interface** *interface* command to view the security configuration parameters of the specified radio interface, including the working mode, attack detection status, wireless intrusion detection status, and wireless intrusion prevention status.

- Run the **display ap** command to view the security configuration parameters of the AP, including the dynamic blacklist and attack detection conditions.
- Run the **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [**detail**] } command to view the security profile configuration.
- Run the **display sta-access-mode** command to view the STA access control mode of the AP.
- Run the **display sta-whitelist** command to view the STA whitelist.
- Run the **display sta-whitelist-profile** { **name** *list-name* | **id** *list-id* | **all** } command to view the whitelist of the STA whitelist profile.
- Run the **display sta-blacklist** command to view the STA blacklist.
- Run the **display sta-blacklist-profile** { **name** *list-name* | **id** *list-id* | **all** } command to view the blacklist of the STA blacklist profile.
- Run the **display service-set** { **id** *service-set-id* | **name** *service-set-name* | **ssid** *ssid* } command to check whether user isolation is enabled in the specified service set.

----End

6.7.5.2 Clearing Detected Device Information

Context

After WIDS and WIPS are configured, you can clear information about detected wireless device and historical records about unauthorized devices. You can also clear information about devices initiating attacks and remove devices from the dynamic blacklist if the dynamic blacklist is configured.

NOTE

Cleared data cannot be restored. Exercise caution when you clear information about wireless devices.

Procedure

- Run the **reset wlan ids detected** { **all** | [**interference** | **rogue**] **ap** | [**rogue**] **bridge** | [**rogue**] **client** | **adhoc** | **ssid** *ssid* | **mac-address** *mac-address* } command to clear information about detected wireless devices.
- Run the **reset wlan ids rogue-history** { **all** | **ap** | **bridge** | **client** | **adhoc** | **ssid** | **mac-address** *mac-address* } command to clear historical records about authorized devices.
- Run the **reset wlan ids attack-detected all** command to clear information about device initiating attacks.
- Run the **reset wlan ids dynamic-blacklist** { **ap** *ap-id* | **mac-address** *mac-address* | **all** } command to remove devices from the dynamic blacklist. The AP can receive packets from these devices.

----End

6.8 Configuration Examples

This section provides several WLAN security configuration examples, including networking requirements, configuration roadmap, operation procedure, and configuration files.

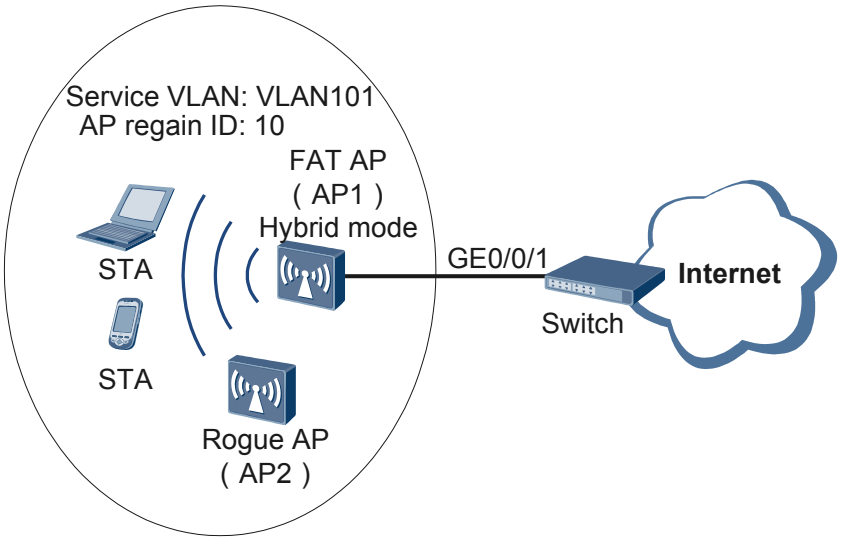
6.8.1 Example for Configuring WIDS and WIPS Functions

Networking Requirements

As shown in **Figure 6-20**, an enterprise branch deploys WLAN basic services and provides a WLAN with the SSID of **test** for employees to access enterprise network resources. STAs automatically obtain IP addresses.

The branch locates in an open place, making the WLAN vulnerable to attacks. For example, an attacker deploys a rogue AP (AP2) on the WLAN to establish connections with STAs to intercept enterprise information, posing great threats to the enterprise network. To prevent such attack, configure WIDS and WIPS functions to enable the AP to detect AP2, preventing STAs from associating with AP2.

Figure 6-20 Networking diagram for configuring WIDS and WIPS against rogue APs



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure WIDS and WIPS functions. Configure AP1 to work in monitoring or hybrid mode to detect wireless device information and defend against rogue AP2 so that STAs disassociate from AP2.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
```

```
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 4 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 5 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 6 Configure WIDS and WIPS functions.

Configure the WIDS function.

```
[AP-wlan-view] quit
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] work-mode hybrid
 Warning: Modify the work mode may cause business interruption, are you sure to
continue?(y/n)[n]:y
[AP-Wlan-Radio0/0/0] device detect enable
```

Configure the WIPS function to defend against rogue APs.

```
[AP-Wlan-Radio0/0/0] countermeasures enable
[AP-Wlan-Radio0/0/0] countermeasures mode rogue ap spoof-ssid
[AP-Wlan-Radio0/0/0] quit
```

Step 7 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 8 Verify the configuration.

Run the **display wlan ids countermeasures device all** command to check information about AP2.

```
[AC] display wlan ids countermeasures device all
Total number of countermeasures device: 1
Flags: a = adhoc, w = ap, c = client
#AP = number of active APs detecting, Ch = channel number
------------------------------------------------------------------------------
 MAC address     Type  #AP   Ch   Last Detected Time   SSID
------------------------------------------------------------------------------
 000b-6b8f-fc6a  -r-w   1   11   2012-01-22/15:33:21   test
------------------------------------------------------------------------------
```

STAs attempt to connect to the Internet through AP2. Countermeasures are taken on AP2, so traffic between STAs and AP2 is stopped and then STA connect to AP1.

```
C:\Documents and Settings\huawei>ping www.baidu.com

Pinging www.a.shifen.com [220.181.112.143] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
```

```
Request timed out.
Reply from 220.181.112.143: bytes=32 time=1433ms TTL=255
Reply from 220.181.112.143: bytes=32 time=40ms TTL=255
Reply from 220.181.112.143: bytes=32 time=11ms TTL=255
Reply from 220.181.112.143: bytes=32 time=46ms TTL=255
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
  radio-profile id 1
   work-mode hybrid
   device detect enable
   countermeasures enable
   countermeasures mode rogue ap spoof-ssid
  service-set id 1 wlan 1
#
return
```

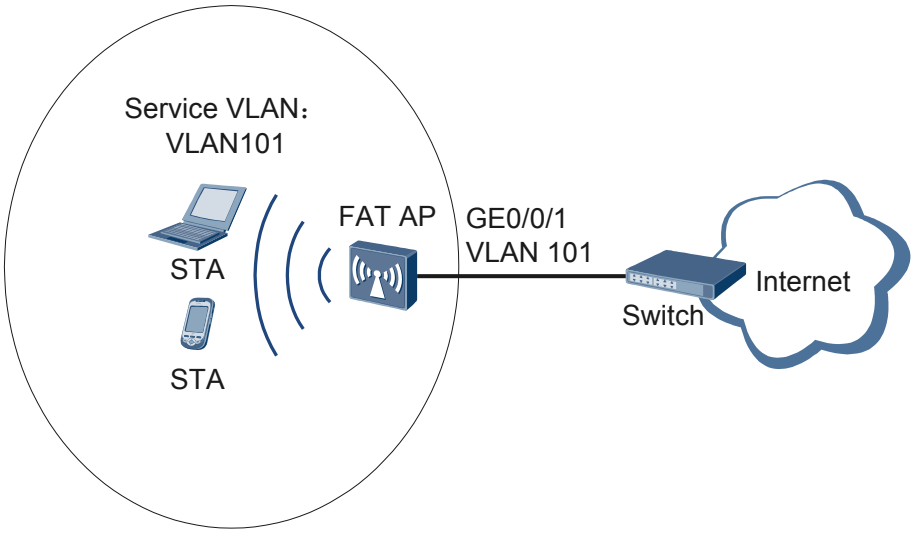
6.8.2 Example for Configuring a WEP Security Policy (Shared-Key Authentication+WEP Encryption)

Networking Requirements

As shown in **Figure 6-21**, the WLAN with the SSID of **test** is available for residents to access the wlan network. STAs automatically obtain IP addresses.

Because the WLAN is open to users, there are potential security risks to service data. Users do not require high security, so a WEP security policy using shared-key authentication and WEP encryption can be configured.

Figure 6-21 Networking diagram for configuring a WEP security policy



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a WEP security policy using shared-key authentication and WEP encryption in a security profile to ensure data security.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a WEP security policy.

```
[AP] wlan
[AP-wlan-view] security-profile name security
[AP-wlan-sec-prof-security] security-policy wep
[AP-wlan-sec-prof-security] wep authentication-method share-key
[AP-wlan-sec-prof-security] wep key wep-40 pass-phrase 0 cipher 12345
[AP-wlan-sec-prof-security] wep default-key 0
[AP-wlan-sec-prof-security] quit
[AP-wlan-view] quit
```

Step 6 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 7 Verify the configuration.

The WLAN with SSID **test** is available for STAs connected to the AP.

If a STA has an incorrect shared key configured, the STA cannot access the WLAN.

NOTE

After the PC scans an SSID, if you double-click the SSID and enter the key, association may fail. You need to add a WLAN on the PC.

- Configuration on the Windows XP operating system:
  1. On the **Association** tab page of the **Wireless network properties** dialog box, add SSID **test**, set the network authentication mode to shared-key mode and encryption mode to WEP, and configure the network key and corresponding key index.
- Configuration on the Windows 7 operating system:
  1. Access the **Manage wireless networks** page, click **Add**, and select **Manually create a network profile**. Add SSID **test**, set the encryption and authentication modes, and click **Next**.
  2. Scan SSIDs to search WLANs. Double-click SSID **test**, click the **Security** tab, and set the key index on the **Security** tab page.

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
  wep authentication-method share-key
  wep key wep-40 pass-phrase 0 cipher %@%@A4FX72`19>o+B><rWe]5E^eP%@%@
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
```

```
#
return
```

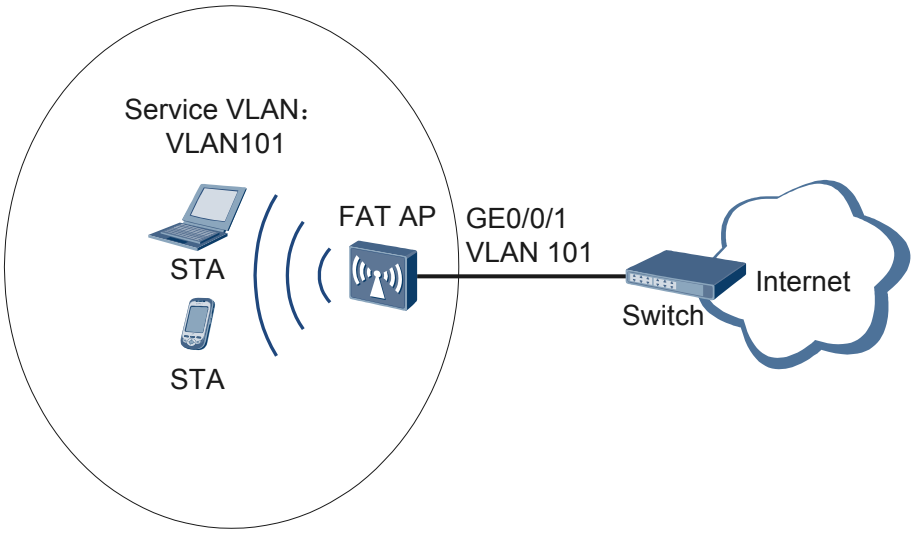
6.8.3 Example for Configuring a WPA2 Security Policy (Pre-shared Key Authentication+CCMP Encryption)

Networking Requirements

As shown in **Figure 6-22**, the AP is deployed in a resident's home. The WLAN with the SSID of **test** is available for residents to access the Internet. STAs automatically obtain IP addresses.

Because the WLAN is open to users, there are potential security risks if no security policy is configured for the WLAN. Users do not require high WLAN security, so no authentication server is required. A WEP or WPA/WPA2 (pre-shared key) security policy can be configured. STAs support WPA/WPA2, TKIP encryption, and CCMP encryption, so pre-shared key authentication and CCMP encryption are used to secure data transmission.

Figure 6-22 Networking diagram for configuring a WPA2 security policy



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a WPA2 security policy using pre-shared key authentication and CCMP encryption in a security profile to ensure data security.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
```

```
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
```

```
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a WPA2 security policy.

```
[AP] wlan
[AP-wlan-view] security-profile name security
[AP-wlan-sec-prof-security] security-policy wpa2
[AP-wlan-sec-prof-security] wpa2 authentication-method psk pass-phrase cipher
1234567a encryption-method ccmp
[AP-wlan-sec-prof-security] quit
[AP-wlan-view] quit
```

Step 6 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 7 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- The wireless PC obtains an IP address after it associates with the WLAN. The STA can access the WLAN after the wireless user enters the password.

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
  security-policy wpa2
  wpa2 authentication-method psk pass-phrase cipher %@%@^D^BT/
A*KLzH;T.x^cwLEsol%@%@ encryption-method ccmp
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
```

```
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

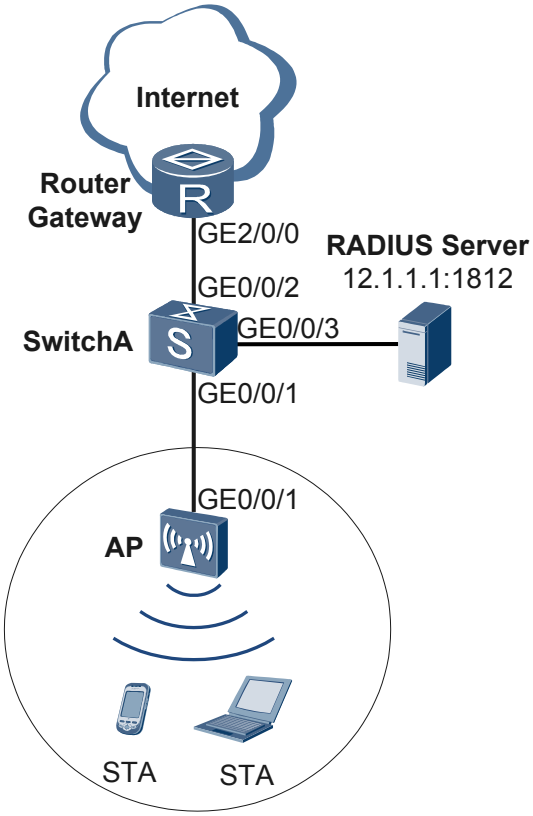
6.8.4 Example for Configuring a WPA Security Policy (802.1x Authentication)

Networking Requirements

As shown in **Figure 6-23**, the enterprise's AP connects to the egress gateway (Router) and RADIUS server. The WLAN with the SSID of **test** is available for employees to access network resources. The gateway also functions as a DHCP server to provide IP addresses on the 10.10.10.0/24 network segment for STAs. The AP controls and manages STAs.

Because the WLAN is open to users, there are potential security risks to enterprise information if no security policy is configured for the WLAN. The enterprise requires high information security, so a WPA security policy using 802.1x authentication and CCMP encryption can be configured. The RADIUS server authenticates STA identities. The AP must be configured to function as an EAP relay, so the AC supports 802.1x authentication.

Figure 6-23 Networking diagram for configuring a WPA security policy



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a RADIUS server template, apply it to an AAA domain, and enable 802.1x authentication on the AP.
3. Configure a WPA security policy using 802.1x authentication and CCMP encryption in a security profile to ensure data security.

NOTE

- Ensure that the RADIUS server IP address, port number, and shared key are correct. When the AP functions as an EAP relay, ensure that the RADIUS server supports the EAP protocol. Otherwise, the RADIUS server cannot process 802.1x authentication requests.

Table 6-2 Data plan

Configuration Item	Data
Service VLAN	VLAN 101
Service set	SSID: test
SwitchA VLAN	VLAN 101, VLAN 102, VLAN 103
DHCP server	IP addresses that Router assigns to STAs: 10.10.10.2 to 10.10.10.254/24
Gateway for STAs	VLANIF 101: 10.10.10.1/24
RADIUS authentication parameters	● IP address: 12.1.1.1 ● Authentication port number: 1812 ● Shared key: 123456 ● AAA domain: huawei.com
User name and password of STAs	● User name: test@huawei.com ● Password: 123456

Procedure

Step 1 Configure SwitchA and the AP can communicate with the upstream device.

Add GE0/0/1 that connects SwitchA to the AP to VLAN 101, VLAN 102, and VLAN 103. Add GE0/0/2 that connects SwitchA to the router to VLAN 102. Add GE0/0/3 that connects SwitchA to the RADIUS server to VLAN 103.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 101 102 103
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
```

```
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 102
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 103
[SwitchA-GigabitEthernet0/0/3] quit
```

Step 2 Configure the AP to communicate with the upstream device.

Configure VLANIF 101 (service VLAN), VLANIF 102, and VLANIF 103.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101 102 103
[AP] interface vlanif 101
[AP-Vlanif101] ip address 10.10.10.1 24
[AP-Vlanif101] quit
[AP] interface vlanif 102
[AP-Vlanif102] ip address 11.1.1.2 24
[AP-Vlanif102] quit
[AP] interface vlanif 103
[AP-Vlanif103] ip address 12.1.1.2 24
[AP-Vlanif103] quit
```

Add GE0/0/1 that connects the AP to the SwitchA to VLAN 101, VLAN 102, and VLAN 103.

```
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[AP-GigabitEthernet0/0/1] quit
```

On the AP, configure a static route.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
```

Step 3 Configure the AP and the Router to assign IP addresses to STAs.

Configure the AP as the DHCP relay agent and enable user entry detection on the AP.

```
[AP] dhcp enable
[AP] dhcp relay detect enable
[AP] interface vlanif 101
[AP-Vlanif101] dhcp select relay
[AP-Vlanif101] dhcp relay server-ip 11.1.1.1
[AP-Vlanif101] quit
```

Configure the Router as a DHCP server to allocate IP addresses to STAs.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] ip pool sta
[Router-ip-pool-sta] gateway-list 10.10.10.1
[Router-ip-pool-sta] network 10.10.10.0 mask 24
[Router-ip-pool-sta] quit
[Router] vlan batch 102
[Router] interface vlanif 102
[Router-Vlanif102] ip address 11.1.1.1 24
[Router-Vlanif102] dhcp select global
[Router-Vlanif102] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.10.10.0 24 11.1.1.2
```

Step 4 Configure an AAA domain to which a RADIUS server template is applied.

1. Configure a RADIUS server template, an AAA authentication scheme, and domain information.

   NOTE

   Ensure that the AP and RADIUS server have the same shared key.

   ```
   [AP] radius-server template radius_huawei
   [AP-radius-radius_huawei] radius-server authentication 12.1.1.1 1812
   [AP-radius-radius_huawei] radius-server shared-key cipher 123456
   [AP-radius-radius_huawei] quit
   [AP] aaa
   [AP-aaa] authentication-scheme radius_huawei
   [AP-aaa-authen-radius_huawei] authentication-mode radius
   [AP-aaa-authen-radius_huawei] quit
   [AP-aaa] domain huawei.com
   [AP-aaa-domain-huawei.com] authentication-scheme radius_huawei
   [AP-aaa-domain-huawei.com] radius-server radius_huawei
   [AP-aaa-domain-huawei.com] quit
   [AP-aaa] quit
   ```

   NOTE

   After domain **huawei.com** is configured, the domain name is added to the authentication user name.

2. Test whether a STA can be authenticated using RADIUS authentication. A user name **test@huawei.com** and password **123456** have been configured on the RADIUS server.

   ```
   [AP] test-aaa test@huawei.com 123456 radius-template radius_huawei
   Info: Account test succeed.
   ```

Step 5 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 6 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 7 Enable 802.1x authentication on the WLAN-BSS interface.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] dot1x enable
[AP-Wlan-Bss1] dot1x authentication-method eap
[AP-Wlan-Bss1] force-domain name huawei.com
[AP-Wlan-Bss1] permit-domain name huawei.com
[AP-Wlan-Bss1] quit
```

Step 8 Configure a WPA security policy.

```
[AP] wlan
[AP-wlan-view] security-profile name security
[AP-wlan-sec-prof-security] security-policy wpa
[AP-wlan-sec-prof-security] wpa authentication-method dot1x encryption-method ccmp
[AP-wlan-sec-prof-security] quit
[AP-wlan-view] quit
```

Step 9 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 10 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- The wireless PC obtains an IP address after it associates with the WLAN.
- Use the 802.1x authentication client on a STA and enter the correct user name and password. The STA is authenticated and can access the WLAN. You must configure the client for PEAP authentication.
  - Configuration on the Windows XP operating system:
    1. On the **Association** tab page of the **Wireless network properties** dialog box, add SSID **test**, set the authentication mode to WPA, encryption mode to CCMP, and encryption algorithm to AES.
    2. On the **Authentication** tab page, set EAP type to PEAP and click **Properties**. In the **Protected EAP Properties** dialog box, deselect **Validate server certificate** and click **Configure**. In the displayed dialog box, deselect **Automatically use my Windows logon name and password** and click **OK**.
  - Configuration on the Windows 7 operating system:
    1. Access the **Manage wireless networks** page, click **Add**, and select **Manually create a network profile**. Add SSID **test**. Set the authentication mode to **WPA-Enterprise**, the encryption mode to CCMP, and the algorithm to AES. Click **Next**.
    2. Scan SSIDs and double-click SSID **test**. On the **Security** tab page, set EAP type to PEAP and click **Settings**. In the displayed dialog box, deselect **Validate server**

certificate and click **Configure**. In the displayed dialog box, deselect **Automatically use my Windows logon name and password** and click **OK**.

----End

Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 101 to 103
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 103
#
return
```

- Configuration file of Router

```
#
sysname Router
#
 vlan batch 102
#
dhcp enable
#
ip pool sta
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
#
interface Vlanif102
 ip address 11.1.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 102
#
ip route-static 10.10.10.0 24 11.1.1.2
#
return
```

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101 to 103
#
dhcp enable
#
dhcp relay detect enable
#
radius-server template radius_huawei
 radius-server authentication 12.1.1.1 1812 weight 80
 radius-server shared-key cipher %@%@hH67%f}f8X"AE&Pw`wS~{:;0%@%@
#
```

```
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 domain huawei.com
  authentication-scheme radius_huawei
  radius-server radius_huawei
#
interface Vlanif101
 ip address 10.10.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 11.1.1.1
#
interface Vlanif102
 ip address 11.1.1.2 255.255.255.0
#
interface Vlanif103
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 dot1x enable
 dot1x authentication-method eap
 permit-domain name huawei.com
 force-domain name huawei.com
#
ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
  security-policy wpa
  wpa authentication-method dot1x encryption-method ccmp
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

6.8.5 Example for Configuring a WAPI Security Policy (Pre-shared Key Authentication)

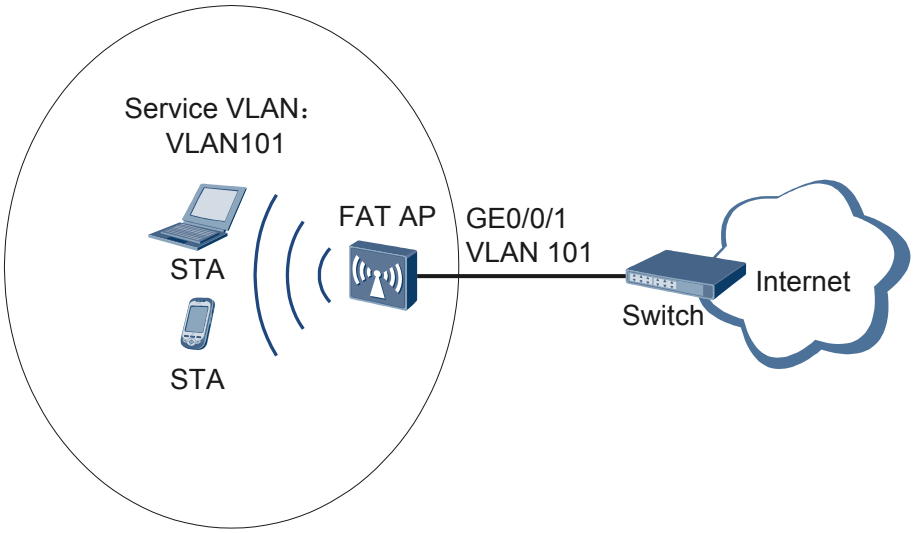
Networking Requirements

As shown in **Figure 6-24**, the AP is deployed in a resident's home. The WLAN with the SSID of **test** is available for residents to access the Internet. STAs automatically obtain IP addresses.

Because the WLAN is open to users, there are potential security risks to service data. Users do not require high WLAN security, so no extra authentication system is required. STAs support

WAPI, so a WAPI security policy using pre-shared key authentication can be configured. Unicast and broadcast keys are updated based on time to secure data transmission.

Figure 6-24 Networking diagram for configuring a WAPI security policy



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a WAPI security policy using pre-shared key authentication in a security profile to ensure data security.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a WAPI security policy.

```
[AP] wlan
[AP-wlan-view] security-profile name security
[AP-wlan-sec-prof-security] security-policy wapi
[AP-wlan-sec-prof-security] wapi authentication-method psk pass-phrase cipher
1234567@
[AP-wlan-sec-prof-security] wapi usk key-update time-based
[AP-wlan-sec-prof-security] wapi msk key-update time-based
[AP-wlan-sec-prof-security] wapi msk-update-interval 20000
[AP-wlan-sec-prof-security] wapi usk-update-interval 20000
[AP-wlan-sec-prof-security] quit
[AP-wlan-view] quit
```

Step 6 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 7 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- The wireless PC obtains an IP address after it associates with the WLAN. The STA can access the WLAN after the wireless user enters the password.

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
  security-policy wapi
  wapi authentication-method psk pass-phrase cipher %@%@Te^%!]pP^@~\d(W6%
_K3x<2#%@%@
  wapi usk-update-interval 20000
  wapi msk-update-interval 20000
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

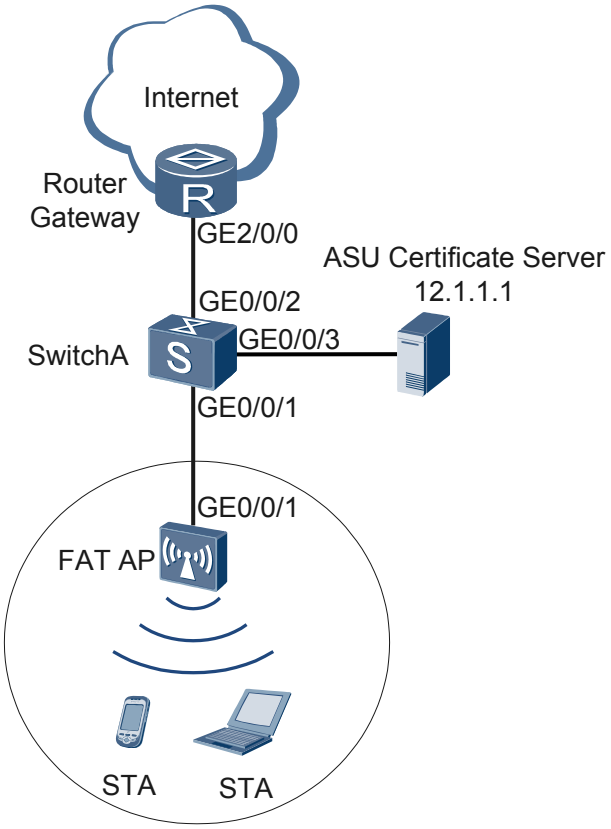
6.8.6 Example for Configuring a WAPI Security Policy (Certificate Authentication)

Networking Requirements

As shown in **Figure 6-25**, the enterprise's AP connects to the egress gateway (Router) and ASU certificate server. The WLAN with the SSID of **test** is available for employees to access network resources. The gateway also functions as a DHCP server to provide IP addresses on the 10.10.10.0/24 network segment for STAs. The AP controls and manages STAs.

Because the WLAN is open to users, there are potential security risks to enterprise information if no security policy is configured for the WLAN. To meet enterprise's high information security requirement and implement bidirectional authentication between the WLAN clients and server, configure a WAPI security policy. Compared with WPA/WPA2, an ASU certificate server and WPI encryption provide higher security for WLAN networks.

Figure 6-25 Networking diagram for configuring a WAPI security policy



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.

2. Configure a WAPI security policy using certificate authentication in a security profile and import the obtained certificates to ensure data security.

Table 6-3 Data plan

Configuration Item	Data
Service VLAN	VLAN 101
Service set	SSID: test
SwitchA VLAN	VLAN 101, VLAN 102, VLAN 103
DHCP server	IP addresses that Router assigns to STAs: 10.10.10.2 to 10.10.10.254/24
Gateway for STAs	VLANIF 101: 10.10.10.1/24
ASU certificate server	IP address: 12.1.1.1
Certificates saved on the AP	● AP certificate: flash:/ap.cer ● Certificate of the AP certificate issuer: flash:/asu.cer ● ASU certificate: flash:/asu.cer ● AP private key certificate: flash:/ap.cer

Procedure

Step 1 Configure SwitchA and the AP can communicate with the upstream device.

Add GE0/0/1 that connects SwitchA to the AP to VLAN 101, VLAN 102, and VLAN 103. Add GE0/0/2 that connects SwitchA to the router to VLAN 102. Add GE0/0/3 that connects SwitchA to the RADIUS server to VLAN 103.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 101 102 103
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 102
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 103
[SwitchA-GigabitEthernet0/0/3] quit
```

Step 2 Configure the AP to communicate with the upstream device.

Configure VLANIF 101 (service VLAN), VLANIF 102, and VLANIF 103.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101 102 103
[AP] interface vlanif 101
[AP-Vlanif101] ip address 10.10.10.1 24
```

```
[AP-Vlanif101] quit
[AP] interface vlanif 102
[AP-Vlanif102] ip address 11.1.1.2 24
[AP-Vlanif102] quit
[AP] interface vlanif 103
[AP-Vlanif103] ip address 12.1.1.2 24
[AP-Vlanif103] quit
```

Add GE0/0/1 that connects the AP to the SwitchA to VLAN 101, VLAN 102, and VLAN 103.

```
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[AP-GigabitEthernet0/0/1] quit
```

On the AP, configure a static route.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
```

Step 3 Configure the AP and the Router to assign IP addresses to STAs.

Configure the AP as the DHCP relay agent and enable user entry detection on the AP.

```
[AP] dhcp enable
[AP] dhcp relay detect enable
[AP] interface vlanif 101
[AP-Vlanif101] dhcp select relay
[AP-Vlanif101] dhcp relay server-ip 11.1.1.1
[AP-Vlanif101] quit
```

Configure the Router as a DHCP server to allocate IP addresses to STAs.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] ip pool sta
[Router-ip-pool-sta] gateway-list 10.10.10.1
[Router-ip-pool-sta] network 10.10.10.0 mask 24
[Router-ip-pool-sta] quit
[Router] vlan batch 102
[Router] interface vlanif 102
[Router-Vlanif102] ip address 11.1.1.1 24
[Router-Vlanif102] dhcp select global
[Router-Vlanif102] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.10.10.0 24 11.1.1.2
```

Step 4 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 5 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 6 Configure a WAPI security policy.

```
[AP] wlan
[AP-wlan-view] security-profile name security
[AP-wlan-sec-prof-security] security-policy wapi
[AP-wlan-sec-prof-security] wapi authentication-method certificate
[AP-wlan-sec-prof-security] wapi asu ip 12.1.1.1
[AP-wlan-sec-prof-security] wapi import certificate ap file-name flash:/ap.cer
[AP-wlan-sec-prof-security] wapi import certificate asu file-name flash:/asu.cer
[AP-wlan-sec-prof-security] wapi import certificate issuer file-name flash:/
asu.cer
[AP-wlan-sec-prof-security] wapi import private-key file-name flash:/ap.cer
[AP-wlan-sec-prof-security] quit
[AP-wlan-view] quit
```

Step 7 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 8 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- The wireless PC obtains an IP address after it associates with the WLAN. The wireless PC is automatically authenticated and can access the WLAN.

----End

Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 101 to 103
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 103
#
return
```

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 101 to 103
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 103
#
return
```

- Configuration file of the AC

```
#
 sysname AP
#
vlan batch 101 to 103
#
dhcp enable
#
dhcp relay detect enable
#
interface Vlanif101
 ip address 10.10.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 11.1.1.1
#
interface Vlanif102
 ip address 11.1.1.2 255.255.255.0
#
interface Vlanif103
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
```

```
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
  security-policy wapi
  wapi asu ip 12.1.1.1
  wapi import certificate ap file-name flash:/ap.cer
  wapi import certificate asu file-name flash:/asu.cer
  wapi import certificate issuer file-name flash:/asu.cer
  wapi import private-key file-name flash:/ap.cer
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

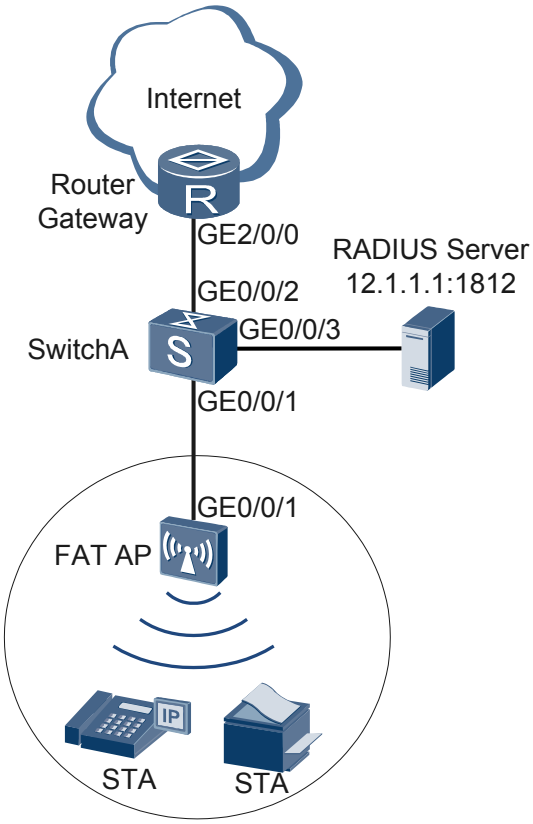
6.8.7 Example for Configuring MAC Address Authentication on the Wireless Side

Networking Requirements

As shown in **Figure 6-26**, the enterprise's AP connects to the egress gateway (Router) and RADIUS server. The WLAN with the SSID of **test** is available for wireless users and terminals to access network resources. The gateway also functions as a DHCP server to provide IP addresses on the 10.10.10.0/24 network segment for STAs. The AP controls and manages STAs.

The WLAN authentication client cannot be installed on wireless devices providing public services, such as wireless printers and phones, so use MAC address authentication. The RADIUS server authenticates wireless devices using their MAC addresses. No authentication is required when STAs access the WLAN, facilitating the use of WLAN services.

Figure 6-26 Networking diagram for configuring MAC address authentication on the wireless side



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a RADIUS server template and apply it to an AAA domain.
3. Configure MAC address authentication on the WLAN-BSS interface to authenticate STAs.

Table 6-4 Data plan

Configuration Item	Data
WLAN service	Open system authentication+non-encryption
Service VLAN	VLAN 101
Service set	SSID: test
SwitchA VLAN	VLAN 101, VLAN 102, VLAN 103
DHCP server	IP addresses that Router assigns to STAs: 10.10.10.2 to 10.10.10.254/24
Gateway for STAs	VLANIF 101: 10.10.10.1/24

Configuration Item	Data
RADIUS authentication parameters	● IP address: 12.1.1.1 ● Port number: 1812 ● Shared key: huawei ● AAA domain: huawei.com
MAC address of a STA	0011-2233-4455

Procedure

Step 1 Configure SwitchA and the AP can communicate with the upstream device.

Add GE0/0/1 that connects SwitchA to the AP to VLAN 101, VLAN 102, and VLAN 103. Add GE0/0/2 that connects SwitchA to the router to VLAN 102. Add GE0/0/3 that connects SwitchA to the RADIUS server to VLAN 103.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 101 102 103
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 102
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 103
[SwitchA-GigabitEthernet0/0/3] quit
```

Step 2 Configure the AP to communicate with the upstream device.

Configure VLANIF 101 (service VLAN), VLANIF 102, and VLANIF 103.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101 102 103
[AP] interface vlanif 101
[AP-Vlanif101] ip address 10.10.10.1 24
[AP-Vlanif101] quit
[AP] interface vlanif 102
[AP-Vlanif102] ip address 11.1.1.2 24
[AP-Vlanif102] quit
[AP] interface vlanif 103
[AP-Vlanif103] ip address 12.1.1.2 24
[AP-Vlanif103] quit
```

Add GE0/0/1 that connects the AP to the SwitchA to VLAN 101, VLAN 102, and VLAN 103.

```
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[AP-GigabitEthernet0/0/1] quit
```

On the AC, configure a static route.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
```

Step 3 Configure the AP and the Router to assign IP addresses to STAs.

Configure the AP as the DHCP relay agent and enable user entry detection on the AP.

```
[AP] dhcp enable
[AP] dhcp relay detect enable
[AP] interface vlanif 101
[AP-Vlanif101] dhcp select relay
[AP-Vlanif101] dhcp relay server-ip 11.1.1.1
[AP-Vlanif101] quit
```

Configure the Router as a DHCP server to allocate IP addresses to STAs.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] ip pool sta
[Router-ip-pool-sta] gateway-list 10.10.10.1
[Router-ip-pool-sta] network 10.10.10.0 mask 24
[Router-ip-pool-sta] quit
[Router] vlan batch 102
[Router] interface vlanif 102
[Router-Vlanif102] ip address 11.1.1.1 24
[Router-Vlanif102] dhcp select global
[Router-Vlanif102] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.10.10.0 24 11.1.1.2
```

Step 4 Configure RADIUS authentication.

1. Configure a RADIUS server template, an AAA authentication scheme, and domain information.

   NOTE

   The STA sends its MAC address as the user name to the RADIUS server for authentication, so the AC needs to be disabled from adding a domain name to the user name.

   ```
   [AP] radius-server template radius_huawei
   [AP-radius-radius_huawei] radius-server authentication 12.1.1.1 1812
   [AP-radius-radius_huawei] radius-server shared-key cipher huawei
   [AP-radius-radius_huawei] undo radius-server user-name domain-included
   [AP-radius-radius_huawei] quit
   [AP] aaa
   [AP-aaa] authentication-scheme radius_huawei
   [AP-aaa-authen-radius_huawei] authentication-mode radius
   [AP-aaa-authen-radius_huawei] quit
   [AP-aaa] domain huawei.com
   [AP-aaa-domain-huawei.com] authentication-scheme radius_huawei
   [AP-aaa-domain-huawei.com] radius-server radius_huawei
   [AP-aaa-domain-huawei.com] quit
   [AP-aaa] quit
   ```

2. Globally configure user names in MAC address authentication without the delimiter "-".

   ```
   [AP] mac-authen username macaddress format without-hyphen
   ```

3. Test whether a STA can be authenticated using RADIUS authentication. In MAC address authentication, STA's MAC address is used as the user name and password.

   ```
   [AP] test-aaa 001122334455 001122334455 radius-template radius_huawei
   Info: Account test succeed.
   ```

Step 5 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 6 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 7 Configure MAC address authentication on the WLAN-BSS interface.

```
[AP] mac-authen
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] mac-authen
[AP-Wlan-Bss1] force-domain name huawei.com
[AP-Wlan-Bss1] permit-domain name huawei.com
[AP-Wlan-Bss1] quit
```

Step 8 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 9 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- After the WLAN function is enabled on wireless devices, they can access the WLAN and provide public services.
- After the STA connects to the WLAN, authentication is performed automatically. You can directly access the WLAN.

----End

Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 101 to 103
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 103
#
return
```

- Configuration file of Router

```
#
sysname Router
#
 vlan batch 102
#
dhcp enable
#
ip pool sta
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
#
interface Vlanif102
 ip address 11.1.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 102
#
ip route-static 10.10.10.0 24 11.1.1.2
#
return
```

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101 to 103
#
mac-authen
#
dhcp enable
#
```

```
dhcp relay detect enable
#
radius-server template radius_huawei
 radius-server authentication 12.1.1.1 1812
 radius-server shared-key cipher %@%@hH67%f}f8X"AE&Pw`wS~{:;0%@%@
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 domain huawei.com
  authentication-scheme radius_huawei
  radius-server radius_huawei
#
 mac-authen username macaddress format without-hyphen
#
interface Vlanif101
 ip address 10.10.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 11.1.1.1
#
interface Vlanif102
 ip address 11.1.1.2 255.255.255.0
#
interface Vlanif103
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 mac-authen
 permit-domain name huawei.com
 force-domain name huawei.com
#
ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

6.8.8 Example for Configuring Portal Authentication on the Wireless Side

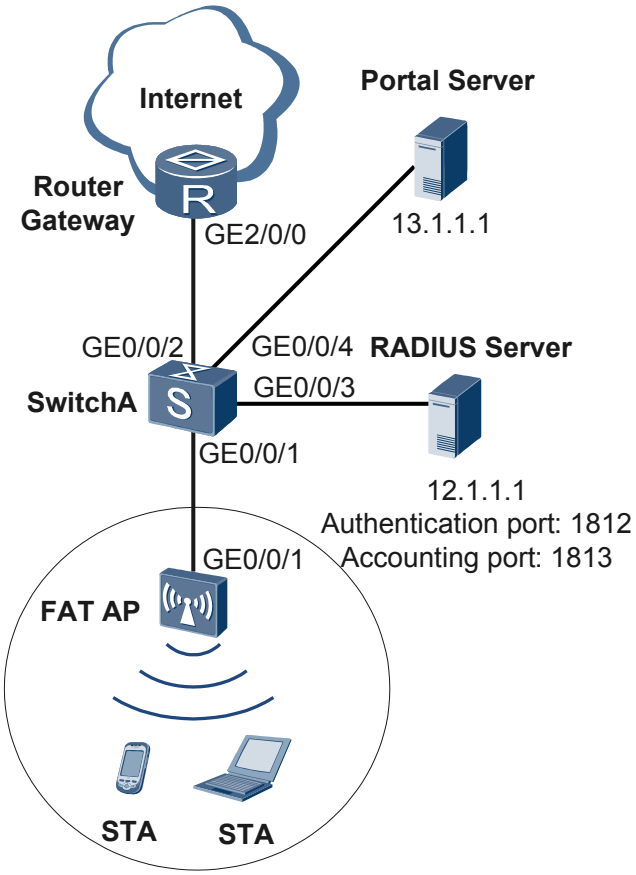
Networking Requirements

As shown in **Figure 6-27**, the AP is deployed in an open place connects to the egress gateway (Router), RADIUS server, and Portal server. The WLAN with the SSID of **test** is available for

users to access network resources. The gateway also functions as a DHCP server to provide IP addresses on the 10.10.10.0/24 network segment for STAs. The AP controls and manages STAs.

Because the WLAN is open to users, there are potential security risks. To facilitate access to the WLAN, use the default security policy on the AP. STAs are not authenticated and data is not encrypted. To uniformly manage STAs and allow only paid users to access the Internet, configure Portal authentication on the AP. Any user who attempts to access the Internet is redirected to the Portal authentication web page. A paid user connects to the Internet after entering the user name and password, and the RADIUS server starts accounting. An unpaid user must pay for the WLAN service and use the obtained user name and password to complete Portal authentication. Generally, the Portal authentication web page provides the paying function.

Figure 6-27 Networking diagram for configuring Portal authentication on the wireless side



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a RADIUS server template, apply it to an AAA domain, and use a RADIUS server to authenticate STAs' identities and perform accounting.
3. Configure Portal authentication. Hypertext Transfer Protocol (HTTP) request packets from a user are redirected to the web page of the Portal server. After the user enters identity information, the STA sends the user identity information to the RADIUS server.

Table 6-5 Data plan

Configuration Item	Data
WLAN service	Open system authentication+non-encryption
Service VLAN	VLAN 101
Service set	SSID: test
SwitchA VLAN	VLAN 101, VLAN 102, VLAN 103
DHCP server	IP addresses that Router assigns to STAs: 10.10.10.2 to 10.10.10.254/24
Gateway for STAs	VLANIF101: 10.10.10.1/24
RADIUS server parameters	● Server IP address: 12.1.1.1 ● Authentication port number: 1812 ● Accounting port number: 1813 ● Shared key: huawei ● AAA domain: huawei.com
User name and password of STAs	● User name: test@huawei.com ● Password: 123456
Portal server parameters	● Server IP address: 13.1.1.1 ● Authentication port number: 50100 ● Shared key: huawei

Procedure

Step 1 Configure SwitchA and the AP can communicate with the upstream device.

Add GE0/0/1 that connects SwitchA to the AP to VLAN 101, VLAN 102, VLAN 103, and VLAN 104. Add GE0/0/2 that connects SwitchA to the router to VLAN 102. Add GE0/0/3 that connects SwitchA to the RADIUS server to VLAN 103. Add GE0/0/4 that connects SwitchA to the portal server to VLAN 104.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 101 102 103 104
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 102
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 103
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface gigabitethernet 0/0/4
```

```
[SwitchA-GigabitEthernet0/0/4] port link-type trunk
[SwitchA-GigabitEthernet0/0/4] port trunk allow-pass vlan 104
[SwitchA-GigabitEthernet0/0/4] quit
```

Step 2 Configure the AP to communicate with the upstream device.

Configure VLANIF 101 (service VLAN), VLANIF 102, VLANIF 103, and VLANIF 104.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101 102 103 104
[AP] interface vlanif 101
[AP-Vlanif101] ip address 10.10.10.1 24
[AP-Vlanif101] quit
[AP] interface vlanif 102
[AP-Vlanif102] ip address 11.1.1.2 24
[AP-Vlanif102] quit
[AP] interface vlanif 103
[AP-Vlanif103] ip address 12.1.1.2 24
[AP-Vlanif103] quit
[AP] interface vlanif 104
[AP-Vlanif104] ip address 13.1.1.2 24
[AP-Vlanif104] quit
```

Add GE0/0/1 that connects the AP to the SwitchA to VLAN 101, VLAN 102, VLAN 103, and VLAN 104.

```
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103 104
[AP-GigabitEthernet0/0/1] quit
```

On the AP, configure a static route.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
```

Step 3 Configure the AP and the Router to assign IP addresses to STAs.

Configure the AP as the DHCP relay agent and enable user entry detection on the AP.

```
[AP] dhcp enable
[AP] dhcp relay detect enable
[AP] interface vlanif 101
[AP-Vlanif101] dhcp select relay
[AP-Vlanif101] dhcp relay server-ip 11.1.1.1
[AP-Vlanif101] quit
```

Configure the Router as a DHCP server to allocate IP addresses to STAs.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] ip pool sta
[Router-ip-pool-sta] gateway-list 10.10.10.1
[Router-ip-pool-sta] network 10.10.10.0 mask 24
[Router-ip-pool-sta] quit
[Router] vlan batch 102
[Router] interface vlanif 102
[Router-Vlanif102] ip address 11.1.1.1 24
[Router-Vlanif102] dhcp select global
[Router-Vlanif102] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.10.10.0 24 11.1.1.2
```

Step 4 Configure RADIUS authentication and accounting.

Configure a RADIUS server template, an AAA authentication scheme, an AAA accounting scheme, and domain information.

```
[AP] radius-server template radius_huawei
[AP-radius-radius_huawei] radius-server authentication 12.1.1.1 1812
[AP-radius-radius_huawei] radius-server accounting 12.1.1.1 1813
[AP-radius-radius_huawei] radius-server shared-key simple huawei
[AP-radius-radius_huawei] quit
[AP] aaa
[AP-aaa] authentication-scheme radius_huawei
[AP-aaa-authen-radius_huawei] authentication-mode radius
[AP-aaa-authen-radius_huawei] quit
[AP-aaa] accounting-scheme radius_huawei
[AP-aaa-accounting-radius_huawei] accounting-mode radius
[AP-aaa-accounting-radius_huawei] quit
[AP-aaa] domain huawei.com
[AP-aaa-domain-huawei.com] authentication-scheme radius_huawei
[AP-aaa-domain-huawei.com] accounting-scheme radius_huawei
[AP-aaa-domain-huawei.com] radius-server radius_huawei
[AP-aaa-domain-huawei.com] quit
[AP-aaa] quit
```

Test whether a STA can be authenticated using RADIUS authentication.

```
[AP] test-aaa test@huawei.com 123456 radius-template radius_huawei
Info: Account test succeed.
```

Step 5 Configure Portal authentication.

Configuring Portal server parameters.

```
[AP] web-auth-server test
[AP-web-auth-server-test] server-ip 13.1.1.1
[AP-web-auth-server-test] port 50100
[AP-web-auth-server-test] shared-key simple huawei
[AP-web-auth-server-test] url http://13.1.1.1
[AP-web-auth-server-test] quit
```

Bind VLAN 101 to the Portal server.

```
[AP] interface vlanif 101
[AP-Vlanif101] web-auth-server test direct
[AP-Vlanif101] quit
```

Step 6 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 7 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 8 Configure Portal authentication on the WLAN-BSS interface.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] force-domain name huawei.com
[AP-Wlan-Bss1] permit-domain name huawei.com
[AP-Wlan-Bss1] quit
```

Step 9 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 10 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- The wireless PC obtains an IP address after it associates with the WLAN.
- Open a browser on the STA to access the Internet. The Portal authentication web page is automatically displayed. Enter the user name and password. The STA is authenticated and can access the WLAN.

----End

Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 101 to 104
#
interface GigabitEthernet0/0/1
 port link-type trunk
```

```
 port trunk allow-pass vlan 101 to 104
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 103
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 104
#
return
```

- Configuration file of Router

```
#
sysname Router
#
 vlan batch 102
#
dhcp enable
#
ip pool sta
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
#
interface Vlanif102
 ip address 11.1.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 102
#
ip route-static 10.10.10.0 24 11.1.1.2
#
return
```

- Configuration file of the AP

```
#
 sysname AP
#
 vlan batch 101 to 104
#
dhcp enable
#
dhcp relay detect enable
#
radius-server template radius_huawei
 radius-server authentication 12.1.1.1 1812 weight 80
 radius-server accounting 12.1.1.1 1813 weight 80
 radius-server shared-key cipher %@%@hH67%f}f8X"AE&Pw`wS~{:;0%@%@
#
web-auth-server test
 server-ip 13.1.1.1
 port 50100
 shared-key cipher %@%@w^y1$5h,lGXtWH(R+B'0{GM{%@%@
 url http://13.1.1.1
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 accounting-scheme radius_huawei
  accounting-mode radius
 domain huawei.com
```

```
  authentication-scheme radius_huawei
  accounting-scheme radius_huawei
  radius-server radius_huawei
#
interface Vlanif101
 ip address 10.10.10.1 255.255.255.0
 web-auth-server test direct
 dhcp select relay
 dhcp relay server-ip 11.1.1.1
#
interface Vlanif102
 ip address 11.1.1.2 255.255.255.0
#
interface Vlanif103
 ip address 12.1.1.2 255.255.255.0
#
interface Vlanif104
 ip address 13.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 104
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 permit-domain name huawei.com
 force-domain name huawei.com
#
ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

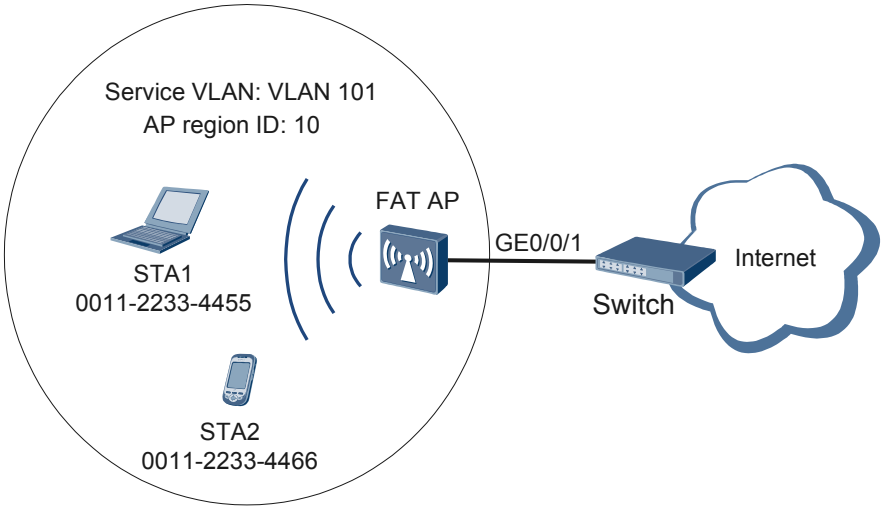
6.8.9 Example for Configuring a STA Whitelist

Networking Requirements

As shown in **Figure 6-28**, an enterprise provides a WLAN with the SSID of **test** for management personnel to access the enterprise network. STAs automatically obtain IP addresses.

The WLAN has a fixed small coverage and faces no external attack risks. MAC addresses of management personnel's wireless terminals can be added to a STA whitelist, preventing common employees from accessing the WLAN.

Figure 6-28 Networking diagram for configuring a STA whitelist



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a STA whitelist. Add MAC addresses of management personnel's wireless terminals to the whitelist. To prevent configuration impacts on other VAPs, configure the STA whitelist for a VAP, instead of an AP.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a STA whitelist for a VAP.

Configure a STA whitelist profile and add MAC addresses of STA1 and STA2 to the whitelist.

```
[AP] wlan
[AP-wlan-view] sta-whitelist-profile name whitelist id 1
[AP-wlan-whitelist-prof-whitelist] sta-mac 0011-2233-4455
[AP-wlan-whitelist-prof-whitelist] sta-mac 0011-2233-4466
[AP-wlan-whitelist-prof-whitelist] quit
```

Bind the service set to the STA whitelist profile and enable the STA whitelist function.

```
[AP-wlan-view] service-set name test
[AP-wlan-service-set-test] sta-access-mode whitelist
[AP-wlan-service-set-test] sta-whitelist-profile id 1
```

```
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 6 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 7 Verify the configuration.

The WLAN with SSID **test** is available for STAs connected to the AP.

STA1 and STA2 can connect to the WLAN, while STAs that are not in the whitelist cannot access the WLAN.

----End

Configuration Files

- Configuration file of the AP wireless side

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 sta-whitelist-profile name whitelist id 1
  sta-mac 0011-2233-4455
  sta-mac 0011-2233-4466
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
  sta-access-mode whitelist
  sta-whitelist-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

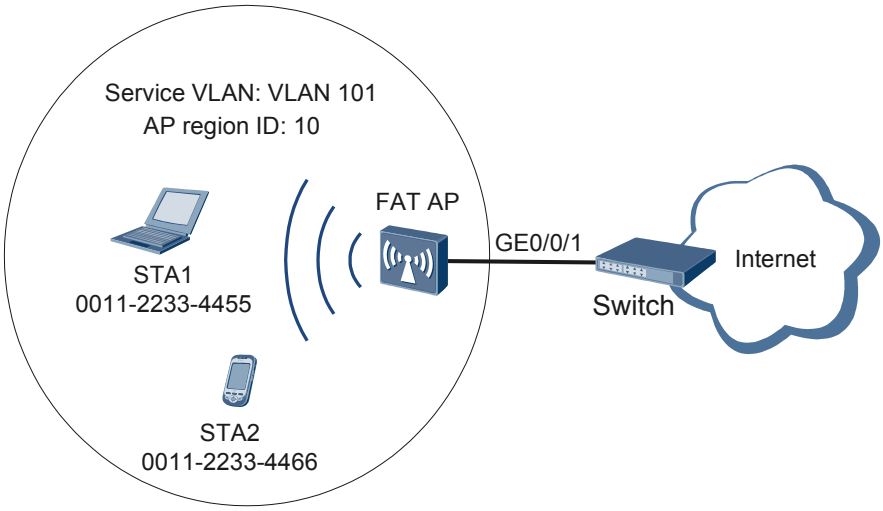
6.8.10 Example for Configuring a STA Blacklist

Networking Requirements

As shown in **Figure 6-29**, an enterprise provides a WLAN with the SSID of **test** for employees to access the enterprise network. STAs automatically obtain IP addresses.

The WLAN has a fixed small coverage and faces no external attack risks. Some faulty STAs may frequently go online and offline, degrading WLAN network stability. To prevent this situation, management personnel can add MAC addresses of the faulty STAs to a blacklist to prevent these STAs from accessing the WLAN. STAs that are not in the blacklist can access the WLAN.

Figure 6-29 Networking diagram for configuring a STA blacklist



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a STA blacklist for an AP. Add MAC addresses of some STAs to the blacklist to prevent the STAs from associating with the AP.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
```

```
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a STA blacklist for an AP.

```
[AP] wlan
[AP-wlan-view] sta-blacklist 0011-2233-4455
[AP-wlan-view] sta-blacklist 0011-2233-4466
[AP-wlan-view] sta-access-mode blacklist
[AP-wlan-view] quit
```

Step 6 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 7 Verify the configuration.

The WLAN with SSID **test** is available for STAs connected to the AP.

STA1 and STA2 cannot access the WLAN.

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 sta-blacklist 0011-2233-4455
 sta-blacklist 0011-2233-4466
 sta-access-mode ap 0 blacklist
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

6.9 FAQ

6.9.1 Why Cannot Users Associate with APs When WPA-PSK Authentication Is Used?

The possible causes are as follows:

- The STA does not support WPA2-PSK. For example, the computer runs an early version of Windows XP without patches installed, the computer may not support WPA2-PSK. Patches need to be installed on the computer.

6.9.2 Why Cannot STA Associate with an AP When WEP Authentication Is Used?

The possible causes are as follows:

- No WEP SSID is added to the STA. Many STAs associate with WEP SSIDs by using encryption without authentication. However, the AP uses both authentication and encryption. Therefore, the STA cannot associate with the SSID. The SSID must be manually configured on the STA. At last, set the encryption type to share mode.
- The key index configured on the AP is different from the key index on the STA. By default, the key index of an AP is 0 (ranging from 0 to 3), and the key index of STA is 1 (ranging from 1 to 4). Key index 0 on the AP matches key index 1 on the STA.

6.9.3 What Are Advantages and Disadvantages of WAPI Authentication?

WLAN authentication and Privacy Infrastructure (WAPI) has three independent elements: STA, AP, and Authentication Service Unit (ASU), to ensure authentication security. Encryption keys are generated after negotiation. WAPI authentication uses the SMS4 algorithm and supports 802.1X authentication applying to a large-scale network.

WAPI applies to scenarios requiring high security level. In WAPI authentication, the ASU server must check certificates, which requires support from STAs. Currently, a few STAs support WAPI. STA hardware needs to be upgraded to support WAPI. Software application is not widely used because of its low efficiency.

6.9.4 What Is the Difference Between Portal Authentication and 802.1X Authentication?

Portal authentication and 802.1X authentication are similar at the network side. Portal authentication is simple but has poor information security. 802.1X authentication is complex to install and configure but ensures high information security. The two authentication modes are used based on service types. 802.1X authentication is recommended for scenarios requiring high security. The combination of portal authentication and 802.1X authentication is used to meet

requirements of different service on the existing networks. The following table shows the comparisons between portal authentication and 802.1X authentication.

Item	Portal	802.1X
Client	Only requires a browser and does not require a client.	Requires a dedicated 802.1X client.
Server	Requires a portal server.	Requires a dedicated RADIUS server.
Installation and configuration	Requires no configuration and is easy to use.	Requires multiple configuration steps.
Encryption	Does not encrypt data.	Uses dynamic WEP encryption.
Security	Passwords entered on web pages are encrypted by SSL. Network traffic is not encrypted and can be intercepted by anyone. No other security measures are required.	802.1X authentication provides higher security than portal authentication. 802.1X encapsulates authentication packets in EAP format and supports multiple encryption algorithms. EAP-TLS, EAP-MD5, and EAP-SIM authentication modes are used based on the site requirements. Certificates are obtained to authenticate clients and servers.

6.9.5 What Authentication Protocols Are Supported During STA Login? Which One Is Recommended and Why?

The following authentication modes are supported: 802.1X, MAC, Portal, MAC+Portal, EAP-TLS, EAP-PEAP, and EAP-PAP. The MAC+Portal mode is recommended. This mode is secure and easy to use. No client is required. Users do not need to enter passwords in a specified period.

6.9.6 Why Does a STA Fail to Associate with an AP When WEP and TKIP Encryption Is Configured in 802.11n Mode?

The 802.11n mode define the WEP or TKIP encryption mode. When the two encryption modes are used, STAs may fail to associate with the AP.

6.9.7 How Can I Separate Two STAs that Connect to the Same SSID?

Huawei APs support Layer 2 isolation. When Layer 2 isolation is enabled, STAs cannot communicate at Layer 2. Only the upstream interface and virtual access point (VAP) interface can exchange data.

6.10 References

This section lists references of WLAN security.

The following table lists the reference for this feature.

Document	Description	Remarks
IEEE 802.11i	Medium Access Control (MAC) Security Enhancements	-

7 Configuration Guide - Security

About This Chapter

This document describes the principles and configurations of Security, and provides configuration examples.

7.1 AAA Configuration
The AAA-capable device checks validity of users and assigns rights to authorized users to ensure network security.

7.2 NAC Configuration
This section describes principles and configuration methods of NAC and provides configuration examples.

7.3 ACL Configuration
An access control list (ACL) is a set of rules that classify packets into different types. This chapter explains how to configure an ACL on a AP to filter packets.

7.4 Local Attack Defense Configuration
Local attack defense limits the rate of packets sent to the CPU, ensuring device security and uninterrupted services when attacks occur.

7.5 Attack Defense Configuration
Attack defense is a network security feature. Attack defense allows the device to identify various types of network attacks and protect itself and the connected network against malicious attacks to ensure device and network operation.

7.6 Traffic Suppression Configuration
This chapter describes basic concepts, configuration procedures and examples, and common configuration errors.

7.7 ARP Security Configuration
This chapter describes the principle and configuration methods of ARP security and provides configuration examples.

7.8 PKI Configuration
Using the PKI function, the device can obtain a digital certificate, which is used to verify the identifies of the two communication parties.

7.9 SSL Configuration

The Secure Sockets Layer (SSL) protocol protects information privacy on the Internet.

7.10 HTTPS Configuration

The Hypertext Transfer Protocol Secure (HTTPS) protocol provides secure web access using security mechanisms provided by the Secure Sockets Layer (SSL) protocol, including data encryption, identity authentication, and message integrity check.

7.1 AAA Configuration

The AAA-capable device checks validity of users and assigns rights to authorized users to ensure network security.

7.1.1 Overview

This section describes the definition, background, and functions of AAA.

Definition

Authentication, Authorization, and Accounting (AAA) provides a management mechanism for network security.

AAA provides the following functions:

- Authentication: verifies whether users are authorized for network access.
- Authorization: authorizes users to use particular services.
- Accounting: records the network resources used by users.

Users can only use one or more security services provided by AAA. For example, if a company wants to authenticate employees that access certain network resources, the network administrator only needs to configure an authentication server. If the company also wants to record operations performed by employees on the network, an accounting server is needed.

In summary, AAA authorizes users to access specific resources and records user operations. AAA is widely used because it features good scalability and facilitates centralized user information management. AAA can be implemented using multiple protocols. Currently, the device uses the Remote Authentication Dial-In User Service (RADIUS) or Huawei Terminal Access Controller Access Control System (HWTACACS) protocol to implement AAA. In most cases, the RADIUS protocol is used.

Purpose

AAA prevents unauthorized users from logging in to the device and improves system security.

7.1.2 Principles

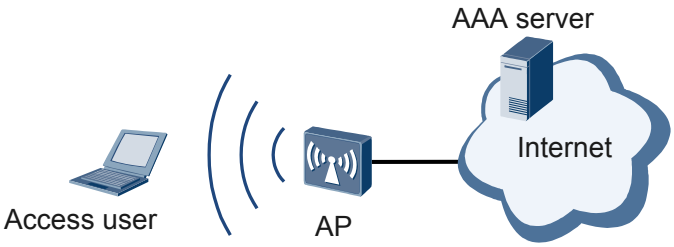
This section describes the implementation of AAA.

7.1.2.1 Concepts

AAA Architecture

AAA uses the client/server structure. AAA architecture features good scalability and facilitates centralized user information management. **Figure 7-1** shows the AAA architecture.

Figure 7-1 AAA architecture



Client/Server model of AAA

Authentication

AAA supports the following authentication modes:

- Non-authentication: Users are completely trusted without validity check. This mode is rarely used.
- Local authentication: User information is configured on the network access server (NAS). This mode features fast processing and low operation cost. The major limitation of local authentication is that information storage is subject to the device hardware capacity.
- Remote authentication: User information is configured on the authentication server. AAA can remotely authenticate users through the Remote Authentication Dial In User Service (**RADIUS**) or Huawei Terminal Access Controller Access Control System (**HWTACACS**) protocol.

Authorization

AAA supports the following authorization modes:

- Non-authorization: Users are not authorized.
- Local authorization: authorizes users according to the attributes configured on the NAS for the local user accounts.
- HWTACACS authorization: authorizes users through the HWTACACS server.
- If-authenticated authorization: applies to scenarios where users must be authenticated and the authentication process is separated from the authorization process. That is, this mode is available for only local authentication and HWTACACS authentication, and is unavailable for RADIUS authentication.
  - After local authentication is successful, local authorization is used.
  - After HWTACACS authentication is successful, all rights are enabled. That is, HWTACACS authorization is not required.
- RADIUS authorization: Users pass the RADIUS authorization upon passing the RADIUS authentication. RADIUS integrates authentication and authorization. Therefore, RADIUS authorization cannot be performed separately.

Accounting

AAA supports the following accounting modes:

- Non-accounting: Users are not charged.
- Remote accounting: supports remote accounting through the RADIUS or HWTACACS server.

7.1.2.2 RADIUS Protocol

7.1.2.2.1 RADIUS Protocol Overview

RADIUS uses the client/server model in distributed mode and protects a network from unauthorized access. It is often used in network environments that require high security and control remote user access. It defines the User Datagram Protocol (UDP)-based RADIUS packet format and message transmission mechanism, and specifies UDP ports 1812 and 1813 as the authentication and accounting ports respectively.

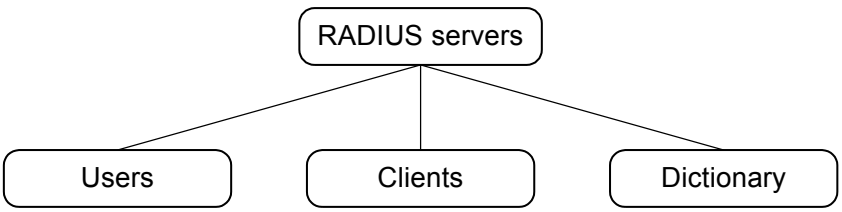
At the beginning, RADIUS was only the AAA protocol used for dial-up users. When diversified user access modes are used, RADIUS can also be applied to these access modes such as Ethernet access. RADIUS provides the access service through authentication and authorization and records the network resources used by users through accounting.

RADIUS has the following characteristics:

- Client/Server model
  - RADIUS client: RADIUS clients run on the network access servers (NAS) to transmit user information to the specified RADIUS server and process requests (for example, accept or reject user access) based on the responses from the servers. RADIUS clients can locate at any node on a network.

    As the RADIUS client, the device supports:
    - Standard RADIUS protocol and its extensions, including Request For Comments (RFC) 2865 and RFC 2866
    - Huawei-developed private attributes
    - Active detection on the RADIUS server status
    - Retransmission for Accounting Stop packets in the local buffer
    - Automatic switching function of the RADIUS server
- RADIUS server: RADIUS servers run on central computers and workstations to maintain user authentication and network service access information. The servers receive connection requests from users, authenticate the users, and send the responses (indicating that the requests are accepted or rejected) to the clients. RADIUS servers need to maintain three databases, as shown in **Figure 7-2**.

Figure 7-2 Databases maintained by the RADIUS servers



  - Users: stores user information such as user names, passwords, protocols, and IP addresses.
  - Clients: stores RADIUS client information such as the shared key and IP address of an access device.
  - Dictionary: stores the attributes in the RADIUS protocol and their value descriptions.
- Security mechanism

  RADIUS clients and servers exchange authentication messages using shared keys that cannot be transmitted through networks, which enhances information exchange security. In addition, passwords are encrypted using shared keys before being transmitted to avoid theft on an insecure network.
- Fine scalability

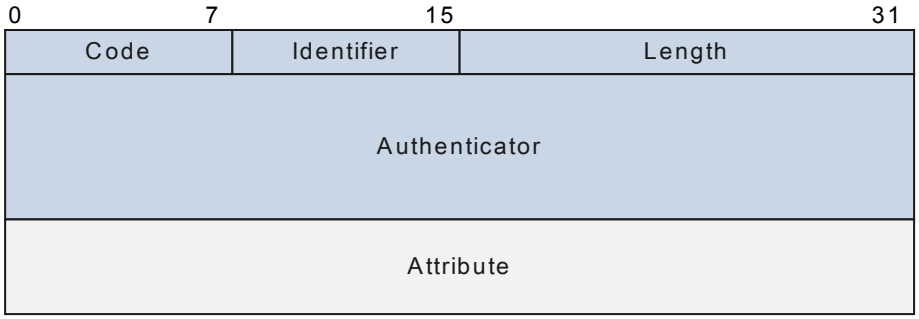
  RADIUS packets consist of the packet header and a certain number of attributes. After new attributes are added to RADIUS packets, its implementation remains unchanged.

7.1.2.2.2 RADIUS Packet Overview

RADIUS Packet Format

RADIUS uses UDP packets to transmit information. **Figure 7-3** shows the RADIUS packet format.

Figure 7-3 RADIUS packet format



Fields in a RADIUS packet include:

- Code: 1 byte. It describes the RADIUS packet type. The Code value varies in different types of RADIUS packets. For example, the value 1 indicates an Access-Request packet, and the value 2 indicates an Access-Accept packet.
- Identifier: 1 byte. It is used to match request packets and reply packets, and detect the request packets retransmitted within a certain period. After a client sends a request packet, the server sends a reply packet with the same Identifier value as the request packet.
- Length: 2 bytes. It specifies the RADIUS packet length. Bytes out of the specified length value are treated as padding and ignored on the receiver. If the length of a received packet is smaller than the Length value, the packet is discarded.
- Authenticator: 16 bytes. It is used to verify the reply packets sent by the RADIUS server and encrypt user password.

- Attribute: variable length. It is the content of a packet carrying authentication, authorization, and accounting information and providing configuration details of request and reply packets. An Attribute field may contain multiple attributes, each of which consists of Type, Length, and Value. For details, see **7.1.2.2.4 RADIUS Attributes**.
  - Type: 1 byte. It indicates the attribute type. The value ranges from 1 to 255.
  - Length: It indicates the length of an attribute (including type, length, and attribute). The unit is byte.
  - Value: It indicates the attribute information. The format and content are dependent on Type and Length. The maximum length is 253 bytes.

RADIUS Packet Type

RADIUS defines 16 tytes of packets. **Table 7-1** describes the authentication packets, **Table 7-2** describes the accounting packets, and **Table 7-3** describes the authorization packets.

Table 7-1 RADIUS authentication packet

Packet Name	Description
Access-Request	This is the first packet transmitted in a RADIUS interaction process. This packet carries user authentication information, such as user name and password. The Access-Request packet is from the RADIUS client to the RADIUS server. The RADIUS server determines whether a user is allowed to access the network according to the user information carried in this packet.
Access-Accept	This packet is sent by the RADIUS server to respond to the Access-Request packet sent by the client. If all attributes in the Access-Request packet are acceptable, the server considers that the user passes the authentication and sends this packet. After receiving this packet, the client grants the network access rights to the user.
Access-Reject	This packet is sent by the RADIUS server to respond to the Access-Request packet sent by the client. If any attribute in the Access-Request packet is unacceptable, the RADIUS server considers that the user fails the authentication and sends this packet.
Access-Challenge	During an EAP authentication, when the RADIUS server receives an Access-Request packet carrying the user name, it generates a random MD5 challenge and sends the MD5 challenge to the client through this packet. After the client encrypts the user password using the MD5 challenge, the client sends the encrypted password in an Access-Request packet to the RADIUS server. The RADIUS server compares the encrypted password received from the client with the locally encrypted password. If they are the same, the server considers the user valid.

Table 7-2 RADIUS accounting packet

Packet Name	Description
Accounting-Request (Start)	If the client uses RADIUS accounting, the client sends this packet to the server before accessing network resources.
Accounting-Response (Start)	After receiving and recording the Accounting-Request (Start) packet, the server returns this packet to the client.
Accounting-Request (Interim-update)	If the accounting server fails to receive the Accounting-Request (Stop) packet, the server cannot stop accounting for the user. To address this problem, configure interim accounting on the client. The client then periodically sends accounting packets to the server.
Accounting-Response (Interim-update)	After receiving an Accounting-Request (Interim-update) packet, the server returns this packet to the client.
Accounting-Request (Stop)	When a user goes offline voluntarily or is forcibly disconnected, the client sends this packet carrying the network resource usage information (including online duration and number of incoming/outgoing bytes) to the server, requesting the server to stop accounting.
Accounting-Response (Stop)	After receiving an Accounting-Request (Stop) packet, the server sends this packet to the client.

Table 7-3 RADIUS authorization packet

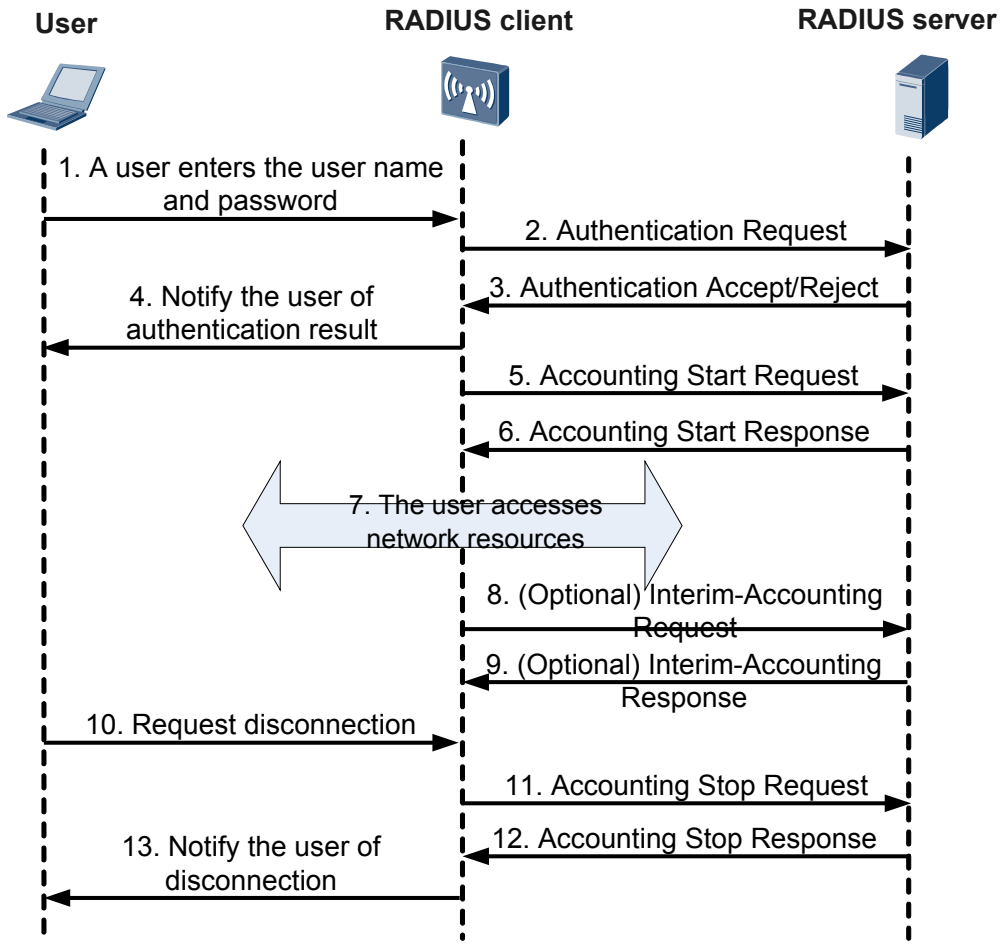
Packet Name	Description
CoA-Request	When the administrator needs to modify the rights of an online user (for example, prohibit the user from accessing a website), the server sends this packet to the client, requesting the client to modify the user rights.
CoA-ACK	If the client successfully modifies the user rights, the client sends this packet to the server.
CoA-NAK	If the client cannot modify the user rights, the client sends this packet to the server.
DM-Request	When the administrator needs to disconnect a user, the server sends this packet to the client, requesting the client to disconnect the user.
DM-ACK	If the client successfully disconnects the user, the client sends this packet to the server.
DM-NAK	If the client cannot disconnect the user, the client sends this packet to the server.

7.1.2.2.3 RADIUS Interaction Process

RADIUS Authentication, Authorization, and Accounting

The access device functions as a RADIUS client to collect user information, including user name and password, and sends the information to the RADIUS server. The RADIUS server authenticates users according to the information, and performs authorization and accounting for the users after the users are authenticated. **Figure 7-4** shows information exchanged between a user, the RADIUS client, and the RADIUS server.

Figure 7-4 RADIUS authentication, authorization, and accounting process



1. A user sends a connection request carrying the user name and password to the RADIUS client (access device).
2. The RADIUS client sends an Access-Request packet containing the user identity information to the RADIUS server according to the user name and password.
3. The RADIUS server verifies the user identity:
   - If the user identity is valid, the RADIUS server returns an Access-Accept packet to the RADIUS client. The Access-Accept packet contains authorization information.

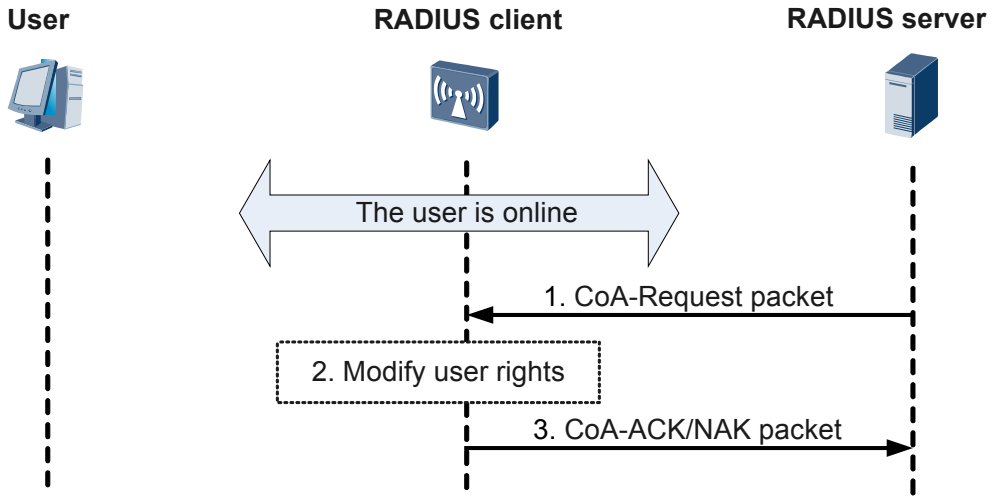
- If the user identity is invalid, the RADIUS server returns an Access-Reject packet to the RADIUS client to reject access from the user.

4. The RADIUS client notifies the user whether authentication is successful.
5. The RADIUS client permits or rejects the user according to the authentication result. If the user is permitted, the RADIUS client sends an Accounting-Request (Start) packet to the RADIUS server.
6. The RADIUS server sends an Accounting-Response (Start) packet to the RADIUS client and starts accounting.
7. The user starts to access network resources.
8. (Optional) If interim accounting is enabled, the RADIUS client periodically sends Accounting-Request (Interim-update) packets to the RADIUS server, preventing incorrect accounting result caused by unexpected user disconnection.
9. (Optional) The RADIUS server returns Accounting-Response (Interim-update) packets and performs interim accounting.
10. The user sends a logout request.
11. The RADIUS client sends an Accounting-Request (Stop) packet to the RADIUS server.
12. The RADIUS server sends an Accounting-Response (Stop) packet to the RADIUS client and stops accounting.
13. The RADIUS client notifies the user of the processing result, and the user stops accessing network resources.

CoA

Change of Authorization (CoA) allows the administrator to change the right of an authenticated online user through RADIUS. For example, a VLAN ID can be delivered to some access users through CoA packets, so that they belong to the same VLAN no matter which interfaces they connect to. **Figure 7-5** shows the CoA interaction process.

Figure 7-5 CoA interaction process



1. The RADIUS server sends a CoA-Request packet to the RADIUS client according to service information, requesting the client to modify user authorization information. The

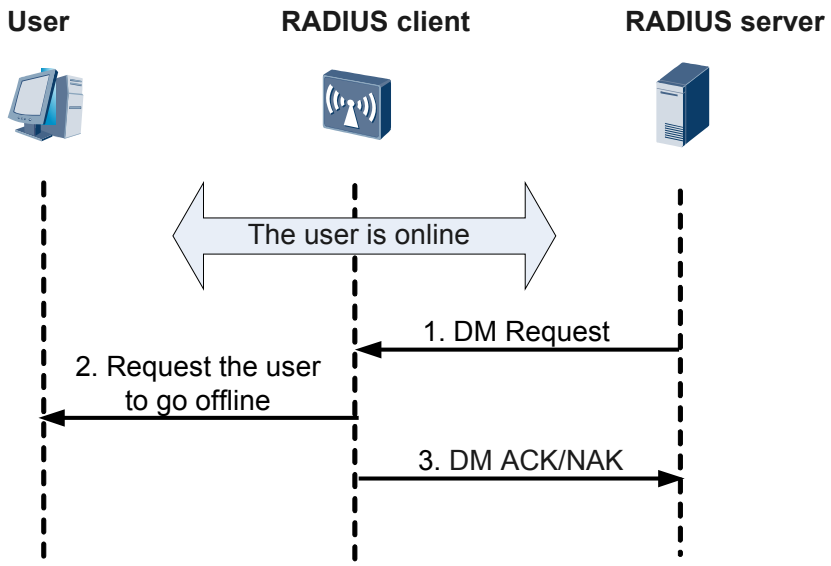
CoA-Request packet may contain the policy name (configured on the RADIUS client) or ACL rules.

2. The RADIUS client modifies user authorization information according to the CoA-Request packet without disconnecting the user.
3. The RADIUS client returns a CoA-ACK or CoA-NAK packet.
   - If the authorization information is modified (for example, the policy name in the CoA packet is the same as that configured on the client), the RADIUS client returns a CoA-ACK packet to the RADIUS server.
   - If the authorization information cannot be modified, the RADIUS client returns a CoA-NAK packet to the RADIUS server.

DM

When a user needs to be disconnected forcibly, the RADIUS server sends a Disconnect Message (DM) to the RADIUS client. **Figure 7-6** shows the DM interaction process.

Figure 7-6 DM interaction process



1. The administrator forcibly disconnects a user on the RADIUS server. The RADIUS server sends a DM Request packet to the RADIUS client, requesting the client to disconnect the user.
2. When receiving the DM Request packet, the RADIUS client requests the user to go offline.
3. The RADIUS client returns a DM-ACK or DM-NAK packet.
   - If the user successfully goes offline, the RADIUS client returns a DM ACK packet to the RADIUS server.
   - If the user cannot go offline, the RADIUS client returns a DM NAK packet to the RADIUS server.

7.1.2.2.4 RADIUS Attributes

RADIUS attributes are classified into **Standard RADIUS Attributes** and **Huawei Proprietary RADIUS Attributes**. Different RADIUS packets have different RADIUS attributes. For details, see **RADIUS Attributes Available in Packets**.

Standard RADIUS Attributes

RFC2865, RFC2866, and RFC3576 define standard RADIUS attributes, which are supported by all mainstream vendors. For details, see **Table 7-4**.

Table 7-4 Standard RADIUS attributes

Attribute No.	Attribute Name	Description
1	User-Name	User name for authentication. The user name format can be "user name @ domain name", or just "user name."
2	User-Password	User password for authentication, which is only valid for the Password Authentication Protocol (PAP).
3	CHAP-Password	User password for authentication, which is only valid for the Challenge Handshake Authentication Protocol (CHAP).
4	NAS-IP-Address	Internet Protocol (IP) address carried in the authentication request packet sent by the NAS. If the RADIUS server is bound to an interface, the attribute is set to the IP address of the bound interface. Otherwise, the attribute is set to the IP address of the interface that sends RADIUS packets.
5	NAS-Port	User access physical port, which is in either of the following formats: ● new: slot ID (8 bits) + sub-slot ID (4 bits) + port number (8 bits) + Virtual Local Area Network (VLAN) ID (12 bits) ● old: slot ID (12 bits) + port number (8 bits) + VLAN ID (12 bits)
6	Service-Type	Service type of the user to be authenticated. ● 1 (Login): Web user ● 2 (Framed): PPP or 802.1x user ● 10 (Call Check): MAC address authentication user or MAC address bypass authentication user
7	Framed-Protocol	Encapsulation protocol of Frame services. ● For a non-management user, the value is fixed as 1. ● For a management user, the value is fixed as 6.
8	Framed-IP-Address	User IP address.

Attribute No.	Attribute Name	Description
11	Filter-Id	User group or user Access Control List (ACL) ID. A RADIUS packet cannot carry the ACL ID and user group name simultaneously. **NOTE** This attribute can only carry the ACL IDs ranging from 3000 to 3999.
12	Framed-MTU	MTU of the data link between user and NAS. For example, in 802.1x Extensible Authentication Protocol (EAP) authentication, the NAS specifies the maximum length of the EAP packet in this attribute. An EAP packet larger than the link MTU will cause packet loss.
14	Login-IP-Host	Management user IP address. ● If the value is 0 or 0xFFFFFFFF, the IP address of management user is not checked. ● If this attribute uses other values, the device checks whether the management user IP address is the same as the delivered attribute value.
15	Login-Service	Service type available to management users: ● 0: telnet ● 5: X25-PAD ● 50: SSH ● 51: FTP ● 52: Terminal **NOTE** An attribute can contain multiple service types.
18	Reply-Message	Access-Accept or Access-Reject packet. ● The Access-Accept packet indicates that a user is successfully authenticated. ● The Access-Reject packet indicates that a user fails in authentication.
19	Callback-Number	Information sent from the authentication server and to be displayed to a user, such as the mobile number.
24	State	If the RADIUS server sends a RADIUS Access-Challenge packet carrying the State attribute to a device, the subsequent RADIUS Access-Request packets sent from the device must carry the State attribute with the same value.
25	Class	If the RADIUS server sends a RADIUS Access-Accept packet carrying the Class attribute to the NAS, the subsequent RADIUS Accounting-Request packets sent from the NAS must carry the Class attribute with the same value.

Attribute No.	Attribute Name	Description
26	Vendor-Specific	Vendor-specific attribute. For details, see **Table 7-5**. A packet can carry one or multiple private attributes. Each private attribute contains one or multiple sub-attributes.
27	Session-Timeout	In the Access-Request packet, this attribute indicates the maximum number of seconds of service to be provided to the user before termination of the session or prompt. In the Access-Challenge packet, this attribute indicates the reauthentication duration of EAP authentication users. **NOTE** This attribute is only valid for 802.1x authentication users.
28	Idle-Timeout	The maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. **NOTE** This attribute is only valid for Portal authentication users.
29	Termination-Action	The action taken by the NAS to finish user services. ● 0: forcible disconnection ● 1: Reauthentication **NOTE** This attribute is only valid for 802.1x authentication users.
30	Called-Station-Id	Number of the NAS. ● Generally, It is the NAS MAC address for wired users. ● It is the SSID for wireless users.
31	Calling-Station-Id	Number of the client. Generally, it is the MAC address of the client.
32	NAS-Identifier	Host name of the NAS.
40	Acct-Status-Type	Accounting-Request type: ● 1: Accounting-Start packet ● 2: Accounting-Stop packet ● 3: Interim-Accounting packet
41	Acct-Delay-Time	Number of seconds the client has been trying to send the accounting packet (excluding the network transmission time).

Attribute No.	Attribute Name	Description
44	Acct-Session-Id	Accounting session ID. The Accounting-Start, Interim-Accounting, and Accounting-Stop packets of the same accounting session must have the same session ID. The format of this attribute is: Host name (7 bits) + Slot ID (2 bits) + Subcard number (1 bit) + Port number (2 bits) + Outer VLAN ID (4 bits) + Inner VLAN ID (5 bits) + Central Processing Unit (CPU) TICK (6 bits) + user connection ID (6 bits).
45	Acct-Authentic	User authentication mode: ● 1: RADIUS authentication ● 2: Local authentication ● 3: Other remote authentications
46	Acct-Session-Time	How long a user has been online, in seconds. **NOTE** If the administrator modifies the system time after the user goes online, the online time calculated by the device may be incorrect.

Attribute No.	Attribute Name	Description
49	Acct-Terminate-Cause	Reason why a user connection is torn down: ● User-Request(1): The user requests termination of service. ● Lost Carrier (2): The connection is torn down due to a handshake failure or heartbeat timeout, for example, an ARP probe failure or PPP handshake failure. ● Lost Service (3): The connection initiated by the peer device is torn down. ● Idle Timeout (4): The idle timer expires. ● Session Timeout (5): The session times out or the traffic threshold is reached. ● Admin Reset (6): The administrator forces the user to go offline. ● Admin Reboot (7): The administrator restarts the NAS. ● Port Error (8): A port fails. ● NAS Error (9): The NAS encounters an internal error. ● NAS Request (10): The NAS ends session for resource change. ● NAS Reboot (11): The NAS automatically restarts. ● Port Unneeded (12): The port is Down. ● Port Preempted (13): The port is occupied. ● Port Suspended (14): The port is suspended. ● Service Unavailable (15): The service is unavailable. ● Callback (16): NAS is terminating current session in order to perform callback for a new session. ● User Error (17): User authentication fails or times out. ● Host Request (18): A host sends a request.
55	Event-Timestamp	Time when an Accounting-Request packet is generated. The value is the number of seconds elapsed since 00:00:00 of January 1, 1970.
60	CHAP-Challenge	Challenge field in CHAP authentication. This field is generated by the NAS for Message Digest algorithm 5 (MD5) calculation.
61	NAS-Port-Type	NAS port type. The attribute value can be configured in the interface view. By default, the type is Ethernet (15).
64	Tunnel-Type	Protocol type of the tunnel. The value is fixed as 13, indicating VLAN.
65	Tunnel-Medium-Type	Medium type used on the tunnel. The value is fixed as 6, indicating Ethernet.

Attribute No.	Attribute Name	Description
79	EAP-Message	Encapsulates Extended Access Protocol packets so that RADIUS supports EAP authentication. When an EAP packet is longer than 253 bytes, the packet is encapsulated into multiple attributes. A RADIUS packet can carry multiple EAP-Message attributes.
80	Message-Authenticator	Authenticates and verifies authentication packets to prevent spoofing packets. This attribute is used only when RADIUS supports EAP authentication.
81	Tunnel-Private-Group-ID	Tunnel private group ID, which is used to deliver user VLAN IDs.
85	Acct-Interim-Interval	Interim accounting interval.
87	NAS-Port-Id	User access port, in either of the following formats: ● New: – For Ethernet access users, the NAS port ID is in the format "slot=xx; subslot=xx; port=xxx; VLAN ID=xxxx", in which "slot" ranges from 0 to 15, "subslot" 0 to 15, "port" 0 to 255, and "VLAN ID" 1 to 4094. – For ADSL access users, the NAS port ID is in the format "slot=xx; subslot=x; port=x; VPI=xxx; VCI=xxxxx", in which "slot" ranges from 0 to 15, "subslot" 0 to 9, "port" 0 to 9, "VPI" 0 to 255, and "VCI" 0 to 65535. ● Old: – For Ethernet access users, the NAS port ID format is port number (2 characters) + sub-slot ID (2 bytes) + card number (3 bytes) + VLAN ID (9 characters). – For ADSL access users: port number (2 characters) + sub-slot ID (2 bytes) + card number (3 bytes) + VPI (8 characters) + VCI (16 characters). The fields are prefixed with 0s if they contain less bytes than specified.

Huawei Proprietary RADIUS Attributes

The RADIUS protocol has good extensibility. The No. 26 attribute (Vendor-Specific) defined in RFC2865 is used to extend RADIUS to implement the functions not supported by standard RADIUS attributes. **Table 7-5** describes Huawei proprietary RADIUS attributes.

Table 7-5 Huawei proprietary RADIUS attributes

Attribute No.	Attribute Name	Description
26-1	HW-Input-Peak-Information-Rate	Peak rate at which the user accesses the NAS, in bit/s.
26-2	HW-Input-Committed-Information-Rate	Average rate at which the user accesses the NAS, in bit/s.
26-3	HW-Input-Committed-Burst-Size	Committed burst size at which the user accesses the NAS, in bit/s.
26-4	HW-Output-Peak-Information-Rate	Peak rate at which the NAS connects to the user, in bit/s.
26-5	HW-Output-Committed-Information-Rate	Average rate at which the NAS connects to the user, in bit/s.
26-6	HW-Output-Committed-Burst-Size	Committed burst size at which the NAS connects to the user, in bit/s.
26-22	HW-Priority	Priority of user service. **NOTE** If the RADIUS server has delivered this attribute, the HW-Up-Priority and HW-Down-Priority attributes are invalid.
26-26	HW_ConnectID	Index of a user connection.
26-28	HW-FTP-Directory	Initial directory of an FTP user.
26-29	HW-Exec-Privilege	Management user (such as Telnet user) priority, ranging from 0 to 16. The value 16 indicates that the user does not have the administrator rights.
26-59	HW-Startup-Time-Stamp	NAS start time, which is the number of seconds elapsed since 00:00:00 of January 1, 1970.
26-60	HW-IP-Host-Address	User IP address and MAC address carried in authentication and accounting packets, in the format A.B.C.D HH:HH:HH:HH:HH:HH. There is a space between the IP address and MAC address. If the user's IP address is detected invalid during authentication, A.B.C.D is set to 255.255.255.255.
26-61	HW-Up-Priority	Upstream priority of user service.
26-62	HW-Down-Priority	Downstream priority of user service.
26-77	HW-Input-Peak-Burst-Size	Upstream peak rate, in bit/s.
26-78	HW-Output-Peak-Burst-Size	Downstream peak rate, in bit/s.

Attribute No.	Attribute Name	Description
26-141	HW-AP-Information	AP MAC address used for wireless user authentication, in format H-H-H. H is a 4-bit hexadecimal number.
26-142	HW_User_Information	User security check information delivered by the RADIUS server to Extensible Authentication Protocol over LAN (EAPoL) user to notify the user of check items.
26-146	HW-Service-Scheme	Service scheme name. A service scheme contains user authorization information and policy.
26-155	HW-URL-Flag	Whether URL is forcibly pushed, for example, used together with HW-Portal-URL: ● 0: no ● 1: yes
26-156	HW-Portal-URL	Forcibly pushed Uniform Resource Locator (URL).
26-156	HW-Portal-URL	Forcibly pushed URL.
26-157	HW-Terminal-Type	Terminal type of user.
26-158	HW-DHCP-Option	DHCP Option, encapsulated in Type-Length-Value (TLV) format. A packet may contain multiple HW-DHCP-Option attributes to carry Option information.
26-159	HW-HTTP-UA	User-Agent information in Hypertext Transfer Protocol (HTTP) packets.
26-163	HW-LLDP-Info	LLDP information. A packet can contain multiple HW-LLDP-Info attributes to carry different options.
26-254	HW-Version	Software version running on the device.
26-255	HW-Product-ID	NAS product name.

RADIUS Attributes Available in Packets

Different RADIUS packets carry different RADIUS attributes. Different RADIUS attributes are available for different packets:

- For the RADIUS attributes available in authentication packets, see **Table 7-6**.
- For the RADIUS attributes available in accounting packets, see **Table 7-7**.
- For the RADIUS attributes available in authorization packets, see **Table 7-8**.

NOTE

- 1: indicates that the attribute must appear once in the packet.
- 0: indicates that the attribute cannot appear in the packet (it will be discarded if it is contained).
- 0-1: indicates that the attribute can appear once or does not appear in the packet.
- 0+: indicates that the attribute may appear multiple times or does not appear in the packet.

Table 7-6 RADIUS attributes available in authentication packets

Attribute No.	Access-Request	Access-Accept	Access-Reject	Access-Challenge
User-Name(1)	1	0	0	0
User-Password(2)	0-1	0	0	0
Chap-Password(3)	0-1	0	0	0
NAS-IP-Address(4)	1	0	0	0
NAS-Port(5)	1	0	0	0
Service-Type(6)	1	0-1	0	0
Framed-Protocol(7)	1	0-1	0	0
Framed-IP-Address(8)	0-1	0	0	0
Filter-Id(11)	0	0-1	0	0
Framed-MTU(12)	0-1	0	0	0
Login-IP-Host(14)	0-1	0-1	0	0
Login-Service(15)	0	0-1	0	0
Reply-Message(18)	0	0-1	0-1	0
Callback-Number(19)	0	0-1	0	0
State(24)	0-1	0-1	0	0-1
Class(25)	0	0-1	0	0
Session-Timeout(27)	0	0-1	0	0-1
Idle-Timeout(28)	0	0-1	0	0
Termination-Action(29)	0	0-1	0	0-1
Called_Station_Id(30)	0-1	0	0	0
Calling-Station-Id(31)	1	0	0	0
NAS-Identifier(32)	1	0	0	0
Acct-session-id(44)	1	0	0	0
CHAP_Challenge(60)	0-1	0	0	0

Attribute No.	Access-Request	Access-Accept	Access-Reject	Access-Challenge
NAS-Port-Type(61)	1	0	0	0
Tunnel-Type(64)	0	0-1	0	0
Tunnel-Medium-Type(65)	0	0-1	0	0
EAP-Message(79)	0-1	0-1	0-1	0-1
Message-Authenticator(80)	0-1	0-1	0-1	0-1
Tunnel-Private-Group-ID(81)	0	0-1	0	0
Acct_Interim_Interval(85)	0	0-1	0	0
NAS-Port-Id(87)	1	0	0	0
HW-Input-Peak-Information-Rate(26-1)	0	0-1	0	0
HW-Input-Committed-Information-Rate(26-2)	0	0-1	0	0
HW-Input-Committed-Burst-Size(26-3)	0	0-1	0	0
HW-Output-Peak-Information-Rate(26-4)	0	0-1	0	0
HW-Output-Committed-Information-Rate(26-5)	0	0-1	0	0
HW-Output-Committed-Burst-Size(26-6)	0	0-1	0	0
HW-Priority(26-22)	0	0-1	0	0
HW_ConnectID(26-26)	1	0	0	0
Ftp_directory(26-28)	0	0-1	0	0
HW-Exec-Privilege(26-29)	0	0-1	0	0
HW_Startup_Timestamp (26-59)	1	0	0	0
HW-IP-Host-Address(26-60)	1	0	0	0
HW-Up-Priority(26-61)	0	0-1	0	0
HW-Down-Priority(26-62)	0	0-1	0	0
HW-Input-Peak-Burst-Size (26-77)	0	0-1	0	0

Attribute No.	Access-Request	Access-Accept	Access-Reject	Access-Challenge
HW-Output-Peak-Burst-Size (26-78)	0	0-1	0	0
HW-URL-Flag(26-155)	0	0-1	0	0
HW-Portal-URL(26-156)	0	0-1	0	0
HW-Terminal-Type(26-157)	0-1	0-1	0	0
HW-DHCP-Option(26-158)	0+	0	0	0
HW-Version(26-254)	1	0	0	0
HW-Product-ID(26-255)	1	0	0	0

Table 7-7 RADIUS attributes available in accounting packets

Attribute No.	Accounting-Request (Start)	Accounting-Request (Interim-Update)	Accounting-Request (Stop)	Accounting-Response (start)	Accounting-Response (Interim-Update)	Accounting-Response (Stop)
User-Name(1)	1	1	1	0	0	0
NAS-IP-Address(4)	1	1	1	0	0	0
NAS-Port(5)	1	1	1	0	0	0
Service-Type(6)	1	1	1	0	0	0
Framed-Protocol(7)	1	1	1	0	0	0
Framed-IP-Address(8)	1	1	1	0	0	0
Class(25)	0-1	0-1	0-1	0	0	0
Session-Timeout(27)	0	0	0	0-1	0-1	0
Called-Station-Id(30)	1	1	1	0	0	0
Calling-Station-Id(31)	1	1	1	0	0	0
NAS-Identifier(32)	1	1	1	0	0	0
Acct-Status-Type(40)	1	1	1	0	0	0
Acct-Delay-Time(41)	0	1	1	0	0	0

Attribute No.	Accounting-Request (Start)	Accounting-Request (Interim-Update)	Accounting-Request (Stop)	Accounting-Response (start)	Accounting-Response (Interim-Update)	Accounting-Response (Stop)
Acct-Session-Id(44)	1	1	1	0	0	0
Acct-Authentic(45)	1	1	1	0	0	0
Acct-Session-Time(46)	0	1	1	0	0	0
Acct-Terminate-Cause (49)	0	0	1	0	0	0
Event-Timestamp(55)	1	1	1	0	0	0
NAS-Port-Type(61)	1	1	1	0	0	0
NAS-Port-Id(87)	1	1	1	0	0	0
NAS-IPv6-Address(95)	0-1	0-1	0-1	0	0	0
HW_ConnectID(26-26)	1	1	1	0	0	0
HW-IP-Host-Address (26-60)	1	1	1	0	0	0
HW-AP-Information (26-141)	0-1	0-1	0-1	0	0	0
HW-Terminal-Type (26-157)	0-1	0-1	0-1	0	0	0
HW-DHCP-Option (26-158)	0+	0+	0+	0	0	0
HW-HTTP-UA (26-159)	0-1	0-1	0-1	0	0	0

Table 7-8 RADIUS attributes available in COA/DM packets

Attribute No.	COA REQUEST	COA ACK	COA NAK	DM REQUEST	DM ACK	DM NAK
User-Name(1)	0-1	0-1	0-1	0-1	0-1	0-1
NAS-IP-Address(4)	0-1	0-1	0-1	0-1	0-1	0-1
NAS-Port(5)	0-1	0-1	0-1	0-1	0-1	0-1

Attribute No.	COA REQUEST	COA ACK	COA NAK	DM REQUEST	DM ACK	DM NAK
Framed-IP-Address(8)	0-1	0-1	0-1	0-1	0-1	0-1
Filter-Id(11)	0-1	0	0	0	0	0
Session-Timeout(27)	0-1	0	0	0	0	0
Calling-Station-Id(31)	0-1	0-1	0-1	0-1	0-1	0-1
NAS-Identifier(32)	0-1	0-1	0-1	0-1	0-1	0-1
Acct-Session-Id(44)	1	1	1	1	1	1
Acct_Interim_Interval (85)	0-1	0	0	0	0	0
HW-Input-Peak-Information-Rate(26-1)	0-1	0	0	0	0	0
HW-Input-Committed-Information-Rate(26-2)	0-1	0	0	0	0	0
HW-Output-Peak-Information-Rate(26-4)	0-1	0	0	0	0	0
HW-Output-Committed-Information-Rate(26-5)	0-1	0	0	0	0	0
HW-Priority(26-22)	0-1	0	0	0	0	0
HW-Up-Priority(26-61)	0-1	0	0	0	0	0
HW-Down-Priority (26-62)	0-1	0	0	0	0	0
HW-Data-Filter(26-82)	0-1	0	0	0	0	0

7.1.2.3 HWTACACS Protocol

7.1.2.3.1 HWTACACS Protocol Overview

HWTACACS is an enhancement to TACACS (RFC 1492). Similar to RADIUS, HWTACACS uses the client/server model to implement communication between NAS and HWTACACS servers.

HWTACACS is used to perform authentication, authorization, and accounting for the users accessing the Internet through Point-to-Point Protocol (PPP) or Virtual Private Dial-up Network (VPDN) and the management users. For example, an HWTACACS server can be configured to perform authentication, authorization, and accounting for the management users logging in to

the device. The device functions as the HWTACACS client to send the user names and passwords to the HWTACACS server. The authorized users can log in to the device and perform operations.

Both HWTACACS and RADIUS protocols can implement authentication, authorization, and accounting. They are similar in the following aspects:

- Client/server model
- Using a public key to encrypt user information
- Good flexibility and extensibility

Compared with RADIUS, HWTACACS is more reliable in transmission and encryption, and is more suitable for security control. **Table 7-9** lists the differences between HWTACACS and RADIUS.

Table 7-9 Comparisons between HWTACACS and RADIUS

HWTACACS	RADIUS
Transmits data through TCP, which is more reliable.	Transmits data through UDP, which is more efficient.
Encrypts the entire packet except for the standard HWTACACS header.	Encrypts only the password field in the packet.
Separates authentication from authorization so that authentication and authorization can be implemented on different security servers. For example, an HWTACACS server can perform authentication and the other one can perform authorization.	Combines authentication and authorization.
Supports command line authorization. The command line use is restricted by command level and AAA. When a user enters a command, the command is executed only after being authorized by the HWTACACS server.	Does not support command line authorization. The commands that a user can use depend on the user level. A user can only use the commands of the same level as or lower level than the user level.
Applies to security control.	Applies to accounting.

7.1.2.3.2 HWTACACS Packet Overview

Unlike RADIUS packets which all use the same format, HWTACACS packets use different formats. However, the **HWTACACS Authentication Packet**, **HWTACACS Authorization Packet**, and **HWTACACS Accounting Packet** use different formats except that they all share the same **HWTACACS Packet Header**.

HWTACACS Packet Header

All HWTACACS packets have a 12-byte packet header, as shown in **Figure 7-7**.

Figure 7-7 HWTACACS packet header

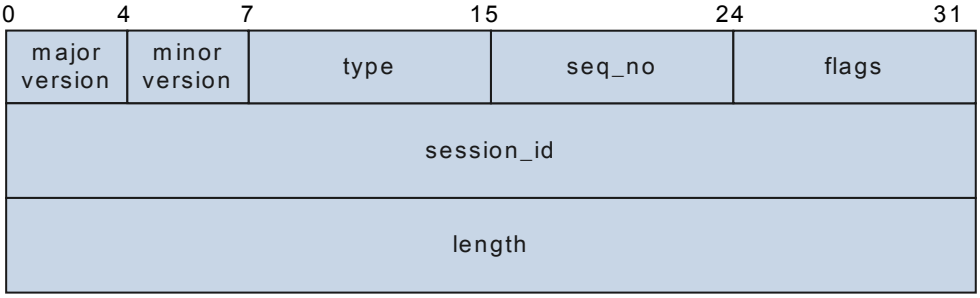


Table 7-10 Fields in HWTACACS packet header

Field	Description
major version	Major version of the HWTACACS protocol. The current version is 0xc.
minor version	Minor version of the HWTACACS protocol. The current version is 0x0.
type	HWTACACS protocol packet type, including authentication (0x01), authorization (0x02), and accounting (0x03).
seq_no	Packet sequence number in a session, ranging from 1 to 254.
flags	Encryption flag on the packet body. Only the first bit among the 8 bits is supported. The value 0 indicates to encrypt the packet body, and the value 1 indicates not to encrypt the packet body.
session_id	Session ID, which is the unique identifier of a session.
length	Length of the HWTACACS packet body, excluding the packet header.

HWTACACS Authentication Packet Format

HWTACACS authentication packets include:

- **Authentication Start**: When an authentication starts, the client sends this packet carrying the authentication type, user name, and authentication data to the server.
- **Authentication Continue**: When receiving the Authentication Response packet from the server, the client returns this packet if the authentication process is not ended.
- **Authentication Reply**: When the server receives the Authentication Start or Authentication Continue packet from the client, the server sends this packet to the client to notify the client of the current authentication status.

The HWTACACS authentication packets have different formats.

- Figure 7-8 shows the format of HWTACACS Authentication Start packets.

Figure 7-8 HWTACACS Authentication Start packet format

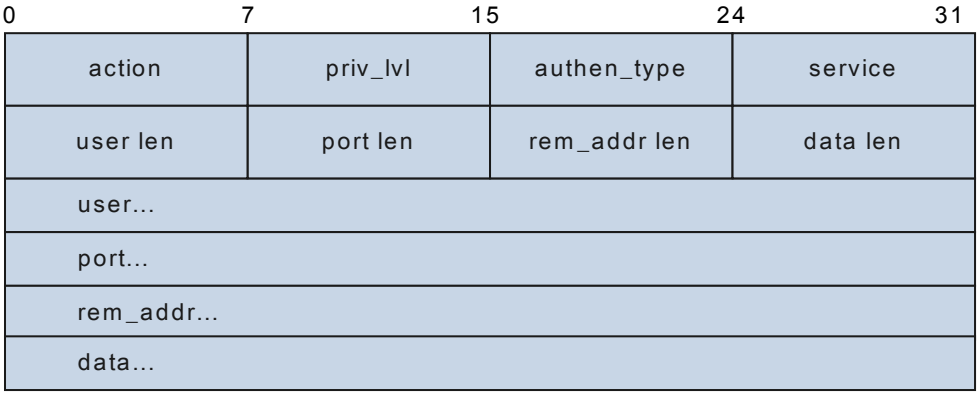


Table 7-11 Fields in HWTACACS Authentication Start packet

Field	Description
action	Authentication action. Only the login authentication (0x01) action is supported.
priv_lvl	User privilege level.
authen_type	Authentication type, including: ● CHAP(0x03) ● PAP(0x02) ● ASCII(0x01)
service	Type of the service requesting authentication. The PPP(0x03), LOGIN (0x01), and NONE(0x00) types are available, corresponding to PPP users, administrators, and other users.
user len	Length of the user name entered by a login user.
port len	Length of the port field.
rem_addr len	rem_addr field length.
data len	Authentication data length.
user	Name of the user requesting authentication. The maximum length is 129.
port	Name of the user interface requesting authentication. The maximum length is 47. ● For management users, this field indicates the user terminal interface, for example, console0 and vty1. For example, the authen_type of Telnet users is ASCII, service is LOGIN, and port is vtyx. ● For other users, this field indicates the user access interface.
rem_addr	IP address of the login user.

Field	Description
data	Authentication data. Different data is encapsulated depending on the values of action and authen_type. For example, when PAP authentication is used, the value of this field is PAP plain-text password.

- Figure 7-9 shows the format of HWTACACS Authentication Continue packets.

Figure 7-9 HWTACACS Authentication Continue packet format

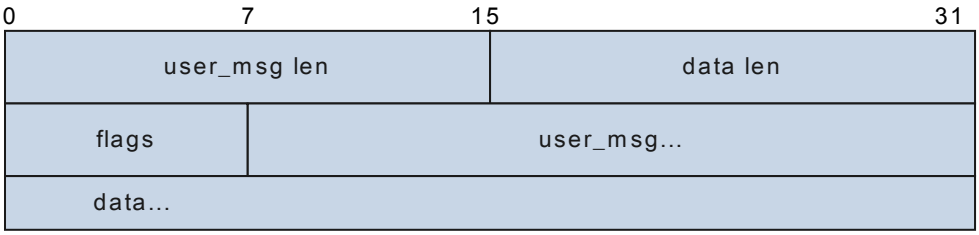


Table 7-12 Fields in HWTACACS Authentication Continue packet

Field	Description
user_msg len	Length of the character string entered by a login user.
data len	Authentication data length.
flags	Authentication continue flag. The value 0 indicates that the authentication continues, and the value 1 indicates that the authentication has ended.
user_msg	Character string entered by the login user. This field carries the user login password to respond to the server_msg field in the Authentication Response packet.
data	Authentication data. Different data is encapsulated depending on the values of action and authen_type. For example, when PAP authentication is used, the value of this field is PAP cipher-text password.

- Figure 7-10 shows the format of HWTACACS Authentication Response packets.

Figure 7-10 HWTACACS Authentication Response packet format

Table 7-13 Fields in HWTACACS Authentication Response packet

Field	Description
status	Authentication status, including: ● PASS (0x01): Authentication is successful. ● FAIL (0x02): Authentication is fail. ● GETDATA (0x03): Request user information. ● GETUSER (0x04): Request user name. ● GETPASS (0x05): Request password. ● RESTART (0x06): Request reauthentication. ● ERROR (0x07): An error occurs when the server receives authentication packets. ● FOLLOW (0x21): The server requests reauthentication.
flags	Whether the client displays the password entered by user in plain text. The value 1 indicates that the password is not displayed in plain text.
server_msg len	Length of the server_msg field.
data len	Authentication data length.
server_msg	Optional field. This field is sent by the server to the user to provide additional information.
data	Authentication data, providing information to client.

HWTACACS Authorization Packet Format

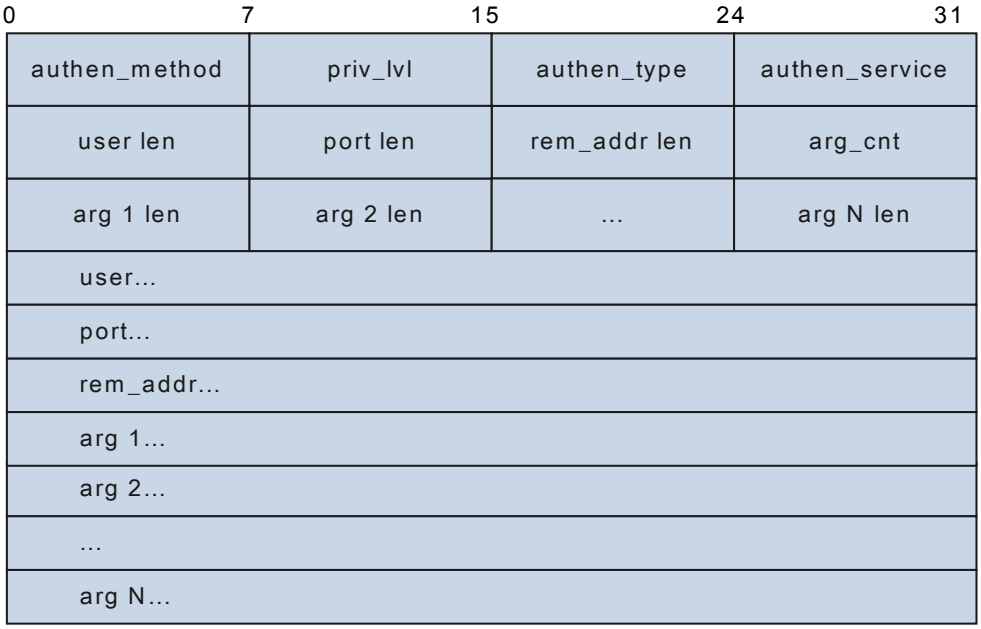
HWTACACS authorization packets include:

- **Authorization Request**: HWTACACS separates authentication from authorization. Therefore, a user can be authenticated by HWTACACS, and authorized using another protocol. If a user is authenticated by HWTACACS, the client sends an Authorization Request packet carrying authorization information to the server.
- **Authorization Response**: After receiving the Authorization Request packet, the server sends this packet carrying the authorization result to the client.

The HWTACACS authorization packets have different formats.

- **Figure 7-11** shows the format of HWTACACS Authorization Request packets.

Figure 7-11 HWTACACS Authorization Request packet format



NOTE

The meanings of the priv_lvl, authen_type, authen_service, user len, port len, rem_addr len, port, and rem_addr fields in the Authorization Request packet are the same as those in the Authentication Start packet, and are not provided here.

Table 7-14 Fields in HWTACACS Authorization Request packet

Field	Description
authen_method	Authentication method, including ● No authentication method configured (0x00) ● None authentication (0x01) ● Local authentication (0x05) ● HWTACACS authentication (0x06) ● RADIUS authentication (0x10)
authen_service	Type of the service requesting authentication. The PPP(0x03), LOGIN (0x01), and NONE(0x00) types are available, corresponding to PPP users, administrators, and other users.
arg_cnt	Number of attributes carried in Authorization Request packet.
argN	Attribute of the Authorization Request packet. including: ● cmd: the first keyword of the command line to be authorized. ● cmd-arg: parameter in the command line to be authorized. The cmd-arg=<cr> is added at the end of the command line.

- **Figure 7-12** shows the format of HWTACACS Authentication Response packets.

NOTE

The meanings of the server_msg len, data len, and server_msg fields are the same as those in HWTACACS Authentication Response packet, and are not provided here.

Figure 7-12 HWTACACS Authorization Response packet format

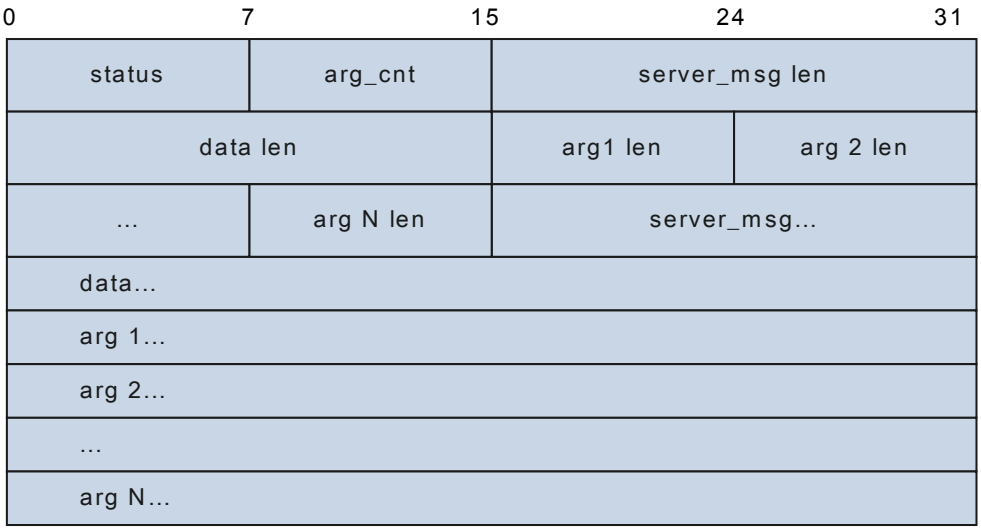


Table 7-15 Fields in HWTACACS Authorization Response packet

Field	Description
status	Authorization status, including: ● Authorization is successful (0x01) ● The attributes in Authorization Request packets are modified by the TACACS server (0x02) ● Authorization is fail (0x10) ● An error occurs on the authorization server (0x11) ● An authorization server is respecified (0x21)
arg_cnt	Number of attributes carried in Authorization Response packet.
argN	Authorization attribute delivered by the HWTACACS authorization server.

HWTACACS Accounting Packet Format

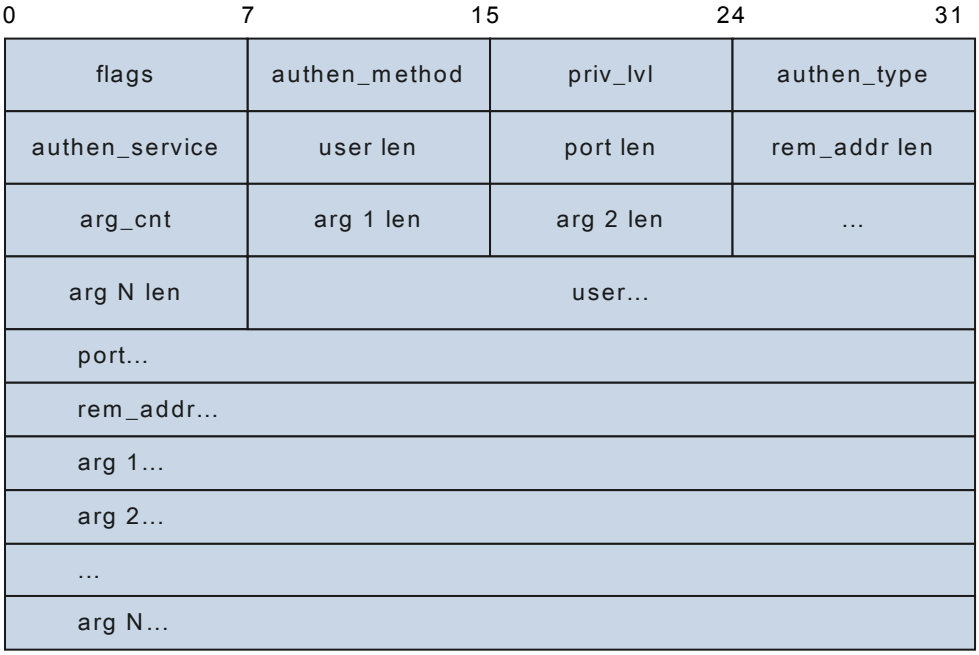
HWTACACS accounting packets include:

- **Accounting Request**: This packet contains authorization information.
- **Accounting Response**: After receiving and recording an Accounting Request packet, the server returns this packet.

The HWTACACS accounting packets have different formats.

- **Figure 7-13** shows the format of HWTACACS Accounting Request packets.

Figure 7-13 HWTACACS Accounting Request packet format



NOTE

The meanings of the authen_method, priv_lvl, authen_type, user len, port len, rem_addr len, port, and rem_addr fields in the Accounting Request packet are the same as those in the Authorization Request packet, and are not provided here.

Table 7-16 Fields in HWTACACS Accounting Request packet

Field	Description
flags	Accounting type: ● Start accounting (0x02) ● Stop accounting (0x04) ● Interim accounting (0x08)
authen_service	Type of the service requesting authentication. The PPP(0x03), LOGIN (0x01), and NONE(0x00) types are available, corresponding to PPP users, administrators, and other users.
arg_cnt	Number of attributes carried in Accounting Request packet.
argN	Attribute of the Accounting Request packet.

- **Figure 7-14** shows the format of HWTACACS Accounting Response packets.

Figure 7-14 HWTACACS Accounting Response packet format

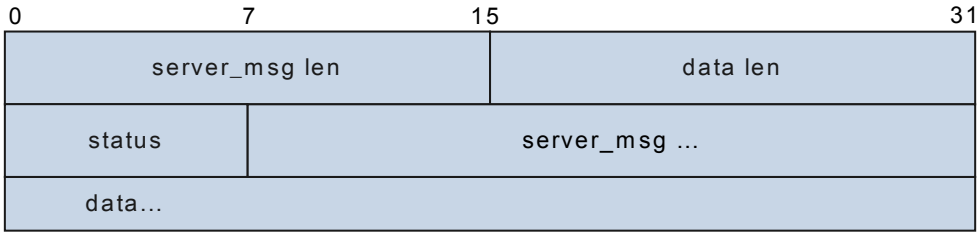


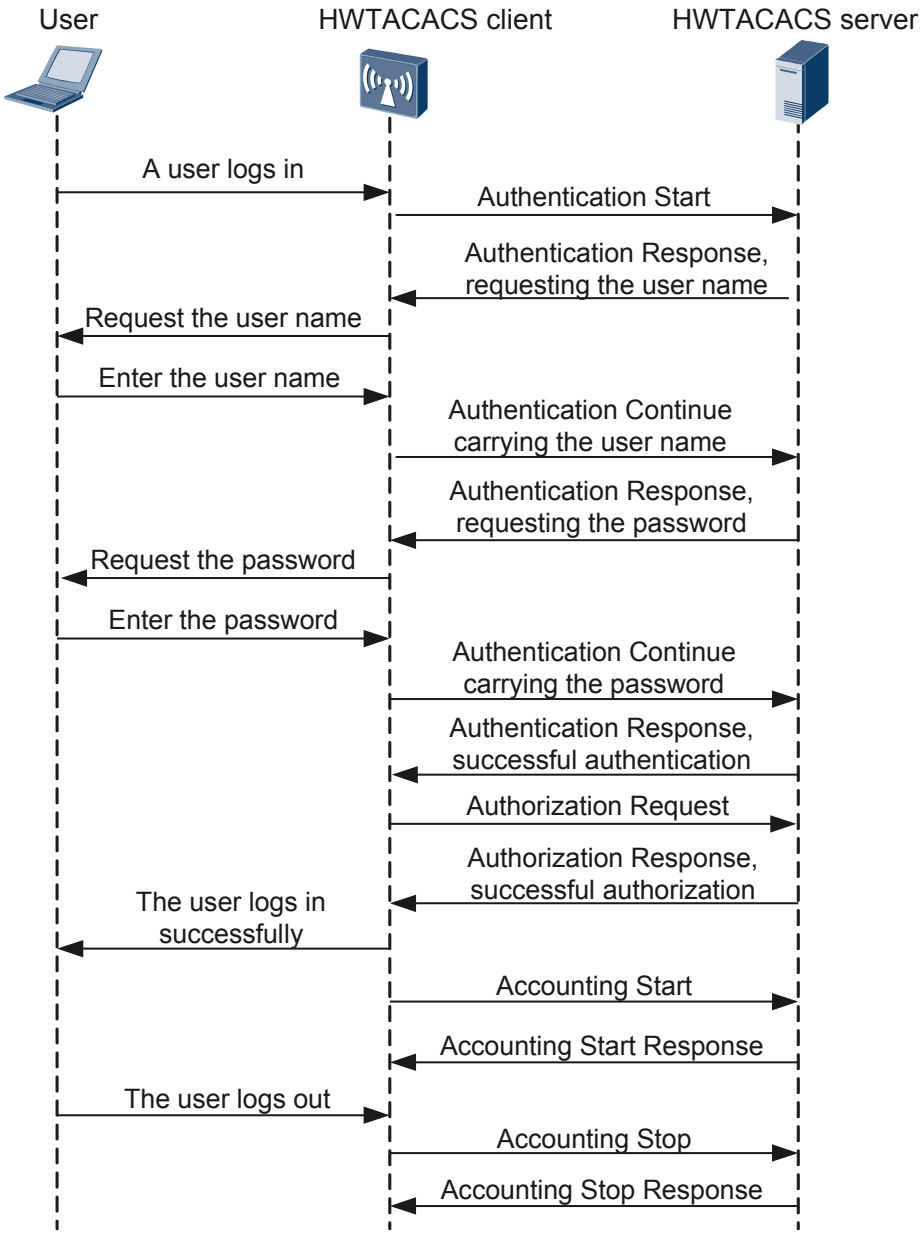
Table 7-17 Fields in HWTACACS Accounting Request packet

Field	Description
server_msg len	Length of the server_msg field.
data len	Length of the data field.
status	Accounting status: ● Accounting is successful (0x01) ● Accounting is fail (0x02) ● No response (0x03)
server_msg	Information sent by the accounting server to the client.
data	Information sent by the accounting server to the administrator.

7.1.2.3.3 HWTACACS Interaction Process

This section describes how HWTACACS performs authentication, authorization, and accounting for Telnet users. **Figure 7-15** shows the message exchange process.

Figure 7-15 HWTACACS message interaction



The HWTACACS message exchange process is as follows:

1. A Telnet user sends a request packet.
2. The HWTACACS client sends an Authentication Start packet to the HWTACACS server after receiving the request packet.
3. The HWTACACS server sends an Authentication Reply packet to request the user name.
4. The HWTACACS client sends a packet to query the user name after receiving the Authentication Reply packet.
5. The user enters the user name.

6. The HWTACACS client sends an Authentication Continue packet containing the user name to the HWTACACS server.
7. The HWTACACS server sends an Authentication Reply packet to request the password.
8. The HWTACACS client queries the password after receiving the Authentication Reply packet.
9. The user enters the password.
10. The HWTACACS client sends an Authentication Continue packet containing the password to the HWTACACS server.
11. The HWTACACS server sends an Authentication Reply packet, indicating that the user has been authenticated.
12. The HWTACACS client sends an Authorization Request packet to the HWTACACS server.
13. The HWTACACS server sends an Authorization Response packet, indicating that the user is authorized.
14. The HWTACACS client receives the Authorization Response packet and displays the login page.
15. The HWTACACS client sends an Accounting Request (start) packet to the HWTACACS server.
16. The HWTACACS server sends an Accounting Response packet.
17. The user requests to go offline.
18. The HWTACACS client sends an Accounting Request (stop) packet to the HWTACACS server.
19. The HWTACACS server sends an Accounting Response packet.

NOTE

Both the HWTACACS protocol and TACACS+ protocol of other vendors can implement authentication, authorization, and accounting. Their authentication procedures and implementations are the same, so the HWTACACS protocol is completely compatible with the TACACS+ protocol.

7.1.2.3.4 HWTACACS Attributes

In the HWTACACS authorization or accounting packets, the argN field carries the information exchanged between server and client.

HWTACACS Attributes

Table 7-18 describes the HWTACACS attributes supported by the device. The device cannot parse the attributes not included in the table.

Table 7-18 Common HWTACACS attributes

Attribute Name	Description
acl	Authorization ACL ID.
addr	User IP address.
autocmd	Commands the system automatically executes after a user logs in.

Attribute Name	Description
bytes_in	Number of bytes received by the device. K, M, and G indicate KByte, MByte, and GByte. No unit is displayed if Byte is used
bytes_out	Number of bytes sent by the device. K, M, and G indicate KByte, MByte, and GByte. No unit is displayed if Byte is used
callback-line	Information sent from the authentication server and to be displayed to a user, such as the mobile number.
cmd	Commands executed by shell. The maximum length is 251 characters. The complete command is encapsulated when the command is recorded and the first keyword is encapsulated when the command is authorized.
cmd-arg	Parameter in the command line to be authorized. The cmd-arg=<cr> is added at the end of the command line.
disc_cause	Disconnection reason. Only accounting stop packets carry this attribute. The reasons include: ● A user requests to go offline (1) ● Data forwarding is interrupted (2) ● Service is interrupted (3) ● Idle cut (4) ● Session timeout (5) ● The administrator requests to go offline (7) ● The NAS is faulty (9) ● The NAS requests to go offline (10) ● The port is suspended (12) ● User information is incorrect (17) ● A host requests to go offline (18)
disc_cause_ext	Extended disconnection reason. Only accounting stop packets carry this attribute. The reasons include: ● Unknown reason (1022) ● The EXEC terminal tears down the connection (1020) ● An online Telnet user forcibly disconnects this user (1022) ● The user cannot be switched to the SLIP/PPP client due to no remote IP address (1023) ● PPP PAP authentication fails (1042) ● PPP receives the Terminate packet from the remote end (1045) ● The upper-layer device requests the device to tear down the PPP connection (1046) ● PPP handshake fails (1063) ● Session times out (1100)

Attribute Name	Description
dnaverage	Downstream average rate, in bit/s.
dnpeak	Downstream peak rate, in bit/s.
dns-servers	IP address of the primary DNS server.
elapsed_time	Online duration, in seconds.
ftpdir	Initial directory of an FTP user.
gw-password	Tunnel password. The value is a string of 1 to 29 characters. If the value contains more than 29 characters, only the first 29 characters are valid.
ideltime	Idle session timeout period. If a user does not perform any operation within this period, the system disconnects the user.
ip-addresses	LNS IP address. A maximum of 8 LNS IP addresses are supported. The excess IP addresses are ignored. The IP addresses are separated by semicolons or commas.
l2tp-hello-interval	Interval for sending L2TP Hello packets. The device does not support this attribute.
l2tp-hidden-avp	The attribute value pair (AVP) of L2TP. The device does not support this attribute.
l2tp-nosession-timeout	If no session exists within this period, the L2TP tunnel is torn down. The device does not support this attribute.
l2tp-group-num	L2TP group number. Other L2TP attributes take effect only after this attribute is delivered. If this attribute is not delivered, other L2TP attributes are ignored.
l2tp-tos-reflect	TOS of L2TP. The device does not support this attribute.
l2tp-tunnel-authen	Whether the L2TP tunnel is authenticated. The value 0 indicates no authentication, and the value 1 indicates authentication.
l2tp-udp-checksum	UPD packet checksum.
nocallback-verify	No authentication is required for callback.
nohangup	Whether the device automatically disconnects a user. The value is true or false. This attribute is valid only after the autocmd attribute is configured. It decides whether to disconnect a user who has executed the autocmd command. The value true indicates not to disconnect and the value false indicates to disconnect.
paks_in	Number of packets received by the device.

Attribute Name	Description
paks_out	Number of packets sent by the device.
priv-lvl	User level.
protocol	Protocol type. It belongs to service type, and is only valid for PPP and Connection services. The device supports four protocol types: pad, telnet, ip, and vpdn. ● When the service type is connection, the protocol type can be pad or telnet. ● When the service type is ppp, the protocol type can be ip or vpdn. ● For other service types, this attribute is not used.
task_id	Task ID. The task IDs recorded when a task starts and ends must be the same.
timezone	Local time zone.
tunnel-id	Local user name of the tunnel. The value is a string of 1 to 29 characters. If the value contains more than 29 characters, only the first 29 characters are valid.
tunnel-type	Tunnel type.
service	Service type, accounting or authorization.
source-ip	Local IP address of the tunnel.
upaverage	Upstream average rate, in bit/s.
uppeak	Upstream peak rate, in bit/s.

HWTACACS Attributes Available in Packets

Depending on packet types, HWTACACS authorization packets are classified into Authorization Request packets and Authorization Response packets. Depending on use scenarios, HWTACACS authorization packets are classified into EXEC user authorization packets, command line authorization packets, and access user authorization packets. Different authorization packets carry different attributes. For details, see **Table 7-19**.

- EXEC authorization: The HWTACACS server controls rights of the management users logging in through Telnet, terminal, SSH, and FTP.
- Command line authorization: The device authorizes each command line executed by user. Only authorized command lines can be executed.
- Access user authorization: The HWTACACS server controls the rights of NAC users such as 802.1x and Portal users.

Depending on packet types, HWTACACS accounting packets are classified into Accounting Request packets and Accounting Response packets. Depending on connection types, HWTACACS accounting packets are classified into network accounting packets, connection accounting packets, EXEC accounting packets, system accounting packets, and command accounting packets. Different accounting packets carry different attributes. For details, see **Table 7-20**.

- Network accounting: applicable to the networks where PPP users access. For example, when a PPP user connects to a network, the server sends an accounting start packet; when the user is using network services, the server periodically sends interim accounting packets; when the user goes offline, the server sends an accounting stop packet.
- Connection accounting: applicable to the scenarios where users log in to the server through Telnet or FTP clients. When a user connects to the device, the user can run commands to access a remote server and obtain files from the server. The device sends an accounting start packet when the user connects to the remote server and an accounting stop packet when the user disconnects from the remote server.
- EXEC accounting: applicable to the scenarios where users log in to the device through Telnet or FTP. When a user connects to a network, the server sends an accounting start packet; when the user is using network services, the server periodically sends interim accounting packets; when the user goes offline, the server sends an accounting stop packet.
- System accounting: applicable to the fault diagnosis scenarios. The server records the system-level events to help administrators monitor the device and locate network faults.
- Command accounting: When an administrator runs any command on the device, the device sends the command to the HWTACACS server through a command accounting stop packet so that the server can record the operations performed by the administrator.

NOTE

- Y: The packet supports this attribute.
- N: The packet does not support this attribute.

Table 7-19 HWTACACS attributes available in authorization packets

Attribute	Command Line Authorization Packet	EXEC Authorization Response Packet	Access User Authorization Response Packet
acl	N	Y	N
addr	N	N	Y
addr-pool	N	N	Y
autocmd	N	Y	N
callback-line	N	Y	Y
cmd	Y	N	N
cmd-arg	Y	N	N
dnaverage	N	N	Y
dnpeak	N	N	Y
dns-servers	N	N	Y
ftpdir	N	Y	N
gw-password	N	N	Y

Attribute	Command Line Authorization Packet	EXEC Authorization Response Packet	Access User Authorization Response Packet
idletime	N	Y	N
ip-addresses	N	N	Y
l2tp-group-num	N	N	Y
l2tp-tunnel-authen	N	N	Y
nocallback-verify	N	Y	N
nohangup	N	Y	N
priv-lvl	N	Y	N
source-ip	N	N	Y
tunnel-type	N	N	Y
tunnel-id	N	N	Y
upaverage	N	N	Y

Table 7-20 HWTACACS attributes available in accounting packets

Attribute	Network Accounting Start Packet	Network Accounting Stop Packet	Network Interim Accounting Packet	Connection Accounting Start Packet	Connection Accounting Stop Packet	EXEC Accounting Start Packet	EXEC Accounting Stop Packet	EXEC Interim Accounting Packet	System Accounting Stop Packet	Command Line Accounting Stop Packet
addr	Y	Y	Y	Y	Y	N	N	N	N	N
bytes_in	N	Y	Y	N	Y	N	Y	Y	N	N
bytes_out	N	Y	Y	N	Y	N	Y	Y	N	N
cmd	N	N	N	Y	Y	N	N	N	N	Y
disc_cause	N	Y	N	N	N	N	Y	Y	N	N
disc_cause_ext	N	Y	N	N	N	N	Y	Y	N	N

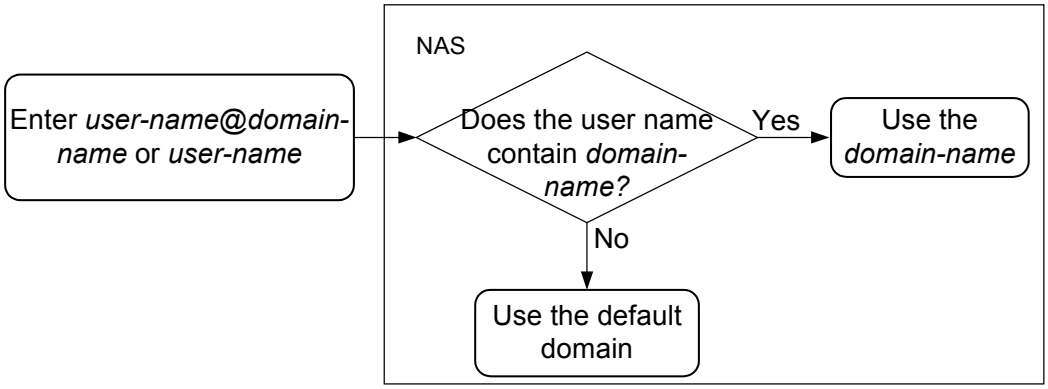
Attribute	Network Accounting Start Packet	Network Accounting Stop Packet	Network Interim Accounting Packet	Connection Accounting Start Packet	Connection Accounting Stop Packet	EXEC Accounting Start Packet	EXEC Accounting Stop Packet	EXEC Interim Accounting Packet	System Accounting Stop Packet	Command Line Accounting Stop Packet
elapsed_time	N	Y	Y	N	Y	N	Y	Y	Y	N
paks_in	N	Y	Y	N	Y	N	Y	Y	N	N
paks_out	N	Y	Y	N	Y	N	Y	Y	N	N
priv-lvl	N	N	N	N	N	N	N	N	N	Y
protocol	Y	Y	Y	Y	Y	N	N	N	N	N
service	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
task_id	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
timezone	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
tunnel-id	N	N	N	N	N	N	N	N	N	N
tunnel-type	Y	N	N	N	N	N	N	N	N	N

7.1.2.4 Domain-based User Management

A domain is a group of users.

A NAS manages users based on domains. Each access user belongs to a domain that is determined by the user name provided for login, as shown in **Figure 7-16**.

Figure 7-16 Using the user name to determine the domain



The device has two default domains: **default** (global default domain for common access users) and **default_admin** (global default domain for administrators). The two domains can be modified but cannot be deleted. If the domain of an access user cannot be obtained, the default domain is used.

- The **default** domain is used for access users such as NAC access users. By default, local authentication is performed for users in this domain.
- The **default_admin** domain is used for administrators such as the administrators who log in using HTTP, SSH, Telnet, FTP, and terminals. By default, local authentication is performed for users in this domain.

NOTE

A user-defined domain can be configured as a global default domain for common access users and administrators.

The preconfigured authentication, authorization, and accounting scheme is used in the corresponding domain view to implement authentication, authorization, and accounting for users. AAA provides the default scheme including local authentication, local authorization, and local accounting. If no authentication, authorization, and accounting scheme is used in the domain of a user, the default scheme is used.

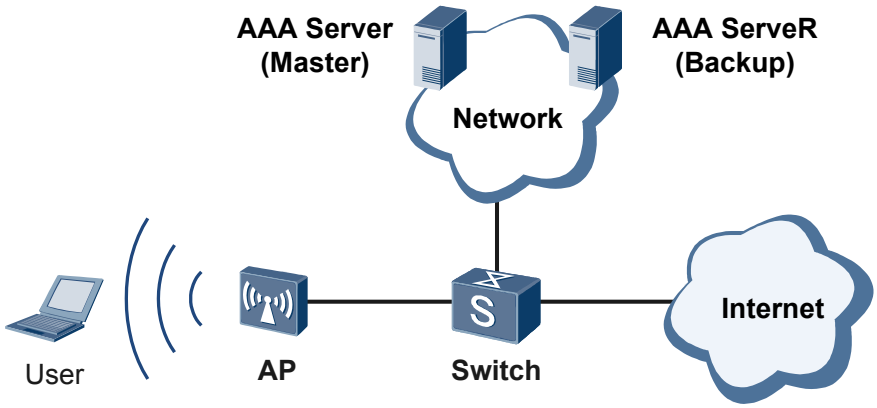
Authorization information configured in a domain has a lower priority than authorization information delivered by an AAA server. That is, the authorization information delivered by an AAA server is used preferentially. When the AAA server does not have or does not support authorization, the authorization attributes configured in a domain take effect. In this manner, you can increase services flexibly by means of domain management, regardless of the authorization attributes provided by the AAA server.

7.1.3 Use Scenario

This section describes AAA use scenarios.

Deploying AAA for Internet Access Users

Figure 7-17 AAA deployment for Internet access users



As shown in **Figure 7-17**, an enterprise network connects to the AP through . Users on the enterprise network need to connect to the Internet. To ensure network security, the administrator controls the Internet access rights of the users.

The administrator configures AAA on the AP to allow the AP to communicate with the AAA server. The AAA server then can manage users centrally. After a user enters the user name and password on the client, the AP forwards the authentication information including user name and password to the AAA server, and the AAA server authenticates the user. After being successfully authenticated, the user can access the Internet. The AAA server also records the network resource usage of the user.

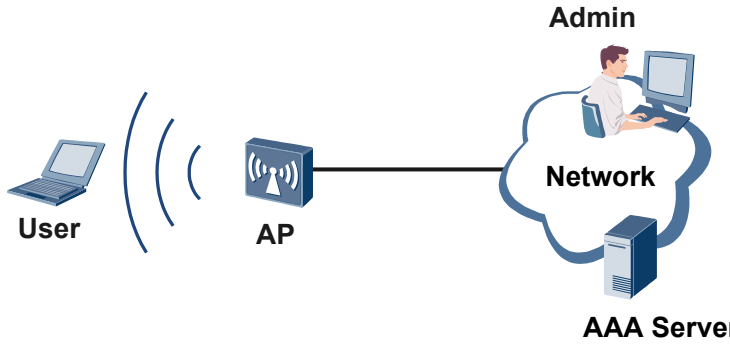
Two AAA servers can be deployed in active/standby mode to improve reliability. When the active server fails, the standby one takes over the AAA services, ensuring uninterrupted services.

Deploying AAA for Management Users

As shown in **Figure 7-18**, the management user (Admin) connects to the AP to manage, configure, and maintain the AP.

After the management user logs in to the AP with AAA configured, the AP sends the user name and password of the user to the AAA server. The AAA server then authenticates the user and records the user operations.

Figure 7-18 AAA deployment for management users



7.1.4 AAA Configuration Tasks

After AAA configuration is complete, the device authenticates users and authorizes users to use particular services. In addition, the device also records the network resource usage of the user.

The device supports the combination of local, Remote Authentication Dial In User Service (RADIUS), and Huawei Terminal Access Controller Access Control System (HWTACACS) authentication, authorization, and accounting. For example, the device provides local authentication, local authorization, and RADIUS accounting.

In practice, as shown in **Table 7-21**, the following schemes are used separately. Multiple authentication or authorization modes can be used in a scheme. For example, local authentication is used as a backup of RADIUS authentication and HWTACACS authentication, and local authorization is used as a backup of HWTACACS authorization.

Table 7-21 AAA configuration tasks

Configuration Task	Overview	Task
Local authentication and authorization	If users need to be authenticated or authorized but no RADIUS server or HWTACACS server is deployed on the network, use local authentication and authorization. Local authentication and authorization feature fast processing and low operation cost, whereas the amount of information that can be stored is limited by the device hardware capacity. Local authentication and authorization are often used for administrators.	**7.1.5.1 Configuring Local Authentication and Authorization**
RADIUS authentication, authorization, and accounting	RADIUS protects a network from unauthorized access, which is often used on the networks demanding high security and remote user access control.	**7.1.5.2 Configuring RADIUS AAA**
HWTACACS authentication, authorization, and accounting	HWTACACS protects a network from unauthorized access and supports command-line authorization. Compared with RADIUS, HWTACACS is more reliable in transmission and encryption, and is more suitable for security control.	**7.1.5.3 Configuring HWTACACS AAA**

7.1.5 Configuring AAA

This section describes the AAA configuration procedure.

7.1.5.1 Configuring Local Authentication and Authorization

After local authentication and authorization are configured, the device authenticates and authorizes access users based on the local user information.

Local Authentication and Authorization

In local authentication and authorization, user information including the local user name, password, and attributes is configured on the device. Local authentication and authorization feature fast processing and low operation cost, whereas the amount of information that can be stored is limited by the device hardware capacity.

Pre-configuration Tasks

Before configuring local authentication and authorization, completing the following task:

- Configuring physical attributes for interfaces to ensure that the physical layer status of the interfaces is Up

7.1.5.1.1 Configuring AAA Schemes

Context

To use local authentication and authorization, set the authentication mode in an authentication scheme to local authentication and the authorization mode in an authorization scheme to local authorization.

By default, the device performs local authentication and authorization for access users.

Procedure

- Configuring an authentication scheme
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     aaa

     The AAA view is displayed.
  3. Run:
     authentication-scheme *authentication-scheme-name*

     An authentication scheme is created, and the corresponding authentication scheme view or an existing authentication scheme view is displayed.

     By default, there is an authentication scheme named **default** on the device. This default scheme can be modified but cannot be deleted.
  4. Run:
     authentication-mode local

     The authentication mode is set to local authentication.

     By default, local authentication is used.
  5. Run:
     quit

     The AAA view is displayed.
  6. (Optional) Run:
     domainname-parse-direction { **left-to-right** | **right-to-left** }

     The direction in which the user name and domain name are parsed is configured.

     By default, a domain name is parsed from left to right.
- Configuring an authorization scheme

1. Run:
   system-view

   The system view is displayed.
2. Run:
   aaa

   The AAA view is displayed.
3. Run:
   authorization-scheme *authorization-scheme-name*

   An authorization scheme is created, and the corresponding authorization scheme view or an existing authorization scheme view is displayed.

   By default, there is a default authorization scheme named **default** on the device. This default authorization scheme can be modified but cannot be deleted.
4. Run:
   authorization-mode local [**none**]

   The authorization mode is configured.

   By default, local authorization is used.
5. Run:
   quit

   The AAA view is displayed.
6. (Optional) Run:
   authorization-modify mode { **modify** | **overlay** }

   The update mode of user authorization information delivered by the authorization server is configured.

   By default, the update mode of user authorization information delivered by the authorization server is **overlay**.

----End

7.1.5.1.2 Configuring a Local User

Context

When local authentication and authorization are configured, configure authentication and authorization information on the device, including the user name, password, and user level.

NOTE

After you change the rights (including the password, access type, FTP directory, and level) of a local account, the rights of users already online do not change. The change takes effect to users who go online after the change.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Create a local user account and set the password as required.

- Run the **local-user** *user-name* **password** command to create a local user and set the password.

  By default, the local account password is admin@huawei.com.

- Run the **local-user** *user-name* **password** { **cipher** | **irreversible-cipher** } *password* command to create a local user and set the password.

  By default, the local account password is admin@huawei.com.

NOTE

If the user name contains a domain name delimiter such as @, |, and %, the character string before the delimiter is the user name and the character string behind the delimiter is the domain name. If the user name does not contain a domain name delimiter, the entire character string is the user name. Ordinary users are authenticated in the **default** domain, and management users are authenticated in the **default_admin** domain.

Step 4 Run:

```
local-user user-name service-type { 8021x | bind | ftp | http | ppp | ssh | telnet | terminal | web | x25-pad } *
```

The access type is configured for the local user.

By default, a local user can use any access type.

Step 5 (Optional) Run:

```
local-user user-name idle-timeout minutes [ seconds ]
```

The idle timeout interval is configured for the local user.

Step 6 (Optional) Run:

```
local-user user-name ftp-directory directory
```

The FTP directory is configured for the local user.

By default, the FTP directory of a local user is empty.

NOTE

When the device functions as an FTP server, you must configure the FTP directory that FTP users can access. Otherwise, FTP users cannot access the device.

Step 7 (Optional) Configure the level of the local user or the group to which the local user belongs to.

- Run the **local-user** *user-name* **privilege level** *level* command to configure the level of the local user.
- Run the **local-user** *user-name* **user-group** *group-name* command to add the local user to the specified user group.

Step 8 (Optional) Run:

```
local-user user-name expire-date expire-date
```

The expiry date of the local account is specified.

By default, a local account is permanently valid.

Step 9 (Optional) Run:

```
local-user user-name state { active | block }
```

The state of the local user is configured.

By default, a local user is in active state.

The device processes requests from users in different states as follows:

- If a local user is in active state, the device accepts and processes the authentication request from the user.
- If a local user is in blocking state, the device rejects the authentication request from the user.

Step 10 (Optional) Run:

```
local-user user-name access-limit max-number
```

The maximum number of connections that can be established by the local user is configured.

By default, the number of connections established by a user is not limited.

Step 11 (Optional) Run:

```
local-user user-name device-type device-type &<1-8>
```

The device type for user access is configured.

By default, no device type is configured.

Step 12 (Optional) Run:

```
local-aaa-user wrong-password retry-interval retry-interval retry-time retry-time
block-time block-time
```

Local account locking is enabled and the retry interval, consecutive authentication failure counts, and locking duration are set.

By default, the local account locking function is enabled, retry interval is 30 minutes, maximum number of consecutive incorrect password attempts is 30, and account locking period is 30 minutes.

Step 13 Run:

```
return
```

The user view is displayed.

Step 14 (Optional) Run:

```
local-user change-password
```

The password of the local user is changed.

----End

7.1.5.1.3 (Optional) Configuring a Service Scheme

Context

Access users must obtain authorization information before going online. Authorization information about users can be managed by configuring a service scheme.

NOTE

In the service scheme, you only need to run the **admin-user privilege level** command to configure AAA. Other commands need to be configured only when they are referenced by other features such as IPSec in the service scheme.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
service-scheme service-scheme-name
```

A service scheme is created and the service scheme view is displayed.

By default, no service scheme is configured on the device.

Step 4 Run:

```
admin-user privilege level level
```

The user is configured to log in to the device as the administrator and the administrator level for login is specified.

level ranges from 0 to 15. By default, the user level is not configured.

Step 5 (Optional) Run:

```
dns ip-address
```

The IP address of the primary DNS server is configured.

By default, no primary DNS server address is configured in a service scheme.

Step 6 (Optional) Run:

```
dns ip-address secondary
```

The IP address of the secondary DNS server is configured.

By default, no secondary DNS server address is configured in a service scheme.

----End

7.1.5.1.4 Configuring a Domain

Context

The created authentication and authorization schemes take effect only after being applied to a domain. When local authentication and authorization are used, non-accounting is used by default.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
domain domain-name
```

A domain is created and the domain view is displayed, or an existing domain view is displayed.

The device has two default domains: **default** and **default_admin**. The **default** domain is used by common access users and the **default_admin** domain is used by administrators.

Step 4 Run:

```
authentication-scheme authentication-scheme-name
```

An authentication scheme is applied to the domain.

By default, the authentication scheme named **default** is applied to a domain.

Step 5 Run:

```
authorization-scheme authorization-scheme-name
```

An authorization scheme is applied to the domain.

By default, no authorization scheme is applied to a domain.

Step 6 (Optional) Run:

```
user-group group-name
```

A user group is applied to the domain.

By default, no user group is applied to a domain.

Step 7 (Optional) Run:

```
service-scheme service-scheme-name
```

A service scheme is applied to the domain.

By default, no service scheme is applied to a domain.

Step 8 (Optional) Run:

```
state { active | block }
```

The domain state is configured.

When a domain is in blocking state, users in this domain cannot log in. By default, a domain is in active state after being created.

Step 9 Run:

```
quit
```

Exit from the domain view.

Step 10 (Optional) Run:

domain-name-delimiter *delimiter*

A domain name delimiter is configured.

A domain name delimiter can be any of the following: \ / : < > | @ ' %.

The default domain name delimiter is @.

Step 11 Run:

quit

Return to the system view.

Step 12 (Optional) Run:

interface wlan-bss *wlan-bss-number*

A WLAN-BSS interface is created and its view is displayed.

Step 13 (Optional) Run:

force-domain name *domain-name*

The forcible authentication domain is configured on an interface.

By default, no forcible authentication domain is configured on an interface.

NOTE

This step is applicable to only wireless users.

Step 14 (Optional) Run:

permit-domain name *domain-name* &<1-4>

The permitted domain is configured for wireless users.

By default, no permitted domain is specified for wireless users.

NOTE

This step is applicable to only wireless users.

----End

7.1.5.1.5 Checking the Configuration

Procedure

- Run the **display aaa configuration** command to check the AAA summary.
- Run the **display authentication-scheme** [*authentication-scheme-name*] command to check the authentication scheme configuration.
- Run the **display authorization-scheme** [*authorization-scheme-name*] command to check the authorization scheme configuration.
- Run the **display access-user** [**domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* | **slot** *slot-id* | **ssid** *ssid-name* | **user-group** *user-group-name*] [**detail**] or **display access-user** [**mac-address** *mac-address* | **user-id** *user-id* | **statistics**] command to check the information about online users.

- Run the **display domain** [**name** *domain-name*] command to check the domain configuration.
- Run the **display local-user** [**domain** *domain-name* | **state** { **active** | **block** } | **username** *username*] * command to check the brief information about local users.

----End

7.1.5.2 Configuring RADIUS AAA

RADIUS is often used to implement authentication, authorization, and accounting (AAA).

RADIUS Authentication, Authorization, and Accounting

RADIUS uses the client/server model and protects a network from unauthorized access. It is often used in network environments that require high security and control remote user access.

Pre-configuration Tasks

Before configuring RADIUS AAA, completing the following task:

- Configuring physical attributes for interfaces to ensure that the physical layer status of the interfaces is Up

7.1.5.2.1 Configuring AAA Schemes

Context

To use RADIUS AAA, set the authentication mode in an authentication scheme to RADIUS and the accounting mode in an accounting scheme to RADIUS.

If RADIUS authentication is configured, you can also configure local authentication or non-authentication as the backup. This allows local authentication or non-authentication to be implemented if RADIUS authentication fails.

Procedure

- Configuring an authentication scheme
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     aaa
     ```
     The AAA view is displayed.
  3. Run:
     ```
     authentication-scheme authentication-scheme-name
     ```
     Create an authentication scheme and enter its view, or directly enter the view of an existing authentication scheme.

By default, there is an authentication scheme named **default** on the device. The default authentication scheme can only be modified, but cannot be deleted.

4. Run:
   authentication-mode radius

   RADIUS authentication is configured.

   By default, local authentication is used.

   To use local authentication as the backup authentication mode, run the **authentication-mode radius local** command to configure local authentication.

   NOTE

   If multiple authentication modes are configured in an authentication scheme, these authentication modes are used according to the sequence in which they were configured. The device uses the authentication mode that was configured later only when it does not receive any response in the current authentication. The device stops the authentication if the current authentication fails.

5. Run:
   quit

   Return to the AAA view.

6. (Optional) Run:
   domainname-parse-direction { **left-to-right** | **right-to-left** }

   The direction in which the user name and domain name are parsed is configured.

7. (Optional) Run:
   remote-aaa-user authen-fail retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

   The remote AAA authentication account locking function is enabled, and the authentication retry interval, maximum number of consecutive authentication failures, and account locking period are set.

   By default, the remote AAA account locking function is enabled, authentication retry interval is 30 minutes, maximum number of consecutive authentication failures is 30, and account locking period is 30 minutes.

8. (Optional) Run:
   remote-user authen-fail unblock { **all** | **username** *username* }

   The remote AAA authentication accounts are unlocked.

- Configuring an accounting scheme

  1. Run:
     system-view

     The system view is displayed.

  2. Run:
     aaa

     The AAA view is displayed.

  3. Run:
     accounting-scheme *accounting-scheme-name*

     An accounting scheme is created and the accounting scheme view is displayed.

There is a default accounting scheme named **default** on the device. The default accounting scheme can only be modified, but cannot be deleted.

4. Run:
   accounting-mode radius

   The accounting mode is configured.

   By default, the accounting mode is **none**.
5. (Optional) Run:
   accounting start-fail { **online** | **offline** }

   A policy for accounting-start failures is configured.

   By default, users cannot go online if accounting-start fails.
6. (Optional) Run:
   accounting realtime *interval*

   Real-time accounting is enabled and the interval for real-time accounting is set.

   By default, the device performs accounting based on user online duration, the real-time accounting function is disabled, and the interval for real-time accounting is not set.
7. (Optional) Run:
   accounting interim-fail [**max-times** *times*] { **online** | **offline** }

   The maximum number of real-time accounting requests is set and a policy used after a real-time accounting failure is configured.

   After real-time accounting is enabled, the maximum number of real-time accounting requests is 3 and the device keeps paid users online after a real-time accounting failure by default.

----End

7.1.5.2.2 Configuring a RADIUS Server Template

Context

In a RADIUS server template, you must specify the IP address, port number, and shared key of a specified RADIUS server. Other settings such as the RADIUS user name format, traffic unit, and number of times RADIUS request packets are retransmitted have default values and can be changed based on network requirements.

The RADIUS server template settings such as the RADIUS user name format and shared key must be the same as those on the RADIUS server.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:

radius-server template *template-name*

The RADIUS server template view is displayed.

Step 3 (Optional) Run:

radius-server algorithm { **loading-share** | **master-backup** }

The algorithm for selecting RADIUS server is configured.

By default, the algorithm for selecting RADIUS servers is master/backup.

Step 4 Run:

radius-server authentication *ip-address port* [**source** { **loopback** *interface-number* | **ip-address** *ip-address* } | **weight** *weight-value*] *

The RADIUS authentication server is configured.

By default, no RADIUS authentication server is configured.

Step 5 Run:

radius-server accounting *ip-address port* [**source** { **loopback** *interface-number* | **ip-address** *ip-address* } | **weight** *weight-value*] *

The RADIUS accounting server is configured.

By default, no RADIUS accounting server is configured.

Step 6 Run:

radius-server shared-key cipher *key-string*

The RADIUS shared key is set.

By default, the RADIUS shared key is **huawei** and the password is in cipher text.

Step 7 (Optional) Run:

radius-server user-name domain-included

The RADIUS user name format is configured.

By default, the device to encapsulates the domain name in the user name when sending RADIUS packets to a RADIUS server.

If the RADIUS server does not accept the user name with the domain name, run the **undo radius-server user-name domain-included** command to delete the domain name from the user name.

Step 8 (Optional) Run:

radius-server traffic-unit { **byte** | **kbyte** | **mbyte** | **gbyte** }

The RADIUS traffic unit is set.

The default RADIUS traffic unit is byte on the device.

Step 9 (Optional) Run:

radius-server { **retransmit** *retry-times* | **timeout** *time-value* } *

The number of times that RADIUS request packets are retransmitted and timeout interval are set.

By default, the number of retransmission times is 3 and the timeout interval is 5 seconds.

Step 10 (Optional) Run:

radius-server nas-port-format { **new** | **old** }

The NAS port format of the RADIUS server is configured.

By default, the new NAS port format is used.

Step 11 (Optional) Run:

radius-server nas-port-id-format { **new** | **old** }

The ID format of the NAS port on the RADIUS server is set.

By default, the new format of the NAS port ID attribute is used.

Step 12 (Optional) Run:

radius-attribute nas-ip *ip-address*

The RADIUS NAS-IP-Address attribute is set.

Step 13 (Optional) Run:

radius-server accounting-stop-packet resend [*resend-times*]

Retransmission of accounting-stop packets is enabled and the number of accounting-stop packets that can be retransmitted each time is set.

By default, the retransmission times is 0. That is, accounting-stop packets are not retransmitted.

Step 14 Run:

radius-server dead-time *dead-time*

The time for the primary RADIUS server to return to the active state is set.

By default, the time for the primary RADIUS server to return to the active state is 5 minutes.

Step 15 (Optional) Run:

radius-attribute check *attribute-name*

The specified attributes in the received RADIUS Access-Accept packets are checked.

By default, the device does not check whether a RADIUS Access-Accept packet contains the specified attributes.

Step 16 (Optional) Run:

radius-attribute set *attribute-name attribute-value*

The value of the RADIUS attribute is changed.

Step 17 Run:

quit

Return to the system view.

Step 18 (Optional) Run:

radius-server authorization *ip-address* { **server-group** *group-name* | **shared-key cipher** *key-string* } * [**ack-reserved-interval** *interval*]

A RADIUS authorization server is configured.

By default, no RADIUS authorization server is configured.

Step 19 Run:

return

The user view is displayed.

Step 20 (Optional) Run:

test-aaa *user-name user-password* **radius-template** *template-name* [**chap** | **pap**]

The device is configured to test whether a user can be authenticated using RADIUS authentication.

----End

7.1.5.2.3 (Optional) Configuring a Service Scheme

Context

Access users must obtain authorization information before going online. Authorization information about users can be managed by configuring a service scheme.

NOTE

In the service scheme, you only need to run the **admin-user privilege level** command to configure AAA. Other commands need to be configured only when they are referenced by other features such as IPSec in the service scheme.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

aaa

The AAA view is displayed.

Step 3 Run:

service-scheme *service-scheme-name*

A service scheme is created and the service scheme view is displayed.

By default, no service scheme is configured on the device.

Step 4 Run:

admin-user privilege level *level*

The user is configured to log in to the device as the administrator and the administrator level for login is specified.

level ranges from 0 to 15. By default, the user level is not configured.

Step 5 (Optional) Run:

dns *ip-address*

The IP address of the primary DNS server is configured.

By default, no primary DNS server address is configured in a service scheme.

Step 6 (Optional) Run:

dns *ip-address* **secondary**

The IP address of the secondary DNS server is configured.

By default, no secondary DNS server address is configured in a service scheme.

----End

7.1.5.2.4 Configuring a Domain

Context

The created authentication scheme, accounting scheme, and RADIUS server template take effect only after being applied to a domain.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

aaa

The AAA view is displayed.

Step 3 Run:

domain *domain-name*

A domain is created and the domain view is displayed, or an existing domain view is displayed.

By default, the device has two domains: **default** and **default_admin**. The two domains can be modified but cannot be deleted.

Step 4 Run:

authentication-scheme *authentication-scheme-name*

An authentication scheme is applied to the domain.

By default, the authentication scheme named **default** is applied to a domain.

Step 5 (Optional) Run:

accounting-scheme *accounting-scheme-name*

An accounting scheme is applied to the domain.

By default, the accounting scheme named **default** is applied to a domain. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

Step 6 (Optional) Run:

user-group *group-name*

A user group is applied to the domain.

By default, no user group is applied to a domain.

Step 7 (Optional) Run:

service-scheme *service-scheme-name*

A service scheme is applied to the domain.

By default, no service scheme is applied to a domain.

Step 8 Run:

radius-server *template-name*

A RADIUS server template is configured for the domain.

By default, no RADIUS server template is applied to a domain.

Step 9 (Optional) Run:

state { **active** | **block** }

The domain state is configured.

When a domain is in blocking state, users in this domain cannot log in. By default, a domain is in active state after being created.

Step 10 Run:

quit

Exit from the domain view.

Step 11 (Optional) Run:

domain-name-delimiter *delimiter*

A domain name delimiter is configured.

A domain name delimiter can be any of the following: \ / : < > | @ ' %.

The default domain name delimiter is @.

Step 12 Run:

quit

Return to the system view.

Step 13 (Optional) Run:

interface wlan-bss *wlan-bss-number*

A WLAN-BSS interface is created and its view is displayed.

Step 14 (Optional) Run:

force-domain name *domain-name*

The forcible authentication domain is configured on an interface.

By default, no forcible authentication domain is configured on an interface.

NOTE

This step is applicable to only wireless users.

Step 15 (Optional) Run:

permit-domain name *domain-name* &<1-4>

The permitted domain is configured for wireless users.

By default, no permitted domain is specified for wireless users.

NOTE

This step is applicable to only wireless users.

----End

7.1.5.2.5 Checking the Configuration

Procedure

- Run the **display aaa configuration** command to check the AAA summary.
- Run the **display authentication-scheme** [*authentication-scheme-name*] command to check the authentication scheme configuration.
- Run the **display accounting-scheme** [*accounting-scheme-name*] command to check the accounting scheme configuration.
- Run the **display service-scheme** [**name** *name*] command to check the configuration about the service scheme.
- Run the **display radius-server configuration** [**template** *template-name*] command to check the RADIUS server template configuration.
- Run the **display radius-server authorization configuration** command to check the RADIUS authorization server configuration.
- Run the **display radius-attribute** [**template** *template-name*] **disable** command to check the disabled RADIUS attributes.
- Run the **display radius-attribute** [**template** *template-name*] **translate** command to check the RADIUS attribute translation configuration.
- Run the **display domain** [**name** *domain-name*] command to check the domain configuration.
- Run the **display radius-server accounting-stop-packet** { **all** | **ip** *ip-address* } command to check the accounting-stop packets of the RADIUS server.
- Run the **display radius-attribute** [**template** *template-name*] **check** command to check the attributes to be checked in RADIUS Access-Accept packets.
- Run the **display remote-user authen-fail** [**blocked** | **username** *username*] command to check the accounts that fail in remote AAA authentication.

----End

7.1.5.3 Configuring HWTACACS AAA

Compared with RADIUS, HWTACACS is more reliable in transmission and encryption, and is more suitable for security control.

HWTACACS Authentication, Authorization, and Accounting

Similar to RADIUS, HWTACACS uses the client/server model to implement AAA for access users by communicating with the HWTACACS server.

HWTACACS protects a network from unauthorized access and supports command-line authorization. Compared with RADIUS, HWTACACS is more suitable for security control.

Pre-configuration Tasks

Before configuring HWTACACS AAA, completing the following task:

- Configuring physical attributes for interfaces to ensure that the physical layer status of the interfaces is Up

7.1.5.3.1 Configuring AAA Schemes

Context

To use HWTACACS authentication, authorization, and accounting, set the authentication mode in an authentication scheme to HWTACACS, the authorization mode in an authorization scheme to HWTACACS, and the accounting mode in an accounting scheme to HWTACACS.

When HWTACACS authentication is used, you can configure local authentication or non-authentication as a backup. This allows local authentication or non-authentication to be implemented if HWTACACS authentication fails. When HWTACACS authorization is used, you can configure local authorization or non-authorization as a backup.

NOTE

By default, the same default authentication, authorization, and accounting schemes are bound to the **default** and **default_admin** domains. If the default schemes are modified, user authentication, authorization, or accounting may fail in a domain. Confirm the action before you modify the default schemes.

Procedure

- Configuring an authentication scheme
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     aaa

     The AAA view is displayed.
  3. Run:
     authentication-scheme *authentication-scheme-name*

     An authentication scheme is created, and the corresponding authentication scheme view or an existing authentication scheme view is displayed.

     By default, there is an authentication scheme named **default** on the device. This default scheme can be modified but cannot be deleted.
  4. Run:
     authentication-mode hwtacacs

     HWTACACS authentication is configured.

     By default, local authentication is used.

     To use local authentication as the backup authentication mode, run the **authentication-mode hwtacacs local** command to configure local authentication.

NOTE

If multiple authentication modes are configured in an authentication scheme, these authentication modes are used according to the sequence in which they were configured. The device uses the authentication mode that was configured later only when it does not receive any response in the current authentication. The device stops the authentication if the current authentication fails.

5. Run:
   quit

   Return to the AAA view.
6. (Optional) Run:
   domainname-parse-direction { **left-to-right** | **right-to-left** }

   The direction in which the user name and domain name are parsed is configured.
7. Run:
   quit

   Return to the system view.
8. (Optional) Run:
   aaa-authen-bypass enable time *time-value*

   The bypass authentication duration is set.

   By default, no bypass authentication duration is set.

- Configuring an authorization scheme
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     aaa

     The AAA view is displayed.
  3. Run:
     authorization-scheme *authorization-scheme-name*

     An authorization scheme is created, and the corresponding authorization scheme view or an existing authorization scheme view is displayed.

     By default, there is a default authorization scheme named **default** on the device. This default authorization scheme can be modified but cannot be deleted.
  4. Run:
     authorization-mode { **hwtacacs** | **local** }* [**none**]

     The authorization mode is configured.

     By default, local authorization is used.

     If HWTACACS authorization is configured, you must configure an HWTACACS server template and apply the template to the corresponding user domain.

NOTE

If multiple authorization modes are configured in an authorization scheme, authorization modes are used in the sequence in which they were configured. The device uses the authorization mode that was configured later only after the current authorization fails.

5. (Optional) Run:

   authorization-cmd *privilege-level* **hwtacacs** [**local**] [**none**]

   Command-line authorization is enabled for users at a certain level.

   By default, command-line authorization is disabled for users of levels 0 to 15.

   If command line authorization is enabled, you must configure an HWTACACS server template and apply the template to the corresponding user domain.

6. Run:

   quit

   Return to the AAA view.

7. Run:

   quit

   Return to the system view.

8. Run:

   quit

   Return to the system view.

9. (Optional) Run:

   aaa-author-bypass enable time *time-value*

   The bypass authorization duration is set.

   By default, no bypass authorization duration is set.

10. (Optional) Run:

    aaa-author-cmd-bypass enable time *time-value*

    The command-line bypass authorization duration is set.

    By default, no command-line bypass authorization duration is set.

- Configuring an accounting scheme

  1. Run:

     system-view

     The system view is displayed.

  2. Run:

     aaa

     The AAA view is displayed.

  3. Run:

     accounting-scheme *accounting-scheme-name*

     An accounting scheme is created, and the corresponding accounting scheme view or an existing accounting scheme view is displayed.

There is a default accounting scheme named **default** on the device. This default accounting scheme can be modified but cannot be deleted.

4. Run:
   accounting-mode hwtacacs

   The accounting mode is configured.

   By default, non-accounting is used.
5. (Optional) Run:
   accounting start-fail { **online** | **offline** }

   A policy for accounting-start failures is configured.

   By default, users cannot go online if accounting-start fails.
6. (Optional) Run:
   accounting realtime *interval*

   Real-time accounting is enabled and the interval for real-time accounting is set.

   By default, real-time accounting is disabled.
7. (Optional) Run:
   accounting interim-fail [**max-times** *times*] { **online** | **offline** }

   The maximum number of real-time accounting requests is set and a policy used after a real-time accounting failure is configured.

   After real-time accounting is enabled, the maximum number of real-time accounting requests is 3 and the device keeps paid users online after a real-time accounting failure by default.

----End

7.1.5.3.2 Configuring an HWTACACS Server Template

Context

In an HWTACACS server template, you must specify the IP address, port number, and shared key of a specified HWTACACS server. Other settings such as the HWTACACS user name format and traffic unit have default values and can be changed based on network requirements.

The HWTACACS server template settings such as the HWTACACS user name format and shared key must be the same as those on the HWTACACS server.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
hwtacacs enable

HWTACACS is enabled.

By default, HWTACACS is enabled.

Step 3 Run:

```
hwtacacs-server template template-name
```

An HWTACACS server template is created and the HWTACACS server template view is displayed.

Step 4 Run:

```
hwtacacs-server authentication ip-address [ port ] [ public-net ]
```

The primary HWTACACS authentication server is configured.

By default, no primary HWTACACS authentication server is configured.

Step 5 (Optional) Run:

```
hwtacacs-server authentication ip-address [ port ] [ public-net ] secondary
```

The secondary HWTACACS authentication server is configured.

By default, no secondary HWTACACS authentication server is configured.

Step 6 Run:

```
hwtacacs-server authorization ip-address [ port ] [ public-net ]
```

The primary HWTACACS authorization server is configured.

By default, no primary HWTACACS authorization server is configured.

Step 7 (Optional) Run:

```
hwtacacs-server authorization ip-address [ port ] [ public-net ] secondary
```

The secondary HWTACACS authorization server is configured.

By default, no secondary HWTACACS authorization server is configured.

Step 8 Run:

```
hwtacacs-server accounting ip-address [ port ] [ public-net ]
```

The primary HWTACACS accounting server is configured.

By default, no primary HWTACACS accounting server is configured.

Step 9 (Optional) Run:

```
hwtacacs-server accounting ip-address [ port ] [ public-net ] secondary
```

The secondary HWTACACS accounting server is configured.

By default, no secondary HWTACACS accounting server is configured.

Step 10 (Optional) Run:

```
hwtacacs-server user-name domain-included
```

The HWTACACS user name format is configured.

By default, the device encapsulates the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

Step 11 (Optional) Run:

```
hwtacacs-server source-ip ip-address
```

The HWTACACS source IP address is set.

By default, the HWTACACS source IP address is 0.0.0.0. The device uses the IP address of the actual outbound interface as the source IP address in HWTACACS packets.

After you set the source IP address of HWTACACS packets on the device, this IP address is used by the device to communicate with the HWTACACS server. The HWTACACS server also uses a specified IP address to communicate with the device.

Step 12 (Optional) Run:

hwtacacs-server shared-key cipher *key-string*

The HWTACACS shared key is configured.

By default, no HWTACACS shared key is configured.

Step 13 (Optional) Run:

hwtacacs-server traffic-unit { **byte** | **kbyte** | **mbyte** | **gbyte** }

The HWTACACS traffic unit is set.

The default HWTACACS traffic unit is byte on the device.

Step 14 (Optional) Run:

hwtacacs-server timer response-timeout *interval*

The response timeout interval for the HWTACACS server is set.

By default, the response timeout interval for an HWTACACS server is 5 seconds.

If the device does not receive the response from the HWTACACS server within the timeout period, the HWTACACS server is faulty. The device then uses other authentication and authorization methods.

Step 15 (Optional) Run:

hwtacacs-server timer quiet *interval*

The interval for the primary HWTACACS server to return to the active state is set.

By default, the interval for the primary HWTACACS server to return to the active state is 5 minutes.

Step 16 Run:

quit

The system view is displayed.

Step 17 (Optional) Run:

hwtacacs-server accounting-stop-packet resend { **disable** | **enable** *number* }

Retransmission of accounting-stop packets is enabled.

By default, the retransmission function is enabled and the number of retransmission times is 100.

Step 18 Run:

return

The user view is displayed.

Step 19 (Optional) Run:

hwtacacs-user change-password hwtacacs-server *template-name*

The password saved on the HWTACACS server is changed.

----End

7.1.5.3.3 (Optional) Configuring a Service Scheme

Context

Access users must obtain authorization information before going online. Authorization information about users can be managed by configuring a service scheme.

NOTE

In the service scheme, you only need to run the **admin-user privilege level** command to configure AAA. Other commands need to be configured only when they are referenced by other features such as IPSec in the service scheme.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

aaa

The AAA view is displayed.

Step 3 Run:

service-scheme *service-scheme-name*

A service scheme is created and the service scheme view is displayed.

By default, no service scheme is configured on the device.

Step 4 Run:

admin-user privilege level *level*

The user is configured to log in to the device as the administrator and the administrator level for login is specified.

level ranges from 0 to 15. By default, the user level is not configured.

Step 5 (Optional) Run:

dns *ip-address*

The IP address of the primary DNS server is configured.

By default, no primary DNS server address is configured in a service scheme.

Step 6 (Optional) Run:

dns *ip-address* **secondary**

The IP address of the secondary DNS server is configured.

By default, no secondary DNS server address is configured in a service scheme.

----End

7.1.5.3.4 Configuring a Domain

Context

The created authentication scheme, authorization scheme, accounting scheme, and HWTACACS server template take effect only after being applied to a domain.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
aaa
```

The AAA view is displayed.

Step 3 Run:

```
domain domain-name
```

A domain is created and the domain view is displayed, or an existing domain view is displayed.

By default, the device has two domains: **default** and **default_admin**. The two domains can be modified but cannot be deleted.

Step 4 Run:

```
authentication-scheme authentication-scheme-name
```

An authentication scheme is applied to the domain.

By default, the default authentication scheme is used for a domain.

Step 5 (Optional) Run:

```
authorization-scheme authorization-scheme-name
```

An authorization scheme is applied to the domain.

By default, no authorization scheme is applied to a domain.

Step 6 (Optional) Run:

```
accounting-scheme accounting-scheme-name
```

An accounting scheme is applied to the domain.

By default, the accounting scheme named **default** is applied to a domain. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

Step 7 (Optional) Run:

```
user-group group-name
```

A user group is applied to the domain.

By default, no user group is applied to a domain.

Step 8 (Optional) Run:

service-scheme *service-scheme-name*

A service scheme is applied to the domain.

By default, no service scheme is applied to a domain.

Step 9 Run:

hwtacacs-server *template-name*

An HWTACACS server template is applied to the domain.

By default, no HWTACACS server template is applied to a domain.

Step 10 (Optional) Run:

state { **active** | **block** }

The domain state is configured.

When a domain is in blocking state, users in this domain cannot log in. By default, a domain is in active state after being created.

Step 11 Run:

quit

Exit from the domain view.

Step 12 (Optional) Run:

domain-name-delimiter *delimiter*

A domain name delimiter is configured.

A domain name delimiter can be any of the following: \ / : < > | @ ' %.

The default domain name delimiter is @.

Step 13 Run:

quit

Return to the system view.

Step 14 (Optional) Run:

interface wlan-bss *wlan-bss-number*

A WLAN-BSS interface is created and its view is displayed.

Step 15 (Optional) Run:

force-domain name *domain-name*

The forcible authentication domain is configured on an interface.

By default, no forcible authentication domain is configured on an interface.

NOTE

This step is applicable to only wireless users.

Step 16 (Optional) Run:

permit-domain name *domain-name* &<1-4>

The permitted domain is configured for wireless users.

By default, no permitted domain is specified for wireless users.

NOTE

This step is applicable to only wireless users.

----End

7.1.5.3.5 Checking the Configuration

Procedure

- Run the **display aaa configuration** command to check the AAA summary.
- Run the **display authentication-scheme** [*authentication-scheme-name*] command to check the authentication scheme configuration.
- Run the **display authorization-scheme** [*authorization-scheme-name*] command to check the authorization scheme configuration.
- Run the **display accounting-scheme** [*accounting-scheme-name*] command to check the accounting scheme configuration.
- Run the **display service-scheme** [**name** *name*] command to check the configuration about the service scheme.
- Run the **display hwtacacs-server template** [*template-name* [**verbose**]] command to check the HWTACACS server template configuration.
- Run the **display hwtacacs-server accounting-stop-packet** { **all** | *number* | **ip** *ip-address* } command to check the accounting-stop packets of the HWTACACS server.
- Run the **display domain** [**name** *domain-name*] command to check the domain configuration.

----End

7.1.6 Maintaining AAA

AAA maintenance includes clearing AAA statistics.

7.1.6.1 Clearing AAA Statistics

Context

NOTICE

The AAA statistics cannot be restored after being cleared. Confirm your operation before clearing the AAA statistics.

Run the following commands to clear the statistics.

Procedure

- Run the **reset aaa** { **abnormal-offline-record** | **offline-record** | **online-fail-record** } command to clear abnormal offline records, offline records and login failures statistics.
- Run the **reset hwtacacs-server statistics** { **accounting** | **all** | **authentication** | **authorization** } command to clear the statistics on HWTACACS authentication, accounting, and authorization.
- Run the **reset hwtacacs-server accounting-stop-packet** { **all** | **ip** *ip-address* } command to clear the statistics on HWTACACS accounting-stop packets.
- Run the **reset radius-server accounting-stop-packet** { **all** | **ip** *ip-address* } command to clear the statistics on RADIUS accounting-stop packets.

----End

7.1.7 Configuration Examples

This section provides several AAA configuration examples, including networking requirements, configuration notes, and configuration roadmap.

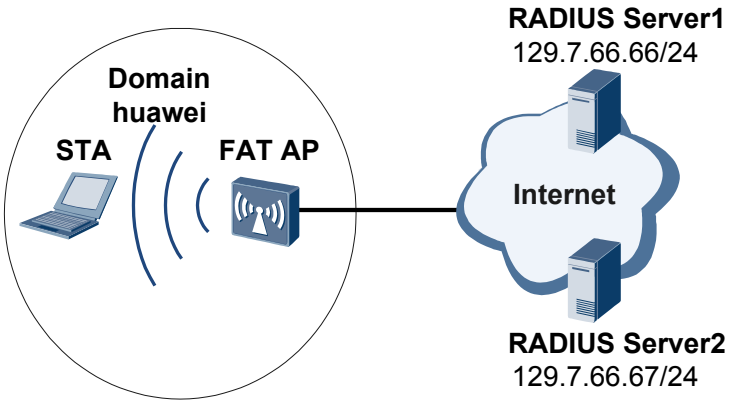
7.1.7.1 Example for Configuring RADIUS Authentication and Accounting

Networking Requirements

As shown in **Figure 7-19**, users access the network through the AP and belong to the domain **huawei**. The remote authentication configuration on the AP is as follows:

- The RADIUS server will authenticate access users for AP. If RADIUS authentication fails, local authentication is used.
- The RADIUS server at 129.7.66.66/24 functions as the primary authentication and accounting server. The RADIUS server at 129.7.66.67/24 functions as the secondary authentication and accounting server. The default authentication port and accounting port are 1812 and 1813.

Figure 7-19 Networking diagram of RADIUS authentication and accounting



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a RADIUS server template.
2. Configure an authentication scheme and an accounting scheme.
3. Apply the RADIUS server template, authentication scheme, and accounting scheme to the domain.

NOTE

The following configurations are performed on the AP.

Ensure that there are reachable routes between the AP and the RADIUS server.

Procedure

Step 1 Configure a RADIUS server template.

Configure a RADIUS template **shiva**.

```
<Huawei> system-view
[Huawei] radius-server template shiva
```

Specify the master/backup algorithm on the RADIUS server.

```
[Huawei-radius-shiva] radius-server algorithm master-backup
```

Configure the IP address and port numbers of the primary RADIUS authentication and accounting server.

```
[Huawei-radius-shiva] radius-server authentication 129.7.66.66 1812 weight 80
[Huawei-radius-shiva] radius-server accounting 129.7.66.66 1813 weight 80
```

Configure the IP address and port numbers of the secondary RADIUS authentication and accounting server.

```
[Huawei-radius-shiva] radius-server authentication 129.7.66.67 1812 weight 40
[Huawei-radius-shiva] radius-server accounting 129.7.66.67 1813 weight 40
```

Set the key and retransmission count for the RADIUS server, and configure the device not to encapsulate the domain name in the user name when sending RADIUS packets to a RADIUS server.

```
[Huawei-radius-shiva] radius-server shared-key cipher hello
[Huawei-radius-shiva] radius-server retransmit 2
[Huawei-radius-shiva] undo radius-server user-name domain-included

[Huawei-radius-shiva] quit
```

Step 2 Configure authentication and accounting schemes.

Create an authentication scheme **auth**. In the authentication scheme, the system performs RADIUS authentication first, and performs local authentication if RADIUS authentication fails.

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme auth
[Huawei-aaa-authen-auth] authentication-mode radius local
[Huawei-aaa-authen-auth] quit
```

Configure the accounting scheme **abc** that uses RADIUS accounting and the policy that the device is kept online when accounting fails.

```
[Huawei-aaa] accounting-scheme abc
[Huawei-aaa-accounting-abc] accounting-mode radius
[Huawei-aaa-accounting-abc] accounting start-fail online
[Huawei-aaa-accounting-abc] quit
```

Step 3 Configure a domain **huawei** and apply authentication scheme **auth**, accounting scheme **abc**, and RADIUS server template **shiva** to the domain.

```
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] authentication-scheme auth
[Huawei-aaa-domain-huawei] accounting-scheme abc
[Huawei-aaa-domain-huawei] radius-server shiva
[Huawei-aaa-domain-huawei] quit
[Huawei-aaa] quit
[Huawei] quit
```

NOTE

After the domain **huawei** is configured, if a user enters the user name in the format of user@huawei, the device authenticates the user in the domain **huawei**. If the user name does not contain the domain name or the domain name in the user name does not exist, the device authenticates the user in the default domain.

The domain that a user belongs to depends on the RADIUS client but not the RADIUS server. After the **undo radius-server user-name domain-included** command is executed on AP, AP sends the user name without the domain name to the RADIUS server when receiving the user name in the format of user@huawei. However, AP places the user in the domain **huawei** for authentication.

Step 4 Verify the configuration.

Run the **display radius-server configuration template** command on AP, and you can see that the configuration of the RADIUS server template meets the requirements.

```
<Huawei> display radius-server configuration template shiva
  ------------------------------------------------------------------------------
  Server-template-name          :  shiva
  Protocol-version              :  standard
  Traffic-unit                  :  B
  Shared-secret-key             :  %$%$1"y;E[c;<.(_RS/w*!`IOxof%$%$
  Timeout-interval(in second)   :  5
  Retransmission                :  2
  EndPacketSendTime             :  0
  Dead time(in minute)          :  5
  Domain-included               :  NO
  NAS-IP-Address                :  0.0.0.0
  Calling-station-id MAC-format :  xxxx-xxxx-xxxx
  Server algorithm              :  master-backup
  Authentication Server 1       :  129.7.66.66     Port:1812  Weight:80
                                   Vrf:- LoopBack:NULL
                                   Source IP: ::
  Authentication Server 2       :  129.7.66.67     Port:1812  Weight:40
                                   Vrf:- LoopBack:NULL
                                   Source IP: ::
  Accounting Server     1       :  129.7.66.66     Port:1813  Weight:80
                                   Vrf:- LoopBack:NULL
                                   Source IP: ::
  Accounting Server     2       :  129.7.66.67     Port:1813  Weight:40
                                   Vrf:- LoopBack:NULL
                                   Source IP: ::
  ------------------------------------------------------------------------------
```

----End

Configuration Files

Configuration files on AP

```
#
```

```
radius-server template shiva
 radius-server shared-key cipher %$%$1"y;E[c;<.(_RS/w*!`IOxof%$%$
 radius-server authentication 129.7.66.66 1812 weight 80
 radius-server authentication 129.7.66.67 1812 weight 40
 radius-server accounting 129.7.66.66 1813 weight 80
 radius-server accounting 129.7.66.67 1813 weight 40
 radius-server retransmit 2
 undo radius-server user-name domain-included
#
aaa
 authentication-scheme auth
  authentication-mode radius local
 accounting-scheme abc
  accounting-mode radius
  accounting start-fail online
 domain huawei
  authentication-scheme auth
  accounting-scheme abc
  radius-server shiva
#
return
```

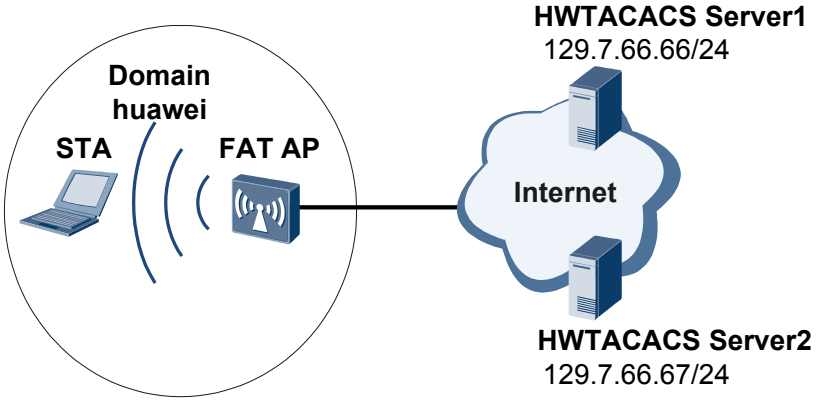
7.1.7.2 Example for Configuring HWTACACS Authentication, Accounting, and Authorization

Networking Requirements

As shown in **Figure 7-20**, the customer requirements are as follows:

- The HWTACACS server will authenticate access users for AP. If HWTACACS authentication fails, local authentication is used.
- The HWTACACS server will authorize access users for AP. If HWTACACS authorization fails, local authorization is used.
- HWTACACS accounting is used by AP for access users.
- Real-time accounting is performed every 3 minutes.
- The IP addresses of primary and secondary HWTACACS servers are 129.7.66.66/24 and 129.7.66.67/24. The port number for authentication, accounting, and authorization is 49.

Figure 7-20 Networking diagram of HWTACACS authentication, accounting, and authorization



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure an HWTACACS server template.
2. Configure authentication, authorization, and accounting schemes.
3. Apply the HWTACACS server template, authentication scheme, authorization scheme, and accounting scheme to the domain.

NOTE

Perform the following configurations only on AP.

Procedure

Step 1 Enable HWTACACS.

```
<Huawei> system-view
[Huawei] hwtacacs enable
```

NOTE

The HWTACACS function is enabled by default. If the HWTACACS configuration has not been modified, you do not need to run this command.

Step 2 Configure an HWTACACS server template.

Configure the HWTACACS server template **ht**.

```
[Huawei] hwtacacs-server template ht
```

Configure the IP addresses and port numbers of the primary HWTACACS authentication, authorization, and accounting servers.

```
[Huawei-hwtacacs-ht] hwtacacs-server authentication 129.7.66.66 49
[Huawei-hwtacacs-ht] hwtacacs-server authorization 129.7.66.66 49
[Huawei-hwtacacs-ht] hwtacacs-server accounting 129.7.66.66 49
```

Configure the IP addresses and port numbers of the secondary HWTACACS authentication, authorization, and accounting servers.

```
[Huawei-hwtacacs-ht] hwtacacs-server authentication 129.7.66.67 49 secondary
[Huawei-hwtacacs-ht] hwtacacs-server authorization 129.7.66.67 49 secondary
[Huawei-hwtacacs-ht] hwtacacs-server accounting 129.7.66.67 49 secondary
```

Configure the shared key of the HWTACACS server.

```
[Huawei-hwtacacs-ht] hwtacacs-server shared-key cipher hello
[Huawei-hwtacacs-ht] quit
```

Step 3 Configure the authentication scheme, authorization scheme, and accounting scheme.

Create an authentication scheme **l-h**. In the authentication scheme, the system performs HWTACACS authentication first, and performs local authentication if HWTACACS authentication fails.

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme l-h
[Huawei-aaa-authen-l-h] authentication-mode hwtacacs local
[Huawei-aaa-authen-l-h] quit
```

Create an authorization scheme **hwtacacs**. In the authorization scheme, the system performs HWTACACS authorization first, and performs local authorization if HWTACACS authorization fails.

```
[Huawei-aaa] authorization-scheme hwtacacs
[Huawei-aaa-author-hwtacacs] authorization-mode hwtacacs local
[Huawei-aaa-author-hwtacacs] quit
```

Create an accounting scheme **hwtacacs** and set HWTACACS accounting.

```
[Huawei-aaa] accounting-scheme hwtacacs
[Huawei-aaa-accounting-hwtacacs] accounting-mode hwtacacs
[Huawei-aaa-accounting-hwtacacs] accounting start-fail online
```

Set the interval of real-time accounting to 3 minutes.

```
[Huawei-aaa-accounting-hwtacacs] accounting realtime 3
[Huawei-aaa-accounting-hwtacacs] quit
```

Step 4 Configure a domain **huawei**, and apply the authentication scheme **l-h**, authorization scheme **hwtacacs**, accounting scheme **hwtacacs**, and the HWTACACS server template **ht** to the domain.

```
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] authentication-scheme l-h
[Huawei-aaa-domain-huawei] authorization-scheme hwtacacs
[Huawei-aaa-domain-huawei] accounting-scheme hwtacacs
[Huawei-aaa-domain-huawei] hwtacacs-server ht
[Huawei-aaa-domain-huawei] quit
[Huawei-aaa] quit
[Huawei] quit
```

Step 5 Verify the configuration.

Run the **display hwtacacs-server template** command on AP, and you can see that the configuration of the HWTACACS server template meets the requirements.

```
<Huawei> display hwtacacs-server template ht
  ------------------------------------------------------------------------------
  HWTACACS-server template name   : ht
  Primary-authentication-server   : 129.7.66.66:49:-
  Primary-authorization-server    : 129.7.66.66:49:-
  Primary-accounting-server       : 129.7.66.66:49:-
  Secondary-authentication-server : 129.7.66.67:49:-
  Secondary-authorization-server  : 129.7.66.67:49:-
  Secondary-accounting-server     : 129.7.66.67:49:-
  Current-authentication-server   : 129.7.66.66:49:-
  Current-authorization-server    : 129.7.66.66:49:-
  Current-accounting-server       : 129.7.66.66:49:-
  Source-IP-address               : 0.0.0.0
  Shared-key                      : ***************
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : Yes
  Traffic-unit                    : B
  ------------------------------------------------------------------------------
```

Run the **display domain** command on AP, and you can see that the configuration of the domain meets the requirements.

```
<Huawei> display domain name huawei

  Domain-name                     : huawei
  Domain-state                    : Active
  Authentication-scheme-name      : l-h
  Accounting-scheme-name          : hwtacacs
  Authorization-scheme-name       : hwtacacs
  Service-scheme-name             : -
  RADIUS-server-template          : -
  HWTACACS-server-template        : ht
```

```
  User-group                    : -
```

----End

Configuration Files

Configuration files on AP

```
#
hwtacacs-server template ht
 hwtacacs-server authentication 129.7.66.66
 hwtacacs-server authentication 129.7.66.67 secondary
 hwtacacs-server authorization 129.7.66.66
 hwtacacs-server authorization 129.7.66.67 secondary
 hwtacacs-server accounting 129.7.66.66
 hwtacacs-server accounting 129.7.66.67 secondary
 hwtacacs-server shared-key cipher %$%$|)&LT+J>dN>=IqD<gO/Fj$xo%$%$
#
aaa
 authentication-scheme default
 authentication-scheme l-h
  authentication-mode hwtacacs local
 authorization-scheme default
 authorization-scheme hwtacacs
  authorization-mode  hwtacacs local
 accounting-scheme default
 accounting-scheme hwtacacs
  accounting-mode hwtacacs
  accounting realtime 3
  accounting start-fail online
 domain default
 domain default_admin
 domain huawei
  authentication-scheme l-h
 authorization-scheme hwtacacs
  accounting-scheme hwtacacs
  hwtacacs-server ht
#
return
```

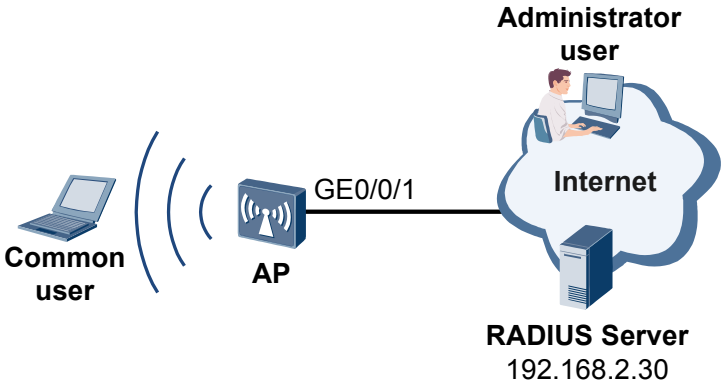
7.1.7.3 Example for Configuring Default Domain-based User Management

Networking Requirements

As shown in **Figure 7-21**, a Fat AP of an enterprise provides wireless Internet access service and functions as a DHCP server to allocate IP addresses to users.

The enterprise administrator wants to allow users to log in without entering the domain name. Common 802.1x users can access the network and obtain corresponding rights after they pass the RADIUS authentication and administrative users can log in and manage the users after they pass the local authentication on the FAT AP.

Figure 7-21 Networking diagram for configuring default domain-based user management



Configuration Roadmap

1. Configure the WLAN service so that STAs can connect to the WLAN. This example uses default configuration parameters.
2. Configure an authentication and accounting scheme and apply it to the default domain **default** to authenticate common access users. In this example, the common user name does not contain the domain name and the common users use 802.1x or Portal authentication.
3. Configure an authentication and accounting scheme and apply it to the default domain **default_admin** to authenticate administrative users. In this example, the administrative user name does not contain the domain name and the administrative users log in through Telnet, SSH, or FTP.

NOTE

Ensure that the Fat AP and the RADIUS server have reachable routes to each other and the RADIUS server IP address, port number, and shared key in the RADIUS server template are configured correctly and are the same as those on the RADIUS server.

Ensure that you have configured a user on the RADIUS server. In this example, the user name is **test1** and the password is **123456**.

Procedure

Step 1 Configure basic WLAN services.

1. Configure basic Fat AP functions.

   # Configure the country code for the Fat AP.

   ```
   <Quidway> system-view
   [Quidway] sysname FAT AP
   [FAT AP] wlan global country-code cn
   ```

   # Create the VLANIF 100 and an IP address, and configure the VLANIF 100 to allocate IP addresses to STAs from an IP address pool.

   ```
   [FAT AP] vlan batch 100
   [FAT AP] dhcp enable
   [FAT AP] interface vlanif 100
   [FAT AP-Vlanif100] ip address 192.168.10.1 24
   [FAT AP-Vlanif100] dhcp select interface
   [FAT AP-Vlanif100] quit
   ```

2. Configure WLAN service parameters.

Create a WMM profile **wmm**.

```
[FAT AP] wlan
[FAT AP-wlan-view] wmm-profile name wmm id 1
[FAT AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile **radio** and bind the WMM profile **wmm** to the radio profile.

```
[FAT AP-wlan-view] radio-profile name radio id 1
[FAT AP-wlan-radio-prof-radio] wmm-profile name wmm
[FAT AP-wlan-radio-prof-radio] quit
[FAT AP-wlan-view] quit
```

Bind the radio profile **radio** to a radio interface.

```
[FAT AP] interface wlan-radio 0/0/0
[FAT AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume
defaul
t value, are you sure to continue?[Y/N]: y
[FAT AP-Wlan-Radio0/0/0] quit
```

Configure a WLAN-BSS interface so that radio packets sent from users can be sent to the WLAN service processing module after reaching the AP.

```
[FAT AP] interface wlan-bss 1
[FAT AP-Wlan-Bss1] port hybrid pvid vlan 100
[FAT AP-Wlan-Bss1] port hybrid untagged vlan 100
[FAT AP-Wlan-Bss1] quit
```

Create a security profile **security**.

```
[FAT AP] wlan
[FAT AP-wlan-view] security-profile name security id 1
[FAT AP-wlan-sec-prof-security] quit
```

Create the traffic profile **traffic**.

```
[FAT AP-wlan-view] traffic-profile name traffic id 1
[FAT AP-wlan-traffic-prof-traffic] quit
```

Create a service set **test** and bind it to the WLAN-BSS interface, security profile, and traffic profile.

```
[FAT AP-wlan-view] service-set name test id 1
[FAT AP-wlan-service-set-test] ssid test
[FAT AP-wlan-service-set-test] wlan-bss 1
[FAT AP-wlan-service-set-test] security-profile name security
[FAT AP-wlan-service-set-test] traffic-profile name traffic
[FAT AP-wlan-service-set-test] quit
[FAT AP-wlan-view] quit
```

Bind the service set **test** to a radio interface.

```
[FAT AP] interface wlan-radio 0/0/0
[FAT AP-Wlan-Radio0/0/0] service-set name test
[FAT AP-Wlan-Radio0/0/0] quit
```

Step 2 Configure RADIUS AAA for common 802.1x users.

Create and configure a RADIUS server template **rd1**.

```
[FAT AP] radius-server template rd1
[FAT AP-radius-rd1] radius-server authentication 192.168.2.30 1812
[FAT AP-radius-rd1] radius-server accounting 192.168.2.30 1813
[FAT AP-radius-rd1] radius-server shared-key cipher hello
[FAT AP-radius-rd1] radius-server retransmit 2
[FAT AP-radius-rd1] quit
```

Create an authentication scheme **abc** and accounting scheme **abc**, and set the authentication mode and accounting mode to RADIUS.

```
[FAT AP] aaa
[FAT AP-aaa] authentication-scheme abc
[FAT AP-aaa-authen-abc] authentication-mode radius
[FAT AP-aaa-authen-abc] quit
[FAT AP-aaa] accounting-scheme abc
[FAT AP-aaa-accounting-abc] accounting-mode radius
[FAT AP-aaa-accounting-abc] quit
```

Test the connection between the Fat AP and the RADIUS server. (A test user account has been configured on the RADIUS server, with the user name **test1** and the password **123456**.)

```
[FAT AP-aaa] test-aaa test1 123456 radius-template rd1
Info: Account test succeed.
```

Bind the authentication scheme **abc**, accounting scheme **abc**, and RADIUS server template **rd1** to the default domain **default**.

```
[FAT AP-aaa] domain default
[FAT AP-aaa-domain-default] authentication-scheme abc
[FAT AP-aaa-domain-default] accounting-scheme abc
[FAT AP-aaa-domain-default] radius-server rd1
[FAT AP-aaa-domain-default] quit
[FAT AP-aaa] quit
```

Configure wireless users to use the authentication modes in the domains **default** and **default_admin**.

```
[FAT AP] interface wlan-bss 1
[FAT AP-Wlan-Bss1] permit-domain name default
[FAT AP-Wlan-Bss1] force-domain name default
[FAT AP-Wlan-Bss1] quit
```

Enable 802.1x authentication globally and on an interface.

```
[FAT AP] dot1x enable
[FAT AP] interface wlan-bss 1
[FAT AP-Wlan-Bss1] dot1x enable
```

Set the authentication mode to EAP for 802.1x users.

```
[FAT AP-Wlan-Bss1] dot1x authentication-method eap
[FAT AP-Wlan-Bss1] quit
```

Configure the WPA IPSec policy.

```
[FAT AP] wlan
[FAT AP-wlan-view] security-profile name security
[FAT AP-wlan-sec-prof-security] security-policy wpa
[FAT AP-wlan-sec-prof-security] wpa authentication-method dot1x encryption-method
ccmp
[FAT AP-wlan-sec-prof-security] quit
[FAT AP-wlan-view] quit
```

Bind the service set **test** to the radio interface.

```
[FAT AP] interface wlan-radio 0/0/0
[FAT AP-Wlan-Radio0/0/0] service-set name test
[FAT AP-Wlan-Radio0/0/0] quit
```

Set the global default domain for common users to **default**. After common users enter their user names in the format of user@default, the device performs AAA authentication on these users in the default domain. If a user name does not contain a domain name or the domain name does not exist, the device authenticates the common user in the default common domain.

```
[AP] domain default
```

Step 3 Configure the administrative user **test** to use local authentication and authorization.

Configure Telnet users to use the AAA authentication mode when logging in to the device through the VTY user interface.

```
[FAT AP] user-interface vty 0 14
[FAT AP-ui-vty0-14] authentication-mode aaa
[FAT AP-ui-vty0-14] quit
```

Create a local user **test** and set the password to **admin@12345** and the user level to 3.

```
[FAT AP] aaa
[FAT AP-aaa] local-user test password cipher admin@12345 privilege level 3
```

Configure the user **test** to log in through Telnet.

```
[FAT AP-aaa] local-user test service-type telnet
```

Enable locking of the local account, set the retry interval to 5 minutes, limit the authentication failure times to 3, and set the account locking interval to 5 minutes.

```
[FAT AP-aaa] local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time
5
```

Configure the authentication scheme **auth** and set the authentication mode to local.

```
[FAT AP-aaa] authentication-scheme auth
[FAT AP-aaa-authen-auth] authentication-mode local
[FAT AP-aaa-authen-auth] quit
```

Configure the authorization scheme **autho** and set the authorization mode to local.

```
[FAT AP-aaa] authorization-scheme autho
[FAT AP-aaa-author-autho] authorization-mode local
[FAT AP-aaa-author-autho] quit
```

Configure a domain **default_admin** and apply the authentication scheme **auth** and authorization scheme **autho** to the domain.

```
[FAT AP-aaa] domain default_admin
[FAT AP-aaa-domain-default_admin] authentication-scheme auth
[FAT AP-aaa-domain-default_admin] authorization-scheme autho
[FAT AP-aaa-domain-default_admin] quit
[FAT AP-aaa] quit
[FAT AP] quit
```

Set the global default domain for administrative users to **default_admin**. After administrative users enter their user names in the format of user@default_admin, the device performs AAA authentication on these users in the default_admin domain. If a user name does not contain a domain name or the domain name does not exist, the device authenticates the administrative user in the default administrative domain.

```
[AP] domain default_admin admin
```

Step 4 Verify the configuration.

- The WLAN with the SSID **test** is available for STAs after the configuration is complete.
- The STAs obtain IP addresses when they successfully associate with the WLAN.
- Use 802.1x authentication on the STA and enter the user name and password. After the STA authentication succeeds, the STA can access the Internet. Configure the STA based on the configured authentication mode PEAP.

- Configuration on the Windows XP operating system:
  1. On the **Association** tab page of the **Wireless network properties** dialog box, add the SSID **test**, set the authentication mode to **WPA**, the encryption mode to **CCMP**, and the encryption algorithm to **AES**.
  2. On the **Authentication** tab page, set **EAP type** to PEAP and click **Properties**. In the dialog box that is displayed, deselect **Validate server certificate** and click **Configure...**. In the dialog box that is displayed, deselect **Automatically use my Windows logon name and password** and click **OK**.
- Configuration on the Windows 7 operating system:
  1. Access the **Manage wireless networks** page, click **Add** and select **Manually create a network profile**. In the dialog box that is displayed, add the SSID **test**, set the authentication mode to **WPA-Enterprise**, the encryption mode to **CCMP**, and the encryption algorithm to **AES**, and click **Next**.
  2. Scan SSIDs and double-click the the SSID **test**. On the **Security** tab page, set **EAP type** to PEAP and click **Settings**. In the dialog box that is displayed, deselect **Validate server certificate** and click **Configure...**. In the dialog box that is displayed, deselect **Automatically use my Windows logon name and password** and click **OK**.

Run the **display dot1x interface** command on the Fat AP to view the 802.1x authentication configuration.

```
<Huawei> display dot1x interface wlan-bss 1

 Wlan-Bss1 status: UP  802.1x protocol is Enabled
  Port control type is Auto
  Authentication mode is MAC-based
  Authentication method is CHAP
  Reauthentication is disabled
  Maximum users: 2048
  Current users: 0
  Guest VLAN is disabled
  Restrict VLAN is disabled

  Authentication Success: 0          Failure: 0
  EAPOL Packets: TX     : 0          RX     : 0
  Sent      EAPOL Request/Identity Packets  : 0
            EAPOL Request/Challenge Packets : 0
            Multicast Trigger Packets       : 0
            EAPOL Success Packets           : 0
            EAPOL Failure Packets           : 0
  Received  EAPOL Start Packets             : 0
            EAPOL Logoff Packets            : 0
            EAPOL Response/Identity Packets : 0
            EAPOL Response/Challenge Packets: 0
```

After STAs go online, run the **display access-user domain** and **display access-user user-id** commands on the AP to view the domain to which the users belong and the AP type.

```
<Huawei> display access-user domain default
 ------------------------------------------------------------------------------
 UserID Username                       IP address                  MAC
 ------------------------------------------------------------------------------
 21     test1                          -                        00e0-4c97-31f6
 ------------------------------------------------------------------------------
<Huawei> display access-user user-id 21

Basic:
  User id                         : 21
```

```
  User name                       : test1
  Domain-name                     : default
  User MAC                        : 00e0-4c97-31f6
  User IP address                 : -
  User access Interface           : Wlan-BSS1
  QinQVlan/UserVlan               : 0/100
  User access time                : 2009/02/15 19:10:52
  User accounting session ID      : 6010SN_000000000001007ae4b5000029
  User access type                : 802.1x
  AP ID                           : 0
  AP name                         : ap-0
  Radio ID                        : 0
  AP MAC                          : dcd2-fc9a-2110
  SSID                            : test
  Online time                     : 139(s)

AAA:
  User authentication type        : 802.1x authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : RADIUS
```

The network administrator can log in to the Fat AP from the NMS through Telnet. After entering the user name **test** and password **admin@12345**, the network administrator can run the **display access-user domain** and **display access-user user-id** commands on the Fat AP to view the domain to which the users belong and the AP type.

```
<Huawei> display access-user domain default_admin
 ------------------------------------------------------------------------------
 UserID Username                         IP address                   MAC
 ------------------------------------------------------------------------------
 4      test                             172.168.254.204               -
 ------------------------------------------------------------------------------
<Huawei> display access-user user-id 4

Basic:
  User ID                         : 4
  User name                       : huawei123
  Domain-name                     : default_admin
  User MAC                        : -
  User IP address                 : 172.168.254.204
  User access time                : 2005/09/03 09:36:19
  User accounting session ID      : 6010SN_002552550000000001e736e000004
  User access type                : Telnet
  Idle Timeout                    : 4294967236(s)

AAA:
  User authentication type        : Administrator authentication
  Current authentication method   : Local
  Current authorization method    : Local
  Current accounting method       : None
```

----End

Configuration File

- Configuration file of the Fat AP

```
#
 sysname FAT AP
#
 vlan batch 100
#
 dhcp enable
#
radius-server template rd1
```

```
 radius-server shared-key cipher %@%@v|a4U)IVs9Y2PV:KP:QE;]Y%%@%@
 radius-server authentication 192.168.2.30 1812 weight 80
 radius-server accounting 192.168.2.30 1813 weight 80
 radius-server retransmit 2
#
aaa
 authentication-scheme auth
 authentication-scheme abc
  authentication-mode radius
 authorization-scheme autho
 accounting-scheme abc
  accounting-mode radius
 domain default
  authentication-scheme abc
  accounting-scheme abc
  radius-server rd1
 domain default_admin
  authentication-scheme auth
  authorization-scheme autho
 local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 5
 local-user test password cipher %@%@5otGNzZ6S.<Z14-)wmg3;RM#%@%@
 local-user test privilege level 3
 local-user test service-type telnet
#
interface Vlanif100
 ip address 192.168.10.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.2.29 255.255.255.0
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 dot1x enable
 dot1x authentication-method eap
 permit-domain name default
 force-domain name default
#
user-interface vty 0 14
 authentication-mode aaa
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
  security-policy wpa
  wpa authentication-method dot1x peap encryption-method ccmp
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
  service-vlan 101
 radio-profile name radio id 1
  wmm-profile id 1
 ap 0 radio 0
  radio-profile id 1
  service-set id 1 wlan 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-ser id 1 wlan 1
#
return
```

7.1.8 References

This section provides the AAA-related RFC recommendations.

Document	Description	Remarks
RFC 2093	Generic AAA Architecture	-
RFC 2094	AAA Authorization Framework	-
RFC 2095	AAA Authorization Application Examples	-
RFC 2096	AAA Authorization Requirements	-
RFC 2058	Remote Authentication Dial In User Service (RADIUS)	-
RFC 2059	RADIUS Accounting	-
RFC 2138	Remote Authentication Dial In User Service (RADIUS)	-
RFC 2139	RADIUS Accounting	-
RFC 2809	Implementation of L2TP Compulsory Tunneling via RADIUS	-
RFC 2865	Remote Authentication Dial In User Service (RADIUS)	-
RFC 2866	RADIUS Accounting	-
RFC 2868	RADIUS Attributes for Tunnel Protocol Support	-
RFC 2869	RADIUS Extensions	-
RFC 0927	TACACS user identification Telnet option	-

7.2 NAC Configuration

This section describes principles and configuration methods of NAC and provides configuration examples.

NOTE

The device supports NAC. NAC controls a user's network access permission that involves personal communication information collection or storage. Huawei will not collect or save user communication information independently. You must use the features in compliance with applicable laws and regulations. Ensure that your customers' privacy is protected when you are collecting or saving communication information.

7.2.1 Overview

This section describes the definition, background, and functions of NAC.

Definition

Network Admission Control (NAC) is an end-to-end access security framework and includes 802.1x authentication, MAC address authentication, and Portal authentication.

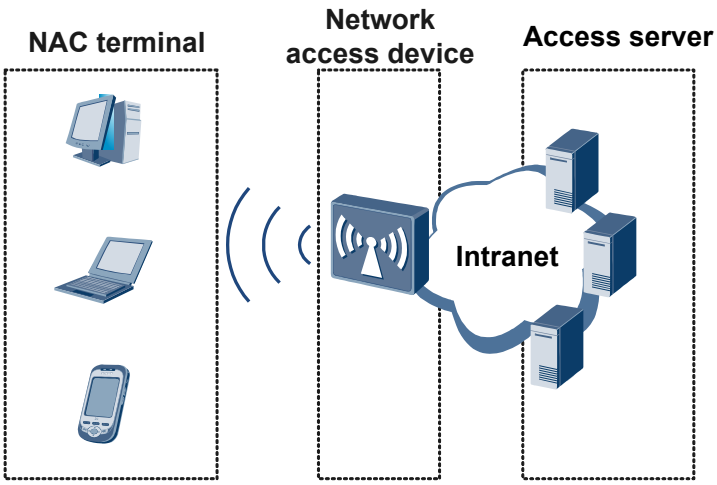
With the development of enterprise network, threats increasingly bring risks, such as viruses, Trojan horses, spyware, and malicious network attacks. On a traditional enterprise network, the intranet is considered as secure and threats come from extranet. However, 80% security threats actually come from the intranet. The intranet threats will cause serious damage in a wide range. Even worse, the system and network will break down. In addition, when internal users browse websites on the external network, the spyware and Trojan horse software may be automatically installed on users' computers, which cannot be sense by the users. Te malicious software may spread on the internal network.

The traditional security measures cannot meet requirements on border defense due to increasing security challenges. The security model should be converted into active mode to solve security problems from the roots (terminals), improving information security level of the entire enterprise.

The NAC solution integrates terminal security and access control and takes the check, audit, secure, and isolation measures to improve the proactive protection capability of terminals. This solution ensures security of each terminal and the entire enterprise network.

As shown in **Figure 7-22**, NAC includes three components: NAC terminal, network access device, and access server.

Figure 7-22 Typical NAC networking diagram



- NAC terminal: functions as the NAC client and interacts with network access devices to authenticate access users. If 802.1x authentication is used, users must install client software.
- Network access device: function as the network access control point that enforces enterprise security policies. It allows, rejects, isolates, or restricts users based on the security policies customized for enterprise networks.
- Access server: includes the access control server, management server, antivirus server, and patch server. It authenticates users, checks terminal security, repairs and upgrades the system, and monitors and audits user actions.

Purpose

Traditional network security technologies focus on threats from external computers, but typically neglect threats from internal computers. In addition, current network devices cannot prevent attacks initiated by devices on internal networks.

The NAC security framework was developed to ensure the security of network communication services. The NAC security framework improves internal network security by focusing on user terminals, and implement security control over access users to provide end-to-end security.

7.2.2 Principles

This section describes the implementation of NAC.

7.2.2.1 802.1x Authentication

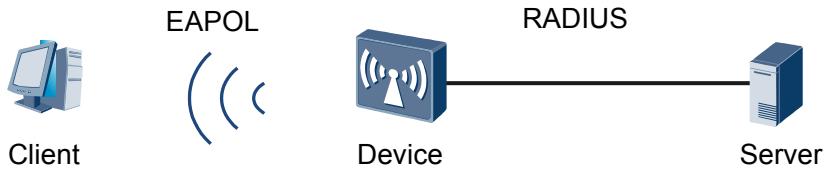
Overview

To resolve wireless local area network (LAN) security issues, the Institute of Electrical and Electronics Engineers (IEEE) 802 LAN/wide area network (WAN) committee developed the 802.1x protocol. Later, the 802.1x protocol was widely applied as a common access control mechanism on LAN interfaces for authentication and security on Ethernet networks.

The 802.1x protocol is an interface-based network access control protocol. It controls users' access to network resources by authenticating the users on access interfaces.

As shown in **Figure 7-23**, an 802.1x system uses a standard client/server architecture with three components: client, device, and server.

Figure 7-23 Diagram of 802.1x authentication system



- The client is the entity at an end of the LAN segment and is authenticated by a device at the other end of the link. The client is usually a user terminal. The user initiates 802.1x authentication using client software. The client must support Extensible Authentication Protocol over LAN (EAPOL).
- The device is the entity at an end of the LAN segment, which authenticates the connected client. The device is usually a network device that supports the 802.1x protocol. The device provides an interface, either physical or logical, for the client to access the LAN.
- The authentication server is the entity that provides authentication service for the device. The authentication server carries out authentication, authorization, and accounting on users, and is usually a RADIUS server.

Authentication Modes

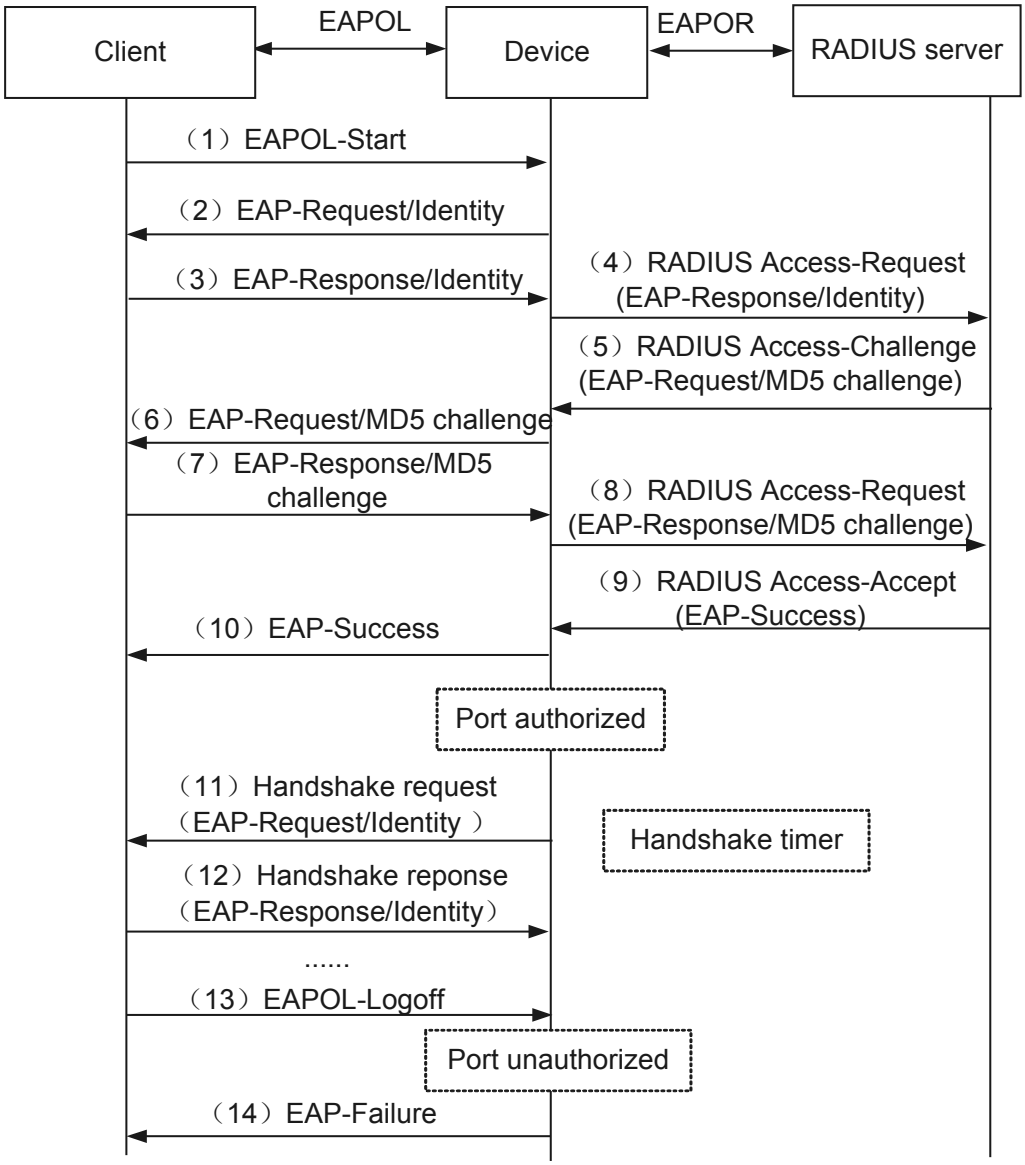
The 802.1x authentication system exchanges authentication information among the client, device, and authentication server using the Extensible Authentication Protocol (EAP). The exchange of EAP packets among the components is described as follows:

1. The EAP packets transmitted between the client and device are encapsulated in EAPOL format and transmitted across the LAN.
2. The device and RADIUS server exchange EAP packets in the following modes:
   - EAP relay: The device relays EAP packets. The device encapsulates EAP packets in EAP over RADIUS (EAPoR) format and sends the packets to the RADIUS server for authentication. This authentication mode simplifies device processing and supports various EAP authentication methods, such as MD5-Challenge, EAP-TLS, and PEAP. However, the RADIUS server must support the corresponding authentication methods.
   - EAP termination: The device terminates EAP packets. The device encapsulates client authentication information into standard RADIUS packets, which are then authenticated by the RADIUS server using the Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). This authentication mode is applicable since the majority of RADIUS servers support PAP and CHAP authentication and server update is unnecessary. However, device processing is complex, and the device supports only the MD5-Challenge EAP authentication method.

The 802.1X authentication system can complete authentication by exchanging information with the RADIUS server in EAP relay mode and EAP termination mode. **Figure 7-24** and **Figure 7-25** demonstrate both of these authentication modes using the client triggering mode.

1. EAP relay authentication

Figure 7-24 Service process in EAP relay mode



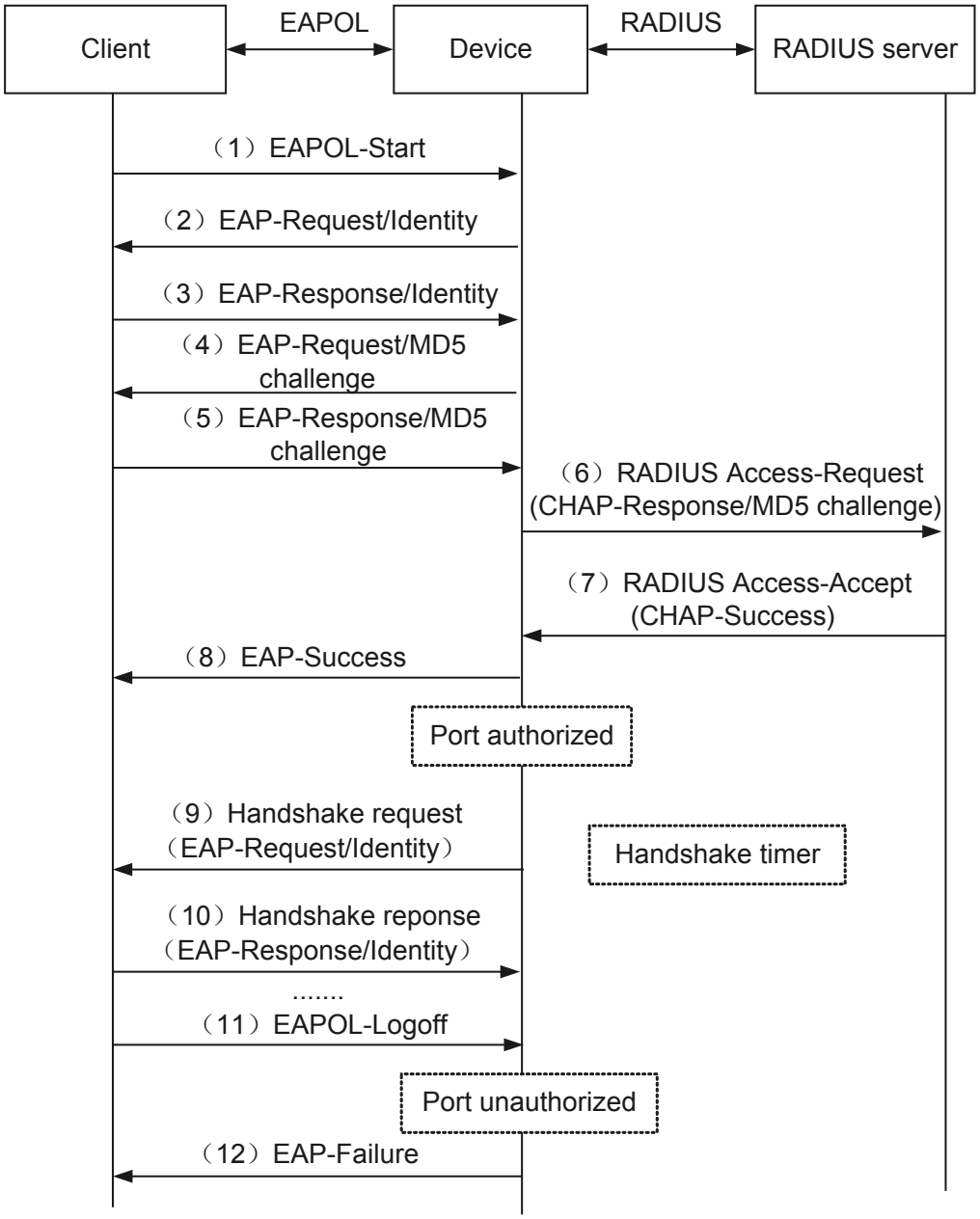
The EAP relay authentication process is described as follows:

1. When a user needs to access an external network, the user starts the 802.1x client program, enters the applied and registered user name and password, and initiates a connection request. At this point, the client sends an authentication request frame (EAPOL-Start) to the device to start the authentication process.
2. After receiving the authentication request frame, the device returns an identity request frame (EAP-Request/Identity), requesting the client to send the previously entered user name.
3. In response to the request sent by the device, the client sends an identity response frame (EAP-Response/Identity) containing the user name to the device.
4. The device encapsulates the EAP packet in the response frame sent by the client into a RADIUS packet (RADIUS Access-Request) and sends the RADIUS packet to the authentication server for processing.

5. After receiving the user name forwarded by the device, the RADIUS server searches the user name table in the database for the corresponding password, encrypts the password with a randomly generated MD5 challenge value, and sends the MD5 challenge value in a RADIUS Access-Challenge packet to the device.
6. The device forwards the MD5 challenge value sent by the RADIUS server to the client.
7. After receiving the MD5 challenge value from the device, the client encrypts the password with the MD5 challenge value, generates an EAP-Response/MD5-Challenge packet, and sends the packet to the device.
8. The device encapsulates the EAP-Response/MD5-Challenge packet into a RADIUS packet (RADIUS Access-Request) and sends the RADIUS packet to the RADIUS server.
9. The RADIUS server compares the received encrypted password and the locally encrypted password. If the two passwords match, the user is considered authorized and the RADIUS server sends a packet indicating successful authentication (RADIUS Access-Accept) to the device.
10. After receiving the RADIUS Access-Accept packet, the device sends a frame indicating successful authentication (EAP-Success) to the client, changes the interface state to Authorized, and allows the user to access the network using the interface.
11. When the user is online, the device periodically sends a handshake packet to the client to monitor the online user.
12. After receiving the handshake packet, the client sends a response packet to the device, indicating that the user is still online. By default, the device disconnects the user if it receives no response from the client after sending two handshake packets. The handshake mechanism allows the server to detect unexpected user disconnections.
13. If the user wants to go offline, the client sends an EAPOL-Logoff frame to the device.
14. The device changes the interface state from Authorized to Unauthorized and sends an EAP-Failure packet to the client.

2. EAP termination authentication

Figure 7-25 Service process in EPA termination mode



Compared with the EAP relay mode, in EAP termination mode, the device randomly generates an MD5 challenge value for encrypting the user password in Step 4, and sends the user name, the MD5 challenge value, and the password encrypted on the client to the RADIUS server for authentication.

User Group Authorization

The device can authorize users based on the user group. After users are authenticated, the authentication server groups users together. Each user group is bound to an ACL so that users in the same user group share an ACL.

7.2.2.2 MAC Address Authentication

Overview

MAC address authentication controls a user's network access permission based on the user's interface and MAC address. The user does not need to install any client software. After detecting the user's MAC address for the first time on an interface where MAC address authentication is running, the device begins authenticating the user. During the authentication, the user does not need to enter a user name or password.

According to the format and contents of the user name that the device finally uses to authenticate the user, MAC address authentication user name formats are classified into two types:

- MAC address user name: The user's MAC address is used as the user name and password during authentication.
- Fixed user name: Regardless of users' MAC addresses, all users use a fixed name and password specified on the device rather than their MAC address as an identity for authentication. Many users may be authenticated on the same interface. In this case, all users requiring MAC address authentication on the interface use the same fixed user name, and the server only needs to configure one user account to meet the authentication demands of all users, which is applicable to a network environment with reliable access clients.

User Group Authorization

The device can authorize users based on the user group. After users are authenticated, the authentication server groups users together. Each user group is bound to an ACL so that users in the same user group share an ACL.

7.2.2.3 Portal Authentication

Introduction to Portal Authentication

Portal authentication is also called web authentication. Generally, Portal authentication websites are also called Portal websites.

When an unauthenticated user accesses the Internet, the device forcibly redirects the user to a specific site. The user then can access resources in the specific site for free. When the user needs to access resources outside the specific site, the user must pass authentication on the portal authentication website first.

A user can access a known Portal authentication website and enter a user name and password for authentication. This mode is called active authentication. If a user attempts to access other external networks through HTTP, the device forcibly redirects the user to the Portal authentication website for Portal authentication. This mode is called forcible authentication.

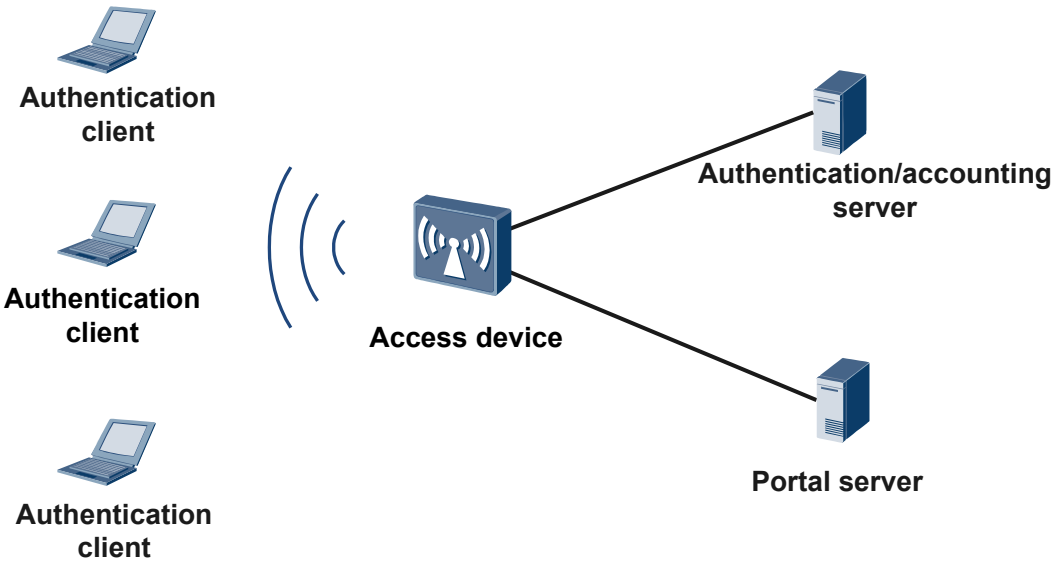
System Architecture

A Portal server can be an external Portal server, or a built-in Portal server.

- **Using an external Portal server**

As shown in **Figure 7-26**, typical networking of a Portal authentication system consists of four entities: authentication client, access device, Portal server, and authentication/accounting server.

Figure 7-26 Portal authentication system using an external Portal server

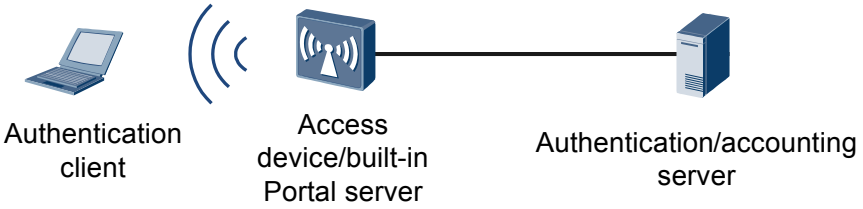


1. Authentication client: is a client system installed on a user terminal. The user terminal can be a browser running HTTP/HTTPS or a host running Portal client software.
2. Access device: is a broadband access device such as switch or router. It provides the following functions:
   - Redirects all HTTP requests from users on authentication subnets to the Portal server before authentication.
   - Interacts with the Portal server and the authentication/accounting server to implement identity authentication/accounting during authentication.
   - Allows the user to access authorized Internet resources after the authentication is passed.
3. Portal server: receives authentication requests from the Portal client. It provides free Portal services and an interface based on web authentication, and exchanges authentication information of the authentication client with the access device.
4. Authentication/accounting server: interacts with the access device to implement user authentication and accounting.

- **Portal authentication system using a built-in Portal server**

The access device with the built-in Portal server implements all Portal server functions. In this case, the Portal authentication system only includes three entities: authentication client, access device, and authentication/accounting server, as shown in **Figure 7-27**.

Figure 7-27 Portal authentication system using a built-in Portal server



The built-in Portal server provides Portal authentication, without the need to deploy an extra Portal server.

The built-in Portal server implements basic functions of the Portal server, including web-based login and logout. It cannot replace the independent Portal server or extensions.

Authentication Modes

Different Portal authentication modes can be used in different networking modes. Portal authentication is classified into Layer 2 and Layer 3 authentication according to the network layer on which it is implemented.

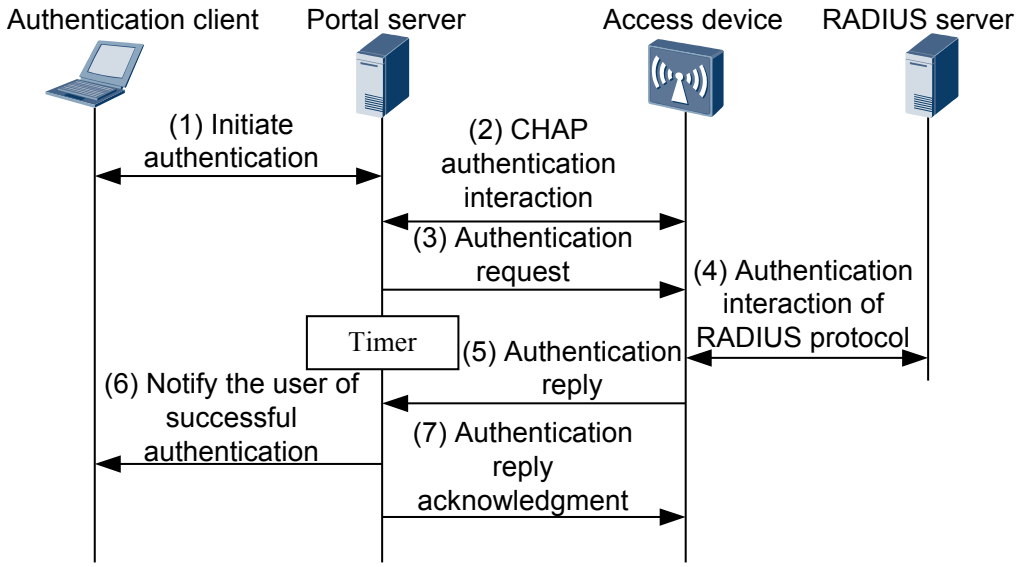
- **Layer 2 authentication**

The authentication client and access device are directly connected (or only Layer 2 devices exist between the authentication client and an access device). The device can learn a user's MAC address, and uses an IP address and a MAC address to identify the user. Portal authentication is configured as Layer 2 authentication.

Layer 2 authentication is simple and highly secure. However, it requires that the user reside on the same subnet as the access device, which makes the networking inflexible.

Figure 7-28 illustrates the packet interaction process when the user goes online and Layer 2 authentication is used.

Figure 7-28 Layer 2 authentication flowchart



1. A Portal user initiates an authentication request through HTTP. The access device allows an HTTP packet destined for the Portal server or an HTTP packet destined for the configured authentication-free network resources to pass. The access device redirects HTTP packets accessing other addresses to the Portal server. The Portal server provides a web page where the user can enter a user name and password for authentication.
2. The Portal server exchanges information with the access device to implement CHAP authentication. If PAP authentication is used, the Portal service directly performs step 3 without exchanging information with the access device to implement PAP authentication.
3. The Portal server sends the user name and password entered by the user to the access device through an authentication request packet, and meanwhile, starts a timer to wait for an authentication reply packet.

4. The access device exchanges a RADIUS protocol packet with the RADIUS server.
5. The access device sends an authentication reply packet to the Portal server.
6. The Portal server sends a packet to the client indicating that the authentication succeeded and notifying the client that the authentication succeeded.
7. The Portal server sends an authentication reply acknowledgment to the access server.

- **Layer 3 authentication**

When the device is deployed at the aggregation or core layer, Layer 3 forwarding devices exist between the authentication client and device. In this case, the device may not obtain the MAC address of the authentication client. Therefore, only the IP address identifies the user. Portal authentication is configured as Layer 3 authentication.

The Layer 3 authentication process is the same as the Layer 2 authentication process. Networking of Layer 3 authentication is flexible, which facilitates remote control. However, only an IP address can be used to identify a user, so Layer 3 authentication has low security.

User Group Authorization

The device can authorize users based on the user group. After users are authenticated, the authentication server groups users together. Each user group is bound to an ACL so that users in the same user group share an ACL.

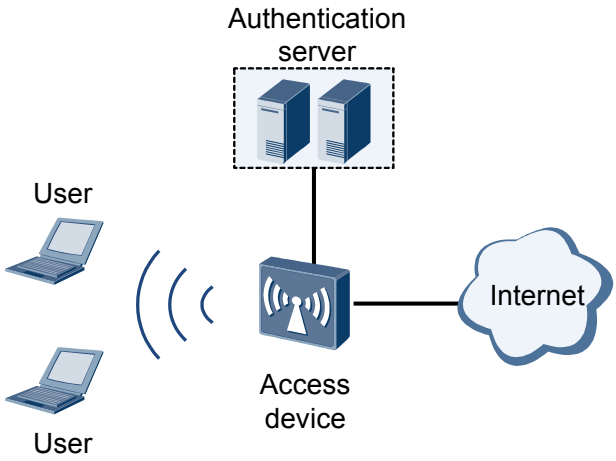
7.2.3 Applications

This section describes the applicable scenario of NAC.

7.2.3.1 802.1x Authentication

As shown in **Figure 7-29**, users' network access needs to be controlled to ensure network security. Only authenticated users are allowed to access network resources authorized by the administrator.

Figure 7-29 Typical application of 802.1x authentication



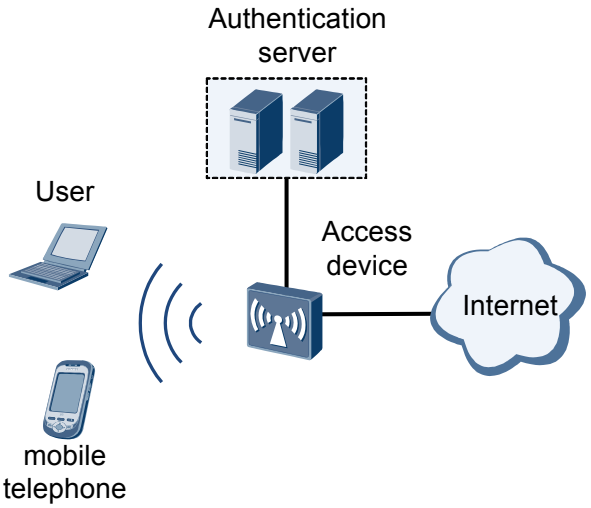
The user terminal is a PC with 802.1x client software installed on it. The user can use the 802.1x client software to initiate an authentication request to the access device. After exchanging

information with the user terminal, the access device sends the user information to the authentication server for authentication. If the authentication succeeds, the access device sets the interface connected to the user to the Up state and allows the user to access the network. If the authentication fails, the access device rejects the user's access request.

7.2.3.2 MAC Address Authentication

As shown in **Figure 7-30**, user terminals' network access needs to be controlled to ensure network security. Only authenticated users are allowed to access network resources authorized by the administrator.

Figure 7-30 Typical application of MAC address authentication

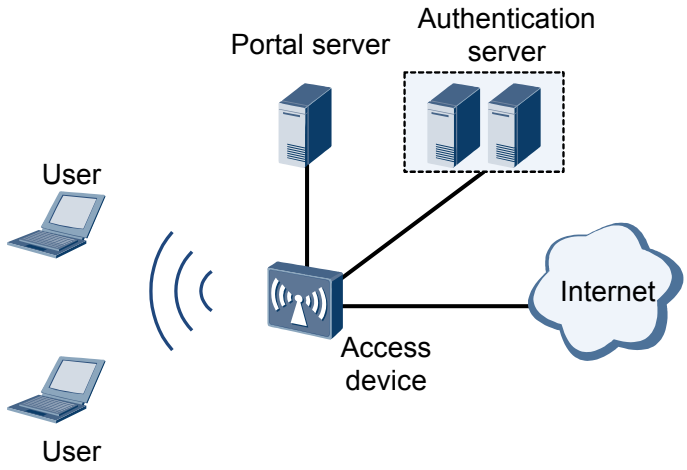


If you cannot install the 802.1x client on a terminal or you do not need to install the 802.1x client on a mobile phone, enable MAC address authentication on the interface connected to the terminal or mobile phone. After that, the access device uses the MAC address of the terminal as the user name and password, and reports the MAC address to the authentication server for authentication. If the authentication succeeds, the access device enables the interface connected to the terminal and allows the terminal to access the network. If the authentication fails, the access device rejects the terminal's access request.

7.2.3.3 Portal Authentication

As shown in **Figure 7-31**, user terminals' network access needs to be controlled to ensure network security. Only authenticated users are allowed to access network resources authorized by the administrator.

Figure 7-31 Typical application of Portal authentication



If the user only requires Portal authentication using a web browser, enable Portal authentication on the access device.

When an unauthenticated user accesses the Internet, the access device redirects the user to the Portal authentication website to start Portal authentication. If the authentication succeeds, the access device sets the interface connected to the user to the Up state and allows the user to access the network. If the authentication fails, the access device rejects the user's access request.

7.2.4 Default Configuration

This section provides the default NAC configuration. You can change the configuration as needed.

Table 7-22 describes the default configuration of 802.1x authentication.

Table 7-22 Default configuration of 802.1x authentication

Parameter	Default setting
802.1x authentication	Disabled
User authentication mode	CHAP authentication

Table 7-23 describes the default configuration of MAC address authentication.

Table 7-23 Default configuration of MAC address authentication

Parameter	Default setting
MAC address authentication	Disabled
User name format	User names and passwords in MAC address authentication are MAC addresses without hyphens.

Parameter	Default setting
User authentication domain	Default

Table 7-24 describes the default configuration of Portal authentication.

Table 7-24 Default configuration of Portal authentication

Parameter	Default setting
Portal authentication	Disabled
Portal protocol versions supported by the device	v2, v1
Number of the destination port that the device uses to send packets to the Portal server	50100
Number of the port that the device uses to listen to Portal protocol packets	2000

7.2.5 Configuring NAC

This chapter describes NAC configuration methods.

7.2.5.1 Configuring 802.1x Authentication

You can configure 802.1x authentication to implement interface-based network access control. This means you can authenticate and control access users connected to an access control device interface.

Prerequisites

802.1x only provides a user authentication solution. To implement this solution, the AAA function must also be configured. Therefore, the following tasks must be complete before you configure 802.1x authentication:

- Configuring the authentication domain and AAA scheme on the AAA client.
- Configuring the user name and password on the RADIUS or HWTACACS server if RADIUS or HWTACACS authentication is used.
- Configuring the user name and password manually on the network access device if local authentication is used.

For the configuration of AAA client, see **7.1 AAA Configuration** in the *Huawei Wireless Access Points Configuration Guide-Security*.

7.2.5.1.1 Enabling 802.1x Authentication

Context

The 802.1x configuration takes effect on an interface only after 802.1x authentication is enabled globally and on the interface.

If there are online users who log in through 802.1x authentication on the interface, disabling the 802.1x authentication is prohibited.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dot1x enable
```

Global 802.1x authentication is enabled.

By default, global 802.1x authentication is disabled.

Step 3 Enable 802.1x authentication on the interface in the system or interface view.

- In the system view:

1. Run:

   ```
   dot1x enable interface { interface-type interface-number1 [ to interface-number2 ] } &<1-10>
   ```

   802.1x authentication of the interface is enabled.

- In the interface view:

1. Run:

   ```
   interface interface-type interface-number
   ```

   The interface view is displayed.

2. Run:

   ```
   dot1x enable
   ```

   802.1x authentication of the interface is enabled.

By default, 802.1x authentication of an interface is disabled.

----End

7.2.5.1.2 (Optional) Setting the User Authentication Mode

Context

During 802.1x authentication, users exchange authentication information with the device using EAP packets. The device uses two modes to exchange authentication information with the RADIUS server.

- EAP termination: The device directly parses EAP packets, encapsulates user authentication information into a RADIUS packet, and sends the packet to the RADIUS server for authentication. EAP termination is classified into PAP or CHAP authentication.
  - PAP is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.
  - CHAP is a three-way handshake authentication protocol. It transmits only the user names (not passwords) in RADIUS packets. CHAP is more secure and reliable than PAP. If high security is required, CHAP is recommended.

  After the device directly parses EAP packets, user information in the EAP packets is authenticated by a local AAA module, or sent to a RADIUS or HWTACACS server.
- EAP relay (specified by **eap**): The device encapsulates EAP packets into RADIUS packets and sends the RADIUS packets to the RADIUS server. The device does not parse the received EAP packets but encapsulates them into RADIUS packets. This mechanism is called EAP over Radius (EAPoR).

The EAP relay mechanism requires that the RADIUS server be capable of parsing many EAP packets and carrying out authentication. Therefore, if the RADIUS server has high processing capabilities, the EAP relay is used. If the RADIUS server has low processing capabilities, EAP termination is recommended, and the device helps the RADIUS server to parse EAP packets.

NOTE

The EAP relay can be configured for 802.1x users only when RADIUS authentication is used.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 You can configure 802.1x authentication in the system view or interface view.

- In the system view:

1. Run the **dot1x authentication-method** { **chap** | **eap** | **pap** } command to set the authentication mode for 802.1x users.

- In the interface view:

1. Run the **interface** *interface-type interface-number* command to enter the interface view.
2. Run the **dot1x authentication-method** { **chap** | **eap** | **pap** } command to set the authentication mode for 802.1x users.

By default, the CHAP authentication mode is used.

----End

7.2.5.1.3 (Optional) Configuring Timers for 802.1x Authentication

Context

During 802.1x authentication, multiple timers implement systematic interactions between access users, access devices, and the authentication server. You can change the values of timers by running the **dot1x timer** command to adjust the interaction process. This command is necessary

in special network environments. It is recommended that you retain the default settings of the timers. You can configure the following types of timers in 802.1x authentication:

- Client timeout timer (**client-timeout**): After sending an EAP-Request/MD5-Challenge request packet to the client, the device starts this timer. If the client does not respond within the period set by the timer, the device retransmits the packet.
- Server timeout timer (**server-timeout**): The device starts this timer after sending a RADIUS Access-Request packet to the authentication server. If the authentication server does not respond within the period set by the timer, the device retransmits the authentication request packet to the authentication server.
- User name request timeout timer (**tx-period**): This timer defines two intervals. After sending an EAP-Request/Identity request packet to the client, the device starts the timer. If the client does not respond within the first interval set by the timer, the device retransmits the authentication request packet. The device multicasts the EAP-Request/Identity request packet at the second interval to detect the client that does not actively send the EAPOL-Start connection request packet for compatibility. The timer defines the interval for sending the multicast packet.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dot1x timer { client-timeout client-timeout-value | server-timeout server-timeout-value | tx-period tx-period-value }
```

The 802.1x timers are configured.

By default, **client-timeout** is set to 5 seconds; **server-timeout** is set to 30 seconds; **tx-period** is set to 30 seconds.

NOTE

The handshake timer, the client timeout timer, and the user name request timeout timer are enabled by default.

----End

7.2.5.1.4 (Optional) Setting the Maximum Number of Times for Sending Authentication Request Packets

Context

If a user does not respond in a specified period of time (set by the **dot1x timer client-timeout** *client-timeout-value* command or the **dot1x timer tx-period** *tx-period-value* command) after the device sends an authentication request packet, the device sends the authentication request packet again. If the device still fails to receive any response from the user when the number of sent authentication requests reaches the maximum, the device stops sending the authentication request packet. This prevents repeated sending of authentication request packets and conserves resources.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dot1x retry max-retry-value
```

The maximum number of times for sending authentication request packets is set.

By default, the maximum number of times for sending authentication request packets is 2.

----End

7.2.5.1.5 (Optional) Configuring the Quiet Function in 802.1x Authentication

Context

After the quiet function is enabled, when the number of times that a user fails 802.1x authentication reaches the maximum number allowed, the device quiets the user, and during the quiet period, the device discards the 802.1x authentication requests from the user. This prevents the impact of frequent user authentications on the system.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
dot1x quiet-period
```

The quiet function is enabled.

By default, the quiet function is disabled.

Step 3 (Optional) Run:

```
dot1x quiet-times fail-times
```

The maximum number of authentication failures within 60 seconds before the device quiets the 802.1x authentication user is configured.

By default, an 802.1x user enters the quiet state after three authentication failures within 60 seconds.

Step 4 (Optional) Run:

```
dot1x timer quiet-period quiet-period-value
```

The quiet timer is set.

By default, the quiet timer is 60 seconds.

----End

7.2.5.1.6 (Optional) Configuring Re-authentication for 802.1x Authentication Users

Context

If the administrator modifies user information on the authentication server, parameters such as the user access permission and authorization attribute are changed. If a user has passed 802.1x authentication, you must re-authenticate the user to ensure user validity.

After the user goes online, the device saves user authentication information. After re-authentication is enabled for 802.1x authentication users, the device sends the saved authentication information of the online user to the authentication server for re-authentication. If the user's authentication information does not change on the authentication server, the user is kept online. If the authentication information has been changed, the user is forced to go offline, and then re-authenticated according to the changed authentication information.

You can configure re-authentication for 802.1x authentication users using either of the following methods:

- Re-authenticate all online 802.1x authentication users on a specified interface periodically.
- Re-authenticate an online 802.1x authentication user once with a specified MAC address.

Procedure

- Configure periodic re-authentication for all online 802.1x authentication users on a specified interface.
  1. Run:
     system-view

     The system view is displayed.
  2. Enable periodic re-authentication for all online 802.1x authentication users on the specified interface in the system or interface view.
     - In the system view:

     a. Run:
     dot1x reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

     Periodic 802.1x re-authentication is enabled on the interface.

     - In the interface view:

     a. Run:
     interface *interface-type interface-number*

     The interface view is displayed.

     b. Run:
     dot1x reauthenticate

     Periodic 802.1x re-authentication is enabled on the interface.

     c. Run:
     quit

     The system view is displayed.

     By default, periodic 802.1x re-authentication is disabled on an interface.
  3. (Optional) Set the re-authentication interval for online 802.1x authentication users in the system or interface view.

- In the system view:

a. Run the **dot1x timer reauthenticate-period** *reauthenticate-period-value* command to set the re-authentication interval for online 802.1x authentication users.

- In the interface view:

a. Run the **interface** *interface-type interface-number* command to enter the interface view.

b. Run the **dot1x timer reauthenticate-period** *reauthenticate-period-value* command to set the re-authentication interval for online 802.1x authentication users.

By default, the device re-authenticates online 802.1x authentication users at the interval of 3600 seconds.

- Configure re-authentication for an online 802.1x authentication user with a specified MAC address.

1. Run:

```
system-view
```

The system view is displayed.

2. Run:

```
dot1x reauthenticate mac-address mac-address
```

Re-authentication is enabled for the online 802.1x authentication user with the specified MAC address.

By default, re-authentication for the online 802.1x authentication user with a specified MAC address is disabled.

----End

7.2.5.1.7 (Optional) Configuring Web Push

Context

After a user is successfully authenticated, the user is forcibly redirected to a web page when the user accesses web pages for the first time. In addition to pushing advertisement pages, the device can obtain user terminal information through the HTTP packets sent by the users, and apply the information to other services, such as BYOD. There are two ways to push web pages:

1. URL: pushes the URL corresponding to the web page.
2. URL template: pushes the URL template. A URL template must be created. The URL template contains the URL of the pushed web page and URL parameters.

Procedure

Step 1 Configure the URL template.

1. Run the **system-view** command to enter the system view.
2. Run the **url-template name** *template-name* command to create a URL template and enter the URL template view.

By default, no URL template exists on the device.

3. Run the **url** [**ssid** *ssid*] [**push-only**] *url-string* command to configure the redirection URL corresponding to the Portal server.
4. Run the **url-parameter** { **ac-ip** *ac-ip-value* | **ac-mac** *ac-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **redirect-url** *redirect-url-value* | **ssid** *ssid-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* } * command to set the parameters carried in the URL.

   By default, a URL does not carry parameters.
5. Run the **url-parameter mac-address format delimiter** *delimiter* { **normal** | **compact** } command to set the MAC address format in the URL.

   By default, the MAC address format in URL is XXXXXXXXXXXX.
6. Run the **parameter** { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } * command to set the characters in the URL.

   By default, the start character is ?, assignment character is =, and delimiter is &.
7. Run the **quit** command to return to the system view.

Step 2 Configure the Web push function.

1. Run the **aaa** command to enter the AAA view.
2. Run the **domain** *domain-name* command to create an AAA domain and enter the AAA domain view.

   The device has two default domains: default and default_admin. The default domain is used by common access users and the default_admin domain is used by administrators.
3. Run the **force-push** { **url-template** *template-name* | **url** *url-address* } command to enable the forcible URL template or URL push function.

----End

7.2.5.1.8 (Optional) Configuring the User Group Function

Context

In NAC applications, there are many access users, but user types are limited. You can create user groups on the device and associate each user group to an ACL. In this way, users in the same group share rules in the ACL.

After creating user groups, you can set priorities and VLANs for the user groups, so that users in different user groups have different priorities and network access rights. The administrator can then flexibly manage users.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configuring a QoS profile

1. Run:

   ```
   qos-profile
   ```

A QoS profile is created and the QoS profile view is displayed.

2. Run:
   remark { **inbound** | **outbound** } **8021p** *8021p-value*

   The action of re-marking 802.1p priorities of VLAN packets is configured in the QoS profile.

   By default, the action of re-marking 802.1p priorities of VLAN packets is not configured in a QoS profile.

3. Run:
   remark { **inbound** | **outbound** } **dscp** *8021p-value*

   The action of re-marking DSCP priorities of IP packets is configured in the QoS profile.

   By default, the action of re-marking DSCP priorities of IP packets is not configured in a QoS profile.

4. Run:
   remark local-precedence { *local-precedence-name* | *local-precedence-value* }

   The action of re-marking internal priorities of packets is configured in the QoS profile.

   By default, the action of re-marking internal priorities of packets is not configured in a QoS profile.

5. Run:
   car { **inbound** | **outbound** } **cir** *cir-value* [**pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]

   Traffic policing parameters are configured in the QoS profile.

   By default, no traffic policing parameter is configured in a QoS profile.

6. Run:
   quit

   Return to the system view.

Step 3 Run:
user-group *group-name*

A user group is created and the user group view is displayed.

Step 4 Run:
acl-id *acl-number*

An ACL is bound to the user group.

By default, no ACL is bound to a user group.

NOTE

Before running this command, ensure that the ACL has been created using the **acl (system view)** or **acl name** command. The ACL number ranges from 3000 to 3031.

The bound ACL applies only to upstream packets of an AP but not downstream packets sent from the AP to the STAs.

Step 5 Run:
user-vlan *vlan-id*

The user group VLAN is configured.

By default, no user group VLAN is configured.

NOTE

Before running this command, ensure that the VLAN has been created using the **vlan** command.

Step 6 Run:

```
qos-profile name
```

The QoS profile is bound to the user group in the user group view.

By default, no QoS profile is bound to a user group.

Step 7 Run:

```
user-isolated { inter-group | inner-group }*
```

Inter-group and intra-group user isolation are configured.

By default, inter-group or intra-group isolation is not configured in a user group.

----End

7.2.5.1.9 Checking the Configuration

Context

You can run the commands to check the configured parameters after completing the 802.1x authentication configuration.

Procedure

- Run the **display dot1x** [**statistics**] [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>] command to check the 802.1x authentication configuration.
- Run the **display user-group** [*group-name*] command to check the user group configuration.
- Run the **display access-user user-group** *group-name* command to check information about online users in a user group.

----End

7.2.5.2 Configuring MAC Address Authentication

MAC address authentication controls a user's network access right based on the user's access interface and MAC address. The user does not need to install any client software. The user device MAC address is used as the user name and password. When detecting the user's MAC address the first time, the network access device starts authenticating the user.

Prerequisites

MAC address authentication only provides a user authentication solution. To implement this solution, the AAA function must also be configured. Therefore, the following tasks must be complete before you configure MAC address authentication:

- Configuring the authentication domain and AAA scheme on the AAA client.

- Configuring the user name and password on the RADIUS or HWTACACS server if RADIUS or HWTACACS authentication is used.
- Configuring the user name and password manually on the network access device if local authentication is used.

For the configuration of AAA client, see **7.1 AAA Configuration** in the *Huawei Wireless Access Points Configuration Guide-Security*.

7.2.5.2.1 Enabling MAC Address Authentication

Context

The MAC address authentication configuration takes effect on an interface only after MAC address authentication is enabled globally and on the interface.

After MAC address authentication is enabled, if there are online users who log in through MAC address authentication on the interface, disabling MAC address authentication is prohibited.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
mac-authen
```

Global MAC address authentication is enabled.

By default, global MAC address authentication is disabled.

Step 3 Enable MAC address authentication on an interface in the system or interface view.

In the system view:

1. Run:

   ```
   mac-authen interface { interface-type interface-number1 [ to interface-number2 ] } &<1-10>
   ```

   MAC address authentication is enabled on the interface.

In the interface view:

1. Run:

   ```
   interface interface-type interface-number
   ```

   The interface view is displayed.

2. Run:

   ```
   mac-authen
   ```

   MAC address authentication is enabled on the interface.

By default, MAC address authentication is disabled on an interface.

----End

7.2.5.2.2 (Optional) Configuring the User Name Format

Context

MAC address authentication uses the following user name formats:

- MAC address: When the MAC address is used as the user name for MAC address authentication, the password can be the MAC address or a self-defined character string.
- Fixed user name: Regardless of users' MAC addresses, all users have a fixed name and password specified by the administrator as an identity for authentication. Many users may be authenticated on the same interface. In this case, all users requiring MAC address authentication on the interface use the same fixed user name, and the server must only configure one user account to authenticate all users. This is applicable to a network environment with reliable access clients.

NOTE

If configured in the system view, the user name format is valid for commands on all interfaces; if configured in the interface view, the user name format is valid for commands on this interface only. If configured in the interface view and system view at the same time, the user name format configured in the interface view has higher priority.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure the user name format in the system or interface view.

1. Run:

   ```
   interface interface-type interface-number
   ```

   The interface view is displayed; or configuration is directly performed in the system view.

2. Run:

   ```
   mac-authen username { fixed username [ password cipher password ] |
   macaddress [ format { with-hyphen | without-hyphen } [ password cipher
   password ] ]  }
   ```

   The user name format is set for MAC address authentication.

   By default, the MAC address without hyphens (-) is used as the user name and password for MAC address authentication.

----End

7.2.5.2.3 (Optional) Configuring the User Authentication Domain

Context

When the MAC address or the fixed user name without a domain name is used as the user name in MAC address authentication, the user is authenticated in a default domain if the administrator does not configure an authentication domain. In this case, many users are authenticated in the default domain, making the authentication scheme inflexible.

NOTE

- When the fixed user name is used for MAC address authentication and the authentication domain is specified in the user name, the user is authenticated in the specified authentication domain.
- Before configuring an authentication domain for the MAC address authentication user, ensure that the authentication domain has been created.

Procedure

- Run:
  ```
  system-view
  ```
  The system view is displayed.
- Run:
  ```
  mac-authen domain isp-name [ mac-address mac-address mask mask ]
  ```
  The authentication domain is configured for the MAC address authentication user.

  By default, MAC address authentication uses the default domain.

----End

7.2.5.2.4 (Optional) Configuring Timers of MAC Address Authentication

Context

During MAC address authentication, multiple timers implement systematic interactions between access users or devices and the authentication server. You can configure the following types of timers in MAC address authentication:

- Quiet timer (**quiet-period**): The device must enter a quiet period after the user fails to be authenticated. During the quiet period, the device does not process authentication requests from the user.
- Server timeout timer (**server-timeout**): The device starts this timer after sending a RADIUS Access-Request packet to the authentication server. If the authentication server does not respond within the period set by the timer, the device retransmits the authentication request packet to the authentication server.

Procedure

Step 1 Run:
```
system-view
```
The system view is displayed.

Step 2 Run:
```
mac-authen timer { quiet-period quiet-value | server-timeout server-timeout-value }
```
The timer parameters are set for MAC address authentication.

By default, **quiet-period** is set to 60 seconds, and **server-timeout** is set to 30 seconds.

NOTE

Timers for setting **quiet-period**, and **server-timeout** are enabled by default.

----End

7.2.5.2.5 (Optional) Configuring Re-authentication for MAC Address Authentication Users

Context

If the administrator modifies user information on the authentication server, parameters such as the user access permission and authorization attribute are changed. If a user has passed MAC address authentication, you must re-authenticate the user to ensure user validity.

After the user goes online, the device saves user authentication information. After re-authentication is enabled for MAC address authentication users, the device sends the saved authentication information of the online user to the authentication server for re-authentication. If the user's authentication information does not change on the authentication server, the user is kept online. If the authentication information has been changed, the user is forced to go offline, and then re-authenticated according to the changed authentication information.

You can configure re-authentication for MAC address authentication users using either of the following methods:

- Re-authenticate all online MAC address authentication users on a specified interface at an interval.
- Re-authenticate the online user once with a specified MAC address.

Procedure

- Re-authenticate all online MAC address authentication users on a specified interface at an interval.
  1. Run:
     system-view

     The system view is displayed.
  2. Enable periodic re-authentication for all online MAC address authentication users on the specified interface in the system or interface view.
     - In the system view:
       a. Run:
          mac-authen reauthenticate interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

          Periodic re-authentication is enabled for all online MAC address authentication users on the specified interface.
     - In the interface view:
       a. Run:
          interface *interface-type interface-number*

          The interface view is displayed.
       b. Run:
          mac-authen reauthenticate

          Periodic re-authentication is enabled for all online MAC address authentication users on the specified interface.
       c. Run:
          quit

          Return to the system view.

By default, periodic re-authentication is enabled for all online MAC address authentication users on the specified interface.

3. (Optional) Set the re-authentication interval for online MAC address authentication users in the system or interface view.
   - In the system view:
     a. Run the **mac-authen timer reauthenticate-period** *reauthenticate-period-value* command to set the re-authentication interval for online MAC address authentication users.
   - In the interface view:
     a. Run the **interface** *interface-type interface-number* command to enter the interface view.
     b. Run the **mac-authen timer reauthenticate-period** *reauthenticate-period-value* command to set the re-authentication interval for online MAC address authentication users.

   By default, the device re-authenticates online MAC address authentication users at the interval of 1800 seconds.

- Configure re-authentication for an online MAC address authentication user with a specified MAC address.
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     mac-authen reauthenticate mac-address mac-address
     ```
     Re-authentication is enabled for the online MAC address authentication user with the specified MAC address.

     By default, re-authentication for an online MAC address authentication user with a specified MAC address is disabled.

----End

7.2.5.2.6 (Optional) Configuring Web Push

Context

After a user is successfully authenticated, the user is forcibly redirected to a web page when the user accesses web pages for the first time. In addition to pushing advertisement pages, the device can obtain user terminal information through the HTTP packets sent by the users, and apply the information to other services, such as BYOD. There are two ways to push web pages:

1. URL: pushes the URL corresponding to the web page.
2. URL template: pushes the URL template. A URL template must be created. The URL template contains the URL of the pushed web page and URL parameters.

Procedure

Step 1 Configure the URL template.

1. Run the **system-view** command to enter the system view.
2. Run the **url-template name** *template-name* command to create a URL template and enter the URL template view.

   By default, no URL template exists on the device.
3. Run the **url** [**ssid** *ssid*] [**push-only**] *url-string* command to configure the redirection URL corresponding to the Portal server.
4. Run the **url-parameter** { **ac-ip** *ac-ip-value* | **ac-mac** *ac-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **redirect-url** *redirect-url-value* | **ssid** *ssid-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* } * command to set the parameters carried in the URL.

   By default, a URL does not carry parameters.
5. Run the **url-parameter mac-address format delimiter** *delimiter* { **normal** | **compact** } command to set the MAC address format in the URL.

   By default, the MAC address format in URL is XXXXXXXXXXXX.
6. Run the **parameter** { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } * command to set the characters in the URL.

   By default, the start character is ?, assignment character is =, and delimiter is &.
7. Run the **quit** command to return to the system view.

Step 2 Configure the Web push function.

1. Run the **aaa** command to enter the AAA view.
2. Run the **domain** *domain-name* command to create an AAA domain and enter the AAA domain view.

   The device has two default domains: default and default_admin. The default domain is used by common access users and the default_admin domain is used by administrators.
3. Run the **force-push** { **url-template** *template-name* | **url** *url-address* } command to enable the forcible URL template or URL push function.

----End

7.2.5.2.7 (Optional) Configuring the User Group Function

Context

In NAC applications, there are many access users, but user types are limited. You can create user groups on the device and associate each user group to an ACL. In this way, users in the same group share rules in the ACL.

After creating user groups, you can set priorities and VLANs for the user groups, so that users in different user groups have different priorities and network access rights. The administrator can then flexibly manage users.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configuring a QoS profile

1. Run:
   qos-profile

   A QoS profile is created and the QoS profile view is displayed.
2. Run:
   remark { **inbound** | **outbound** } **8021p** *8021p-value*

   The action of re-marking 802.1p priorities of VLAN packets is configured in the QoS profile.

   By default, the action of re-marking 802.1p priorities of VLAN packets is not configured in a QoS profile.
3. Run:
   remark { **inbound** | **outbound** } **dscp** *8021p-value*

   The action of re-marking DSCP priorities of IP packets is configured in the QoS profile.

   By default, the action of re-marking DSCP priorities of IP packets is not configured in a QoS profile.
4. Run:
   remark local-precedence { *local-precedence-name* | *local-precedence-value* }

   The action of re-marking internal priorities of packets is configured in the QoS profile.

   By default, the action of re-marking internal priorities of packets is not configured in a QoS profile.
5. Run:
   car { **inbound** | **outbound** } **cir** *cir-value* [**pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]

   Traffic policing parameters are configured in the QoS profile.

   By default, no traffic policing parameter is configured in a QoS profile.
6. Run:
   quit

   Return to the system view.

Step 3 Run:
user-group *group-name*

A user group is created and the user group view is displayed.

Step 4 Run:
acl-id *acl-number*

An ACL is bound to the user group.

By default, no ACL is bound to a user group.

NOTE

Before running this command, ensure that the ACL has been created using the **acl (system view)** or **acl name** command. The ACL number ranges from 3000 to 3031.

The bound ACL applies only to upstream packets of an AP but not downstream packets sent from the AP to the STAs.

Step 5 Run:

user-vlan *vlan-id*

The user group VLAN is configured.

By default, no user group VLAN is configured.

NOTE

Before running this command, ensure that the VLAN has been created using the **vlan** command.

Step 6 Run:

qos-profile *name*

The QoS profile is bound to the user group in the user group view.

By default, no QoS profile is bound to a user group.

Step 7 Run:

user-isolated { **inter-group** | **inner-group** }*

Inter-group and intra-group user isolation are configured.

By default, inter-group or intra-group isolation is not configured in a user group.

----End

7.2.5.2.8 Checking the Configuration

Context

You can run the commands to check the configured parameters after completing the MAC address authentication configuration.

Procedure

- Run the **display mac-authen** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>] command to check the configuration of MAC address authentication.
- Run the **display user-group** [*group-name*] command to check the user group configuration.
- Run the **display access-user user-group** *group-name* command to check information about online users in a user group.

----End

7.2.5.3 Configuring Portal Authentication

In Portal authentication, users do not need a specific client. The Portal server provides users with free portal services and a Portal authentication page.

Prerequisites

Portal authentication only provides a user authentication solution. To implement this solution, the AAA function must also be configured. Therefore, the following tasks must be complete before you configure Portal authentication:

- Configuring the authentication domain and AAA scheme on the AAA client.
- Configuring the user name and password on the RADIUS or HWTACACS server if RADIUS or HWTACACS authentication is used.
- Configuring the user name and password manually on the network access device if local authentication is used.

For the configuration of AAA client, see **7.1 AAA Configuration** in the *Huawei Wireless Access Points Configuration Guide-Security*.

7.2.5.3.1 Configuring Portal Server Parameters

Context

During Portal authentication, you must configure parameters for the Portal server (for example, the IP address for the Portal server) to ensure smooth communication between the device and the Portal server.

The Portal server is classified as either the external Portal server or the built-in Portal server. The external Portal server has independent hardware, while the built-in Portal server is an entity embedded in the access device (that is, functions of the Portal server are implemented by the access device).

Procedure

- Configuring parameters for the external Portal server (binding URL)
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     web-auth-server *server-name*

     A Portal server template is created and the Portal server template view is displayed.

     By default, no Portal server template is created.
  3. Run:
     server-ip *server-ip-address* &<1-10>

     An IP address is configured for the Portal server.

     By default, no IP address is configured for the Portal server.

     NOTE

     The IP address for the Portal server is the IP address for the external Portal server.
  4. Run:
     url *url-string*

     A URL is configured for the portal server.

By default, a Portal server does not have a URL.

5. Run:
   shared-key cipher *key-string*

   The shared key that the device uses to exchange information with the Portal server is configured.

   By default, no shared key is configured.

- Setting parameters of the URL corresponding to an external Portal server (binding URL template)
  1. Configure the URL template.
     a. Run the **system-view** command to enter the system view.
     b. Run the **url-template name** *template-name* command to create a URL template and enter the URL template view.

        By default, no URL template exists on the device.
     c. Run the **url** [**ssid** *ssid*] [**redirect-only**] *url-string* command to configure the redirection URL corresponding to the Portal server.

        By default, no redirection URL is configured for a Portal server.
     d. Run the **url-parameter** { **ac-ip** *ac-ip-value* | **ac-mac** *ac-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **redirect-url** *redirect-url-value* | **ssid** *ssid-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* } * command to set the parameters carried in the URL.

        By default, a URL does not carry parameters.
     e. Run the **url-parameter mac-address format delimiter** *delimiter* { **normal** | **compact** } command to set the MAC address format in the URL.

        By default, the MAC address format in URL is XXXXXXXXXXXX.
     f. Run the **parameter** { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } * command to set the characters in the URL.

        By default, the start character is ?, assignment character is =, and delimiter is &.
     g. Run the **quit** command to return to the system view.
  2. Set parameters for the external Portal server.
     a. Run the **web-auth-server** *server-name* command to create a Portal server template and enter the Portal server template view.

        By default, no Portal server template is created.
     b. Run the **server-ip** *server-ip-address* &<1-10> command to set the IP address corresponding to the Portal server.

        By default, no IP address is configured for the Portal server.
     c. Run the **url-template** *url-template* command to bind a URL template to the Portal server template.

        By default, no URL template is bound to a Portal server template.
- Configuring parameters for the built-in Portal server
  1. Run:
     system-view

The system view is displayed.

2. Run:

   portal local-server ip *ip-address*

   The IP address is configured for the built-in Portal server.

   By default, no IP address is configured for a built-in Portal server.

   NOTE

   The IP address for the built-in Portal server is an IP address of a Layer 3 interface that can be reached by a route between the device and the client.

3. (Optional) Run:

   portal local-server url *url-string*

   The URL address is configured for the built-in Portal server.

   By default, no URL address is configured for a built-in Portal server.

----End

7.2.5.3.2 Enabling Portal Authentication

Context

The device can communicate with the Portal server after the parameters of the Portal server are configured. To enable Portal authentication for access users, you must enable Portal authentication of the device.

To enable Portal authentication on an external Portal server, you must only bind the configured Portal server template to a VLANIF interface. To enable Portal authentication on a built-in Portal server, you must enable the built-in Portal server and enable Portal authentication on a Layer 2 interface of the device.

Procedure

- Enable Portal authentication on the device if the authentication server is an external Portal server.

  1. Run:

     system-view

     The system view is displayed.

  2. Run:

     interface *interface-type interface-number*

     The interface view is displayed.

  3. Run:

     web-auth-server *server-name* { **direct** | **layer3** }

     The Portal server template is bound to the interface.

     By default, no Portal server template is bound to an interface.

  4. (Optional) Run:

     quit

The system view is displayed.

5. (Optional) Run:
   interface wlan-bss *wlan-bss-number*

   A WLAN-BSS interface is created, and the WLAN-BSS interface view is displayed.
6. (Optional) Run:
   web-authentication first-mac

   The function that prefers MAC addresses as accounts for Portal authentication is enabled.

   By default, MAC addresses are not preferred as accounts for Portal authentication.

- Enable Portal authentication on the device if the authentication server is a built-in Portal server.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     portal local-server https ssl-policy *policy-name* [**port** *port-num*]

     The built-in Portal server is enabled on the device.

     By default, the built-in Portal server is disabled on the device.

     NOTE

     The SSL policy must be configured and the digital certificate must be loaded.
  3. Enable Portal authentication on the interface in the system or interface view.
     - In the system view:
       - **portal local-server enable interface** *interface-type interface-number1* [**to** *interface-number2*] &<1-10>

         Portal authentication is enabled on the interface.
     - In the interface view:
       a. Run:
          interface *interface-type interface-number*

          The interface view is displayed.
       b. Run:
          portal local-server enable

          Portal authentication is enabled on the interface.

     By default, Portal authentication is disabled on an interface.
  4. (Optional) Customize built-in Portal server login page.
     - Run:

       The advertisement image file is loaded to the built-in Portal server login page.

       By default, no advertisement image file is loaded to the built-in Portal server login page.
     - Run:
       portal local-server page-text load *string*

       The advertisement page file is loaded to the built-in Portal server.

By default, no advertisement page file is loaded to the built-in Portal server.

- Run:
  portal local-server policy-text load *string*

  The disclaimer page file is loaded to the built-in Portal server.

  By default, no disclaimer page file is loaded to the built-in Portal server.

5. (Optional) Run:
   portal local-server redirect-url enable

   The original page that the user requests to access is displayed when the Portal authentication is successful.

   By default, the original page that the user requests to access is not displayed.

----End

7.2.5.3.3 (Optional) Configuring Parameters for Information Exchange with the Portal server

Context

In Portal authentication network deployment, if the Portal server is an external Portal server, you can configure parameters for information exchange between the device and the Portal server to improve communication security.

NOTE

This function applies only to external Portal servers.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
web-auth-server version v2 [**v1**]

Portal protocol versions supported by the device are configured.

By default, the device uses Portal of v1 and v2.

NOTE

To ensure smooth communication, use the default setting so that the device uses both versions.

Step 3 Run:
web-auth-server listening-port *port-number*

The port number through which the device listens to Portal protocol packets is set.

By default, the device listens to the Portal protocol packets through port 2000.

Step 4 Run:
web-auth-server reply-message

The device is enabled to transparently transmit the authentication responses sent by the authentication server to the Portal server.

By default, the device transparently transmits the authentication responses sent by the authentication server to the Portal server.

Step 5 Run:

```
web-auth-server server-name
```

The Portal server template view is displayed.

Step 6 Run:

```
source-ip ip-address
```

The source IP address for communication with a Portal server is configured.

By default, no source IP address is configured on the device.

Step 7 Run:

```
port port-number [ all ]
```

The destination port number through which the device sends packets to the Portal server is set.

By default, port 50100 is used as the destination port when the device sends packets to the Portal server.

----End

7.2.5.3.4 (Optional) Setting Access Control Parameters for Portal Authentication Users

Context

During deployment of the Portal authentication network, you can set access control parameters for Portal authentication users to flexibly control the user access. For example, you can set authentication free rules for Portal authentication users so that the users can access specified network resources without being authenticated or when the users fail authentication. You can configure the source authentication subnet to allow the device to authenticate only users in the source authentication subnet, while users in other subnets cannot pass Portal authentication.

Procedure

- Set access control parameters for Portal authentication users when an external Portal server is used.
  1. Run:

     ```
     system-view
     ```

     The system view is displayed.
  2. Run:

     ```
     portal free-rule rule-id { destination { any | ip { ip-address mask { mask-length | ip-mask } [ tcp destination-port port | udp destination-port port ] | any } } | source { any | { interface interface-type interface-number | ip { ip-address mask { mask-length | ip-mask } | any } | vlan vlan-id } * } } *
     ```

     The Portal authentication-free rule is set for users.

     By default, no Portal authentication-free rule is set for users.
  3. Run:

     ```
     portal max-user user-number
     ```

The maximum number of concurrent Portal users is set.

By default, the number of Portal authentication users is the maximum number of Portal authentication users supported by the device.

4. Run:
   interface vlanif *vlan-id*

   The Vlanif interface view is displayed.
5. Run:
   portal auth-network *network-address* { *mask-length* | *mask-address* }

   The source subnet is set for Portal authentication.

   By default, the source authentication subnet is 0.0.0.0/0, indicating that users in all subnets must pass Portal authentication.

   NOTE

   The command takes effect for only Layer 3 Portal authentication. In Layer 2 Portal authentication, users on all subnets must be authenticated.
6. Run:
   portal domain *domain-name*

   A forcible Portal authentication domain name is set.

   By default, no forcible Portal authentication domain name is set.

- Set access control parameters for Portal authentication users when a built-in Portal server is used.
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     portal local-server authentication-method { **chap** | **pap** }

     The authentication mode of the built-in Portal server is set.

     By default, the built-in Portal server uses CHAP to authenticate Portal users.

----End

7.2.5.3.5 (Optional) Configuring the Detection Function for Portal Authentication

Context

In practical networking applications of Portal authentication, if communication is interrupted due to a network failure between the device and the Portal server or because the Portal server fails, new Portal authentication users cannot go online, and online Portal users cannot go offline normally.

The Portal detection function allows the device to report failures using logs and traps when the network fails or the Portal server cannot work properly.

NOTE

This function applies only to external Portal servers.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
web-auth-server server-name
```

The Portal server template view is displayed.

Step 3 Run:

```
server-detect { interval interval-period | max-times times | critical-num critical-num | action { log | trap } * } *
```

The detection function of the Portal server is enabled.

By default, the detection function of the Portal server is disabled.

----End

7.2.5.3.6 (Optional) Configuring User Information Synchronization

Context

If communication is interrupted because the network between the device and Portal server is disconnected or the Portal server is faulty, online Portal authentication users cannot go offline. Therefore, user information on the device and on the Portal server may be inconsistent and accounting may be inaccurate.

The user information synchronization function ensures that user information on the Portal server is the same as that on the device, ensuring accurate accounting.

NOTE

This function is valid for only external Portal servers.

For Layer 3 Portal authentication, the device currently can synchronize user information with the Huawei-Symantec TSM Portal server. When the device is connected to other Portal servers, user information may fail to be synchronized and users cannot go offline in real time. In this case, you can run the **cut access-user** command or use the NMS or RADIUS DM to force users to go offline.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
web-auth-server server-name
```

The Portal server template view is displayed.

Step 3 Run:

```
user-sync [ interval interval-period | max-times times ] *
```

User information synchronization is enabled.

By default, user information synchronization is disabled.

----End

7.2.5.3.7 (Optional) Configuring the Quiet Timer

Context

After the quiet timer is enabled, if the number of Portal authentication failures exceeds the specified value within 60s, the device keeps the Portal authentication user in quiet state for a period of time. During the quiet period, the device discards Portal authentication requests from the user. This prevents the impact of frequent authentications on the system.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
portal quiet-period
```

The quiet timer is enabled.

By default, the quiet timer is disabled.

Step 3 Run:

```
portal quiet-times fail-times
```

The maximum number of authentication failures within 60s before a Portal authentication user enters the quiet state is set.

By default, the device allows a maximum of three authentication failures within 60s before a Portal authentication user is kept in quiet state.

Step 4 Run:

```
portal timer quiet-period quiet-period-value
```

The quiet period for Portal authentication is set.

By default, the quiet period for Portal authentication is 60s.

----End

7.2.5.3.8 (Optional) Configuring Web Push

Context

After a user is successfully authenticated, the user is forcibly redirected to a web page when the user accesses web pages for the first time. In addition to pushing advertisement pages, the device can obtain user terminal information through the HTTP packets sent by the users, and apply the information to other services, such as BYOD. There are two ways to push web pages:

1. URL: pushes the URL corresponding to the web page.

2. URL template: pushes the URL template. A URL template must be created. The URL template contains the URL of the pushed web page and URL parameters.

Procedure

Step 1 Configure the URL template.

1. Run the **system-view** command to enter the system view.
2. Run the **url-template name** *template-name* command to create a URL template and enter the URL template view.

   By default, no URL template exists on the device.
3. Run the **url** [**ssid** *ssid*] [**push-only**] *url-string* command to configure the redirection URL corresponding to the Portal server.
4. Run the **url-parameter** { **ac-ip** *ac-ip-value* | **ac-mac** *ac-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **redirect-url** *redirect-url-value* | **ssid** *ssid-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* } * command to set the parameters carried in the URL.

   By default, a URL does not carry parameters.
5. Run the **url-parameter mac-address format delimiter** *delimiter* { **normal** | **compact** } command to set the MAC address format in the URL.

   By default, the MAC address format in URL is XXXXXXXXXXXX.
6. Run the **parameter** { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } * command to set the characters in the URL.

   By default, the start character is ?, assignment character is =, and delimiter is &.
7. Run the **quit** command to return to the system view.

Step 2 Configure the Web push function.

1. Run the **aaa** command to enter the AAA view.
2. Run the **domain** *domain-name* command to create an AAA domain and enter the AAA domain view.

   The device has two default domains: default and default_admin. The default domain is used by common access users and the default_admin domain is used by administrators.
3. Run the **force-push** { **url-template** *template-name* | **url** *url-address* } command to enable the forcible URL template or URL push function.

----End

7.2.5.3.9 (Optional) Configuring the User Group Function

Context

In NAC applications, there are many access users, but user types are limited. You can create user groups on the device and associate each user group to an ACL. In this way, users in the same group share rules in the ACL.

After creating user groups, you can set priorities and VLANs for the user groups, so that users in different user groups have different priorities and network access rights. The administrator can then flexibly manage users.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configuring a QoS profile

1. Run:

   ```
   qos-profile
   ```

   A QoS profile is created and the QoS profile view is displayed.

2. Run:

   ```
   remark { inbound | outbound } 8021p 8021p-value
   ```

   The action of re-marking 802.1p priorities of VLAN packets is configured in the QoS profile.

   By default, the action of re-marking 802.1p priorities of VLAN packets is not configured in a QoS profile.

3. Run:

   ```
   remark { inbound | outbound } dscp 8021p-value
   ```

   The action of re-marking DSCP priorities of IP packets is configured in the QoS profile.

   By default, the action of re-marking DSCP priorities of IP packets is not configured in a QoS profile.

4. Run:

   ```
   remark local-precedence { local-precedence-name | local-precedence-value }
   ```

   The action of re-marking internal priorities of packets is configured in the QoS profile.

   By default, the action of re-marking internal priorities of packets is not configured in a QoS profile.

5. Run:

   ```
   car { inbound | outbound } cir cir-value [ pir pir-value [ cbs cbs-value pbs pbs-value ] ]
   ```

   Traffic policing parameters are configured in the QoS profile.

   By default, no traffic policing parameter is configured in a QoS profile.

6. Run:

   ```
   quit
   ```

   Return to the system view.

Step 3 Run:

```
user-group group-name
```

A user group is created and the user group view is displayed.

Step 4 Run:

```
acl-id acl-number
```

An ACL is bound to the user group.

By default, no ACL is bound to a user group.

NOTE

Before running this command, ensure that the ACL has been created using the **acl (system view)** or **acl name** command. The ACL number ranges from 3000 to 3031.

The bound ACL applies only to upstream packets of an AP but not downstream packets sent from the AP to the STAs.

Step 5 Run:

```
qos-profile name
```

The QoS profile is bound to the user group in the user group view.

By default, no QoS profile is bound to a user group.

Step 6 Run:

```
user-isolated { inter-group | inner-group }*
```

Inter-group and intra-group user isolation are configured.

By default, inter-group or intra-group isolation is not configured in a user group.

----End

7.2.5.3.10 Checking the Configuration

Context

You can run the commands to check the configured parameters after completing the Portal authentication configuration.

Procedure

- When an external Portal server is used, run the following commands to check the configuration.
  - Run the **display portal** [**interface vlanif** *vlan-id*] command to check the Portal authentication configuration on the VLANIF interface.
  - Run the **display web-auth-server configuration** command to check the configuration of the Portal authentication server.
  - Run the **display server-detect state** [**web-auth-server** *server-name*] command to check the status of a Portal server.
  - Run the **display user-group** [*group-name*] command to check the user group configuration.
  - Run the **display access-user user-group** *group-name* command to check summary information about online users in a user group.
  - Run the **display portal quiet-user** { **all** | **user-ip** *ip-address* | **server-ip** *ip-address* } command to check information about Portal authentication users in quiet state.
- When a built-in Portal server is used, run the following commands to check the configuration.
  - Run the **display portal local-server** command to check the configuration of a built-in Portal server.
  - Run the **display portal local-server connect** [**user-ip** *ip-address*] command to check the connection status of Portal authentication users on the built-in Portal server.

- Run the **display portal quiet-user** { **all** | **user-ip** *ip-address* | **server-ip** *ip-address* } command to check information about Portal authentication users in quiet state.

----End

7.2.6 Maintaining NAC

This section describes how to clear statistics for 802.1x authentication and MAC address authentication.

7.2.6.1 Clearing 802.1x Authentication Statistics

Context

NOTICE

Statistics cannot be restored after being cleared. Exercise caution when you run the following command.

Procedure

- Run the **reset dot1x statistics** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>] command in the user view to clear the statistics for 802.1x authentication.

----End

7.2.6.2 Clearing MAC Address Authentication Statistics

Context

NOTICE

Statistics cannot be restored after being cleared. Exercise caution when you run the following command.

Procedure

- Run the **reset mac-authen statistics** [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>] command in the user view to clear the statistics for MAC address authentication.

----End

7.2.7 Configuration Examples

This section provides several NAC configuration examples, including network requirements, configuration roadmap, and configuration procedure.

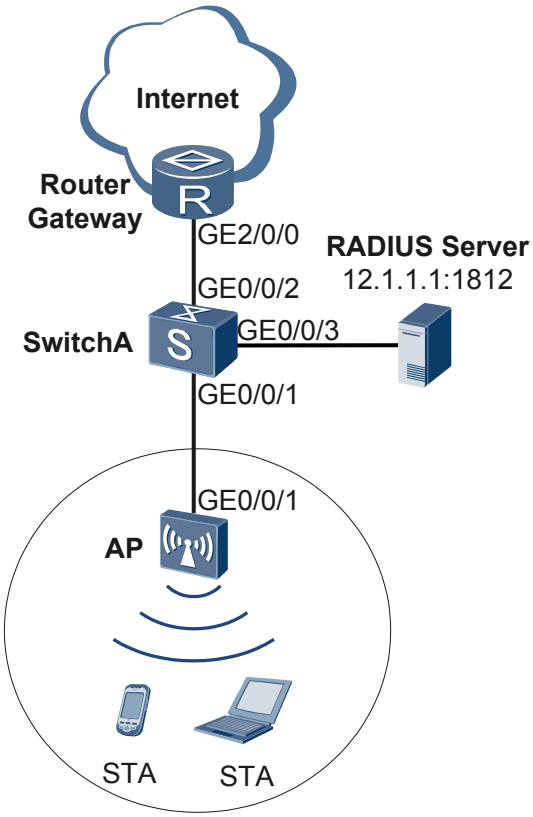
7.2.7.1 Example for Configuring 802.1x Authentication

Networking Requirements

As shown in **Figure 7-32**, the enterprise's AP connects to the egress gateway (Router) and RADIUS server. The WLAN with the SSID of **test** is available for employees to access network resources. The gateway also functions as a DHCP server to provide IP addresses on the 10.10.10.0/24 network segment for STAs. The AP controls and manages STAs.

Because the WLAN is open to users, there are potential security risks to enterprise information if no security policy is configured for the WLAN. The enterprise requires high information security, so a WPA security policy using 802.1x authentication and CCMP encryption can be configured. The RADIUS server authenticates STA identities. The AP must be configured to function as an EAP relay, so the AC supports 802.1x authentication.

Figure 7-32 Networking diagram for configuring a WPA security policy



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.

2. Configure a RADIUS server template, apply it to an AAA domain, and enable 802.1x authentication on the AP.
3. Configure a WPA security policy using 802.1x authentication and CCMP encryption in a security profile to ensure data security.

NOTE

- Ensure that the RADIUS server IP address, port number, and shared key are correct. When the AP functions as an EAP relay, ensure that the RADIUS server supports the EAP protocol. Otherwise, the RADIUS server cannot process 802.1x authentication requests.

Table 7-25 Data plan

Configuration Item	Data
Service VLAN	VLAN 101
Service set	SSID: test
SwitchA VLAN	VLAN 101, VLAN 102, VLAN 103
DHCP server	IP addresses that Router assigns to STAs: 10.10.10.2 to 10.10.10.254/24
Gateway for STAs	VLANIF 101: 10.10.10.1/24
RADIUS authentication parameters	● IP address: 12.1.1.1 ● Authentication port number: 1812 ● Shared key: 123456 ● AAA domain: huawei.com
User name and password of STAs	● User name: test@huawei.com ● Password: 123456

Procedure

Step 1 Configure SwitchA and the AP can communicate with the upstream device.

Add GE0/0/1 that connects SwitchA to the AP to VLAN 101, VLAN 102, and VLAN 103. Add GE0/0/2 that connects SwitchA to the router to VLAN 102. Add GE0/0/3 that connects SwitchA to the RADIUS server to VLAN 103.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 101 102 103
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 102
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
```

```
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 103
[SwitchA-GigabitEthernet0/0/3] quit
```

Step 2 Configure the AP to communicate with the upstream device.

Configure VLANIF 101 (service VLAN), VLANIF 102, and VLANIF 103.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101 102 103
[AP] interface vlanif 101
[AP-Vlanif101] ip address 10.10.10.1 24
[AP-Vlanif101] quit
[AP] interface vlanif 102
[AP-Vlanif102] ip address 11.1.1.2 24
[AP-Vlanif102] quit
[AP] interface vlanif 103
[AP-Vlanif103] ip address 12.1.1.2 24
[AP-Vlanif103] quit
```

Add GE0/0/1 that connects the AP to the SwitchA to VLAN 101, VLAN 102, and VLAN 103.

```
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[AP-GigabitEthernet0/0/1] quit
```

On the AP, configure a static route.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
```

Step 3 Configure the AP and the Router to assign IP addresses to STAs.

Configure the AP as the DHCP relay agent and enable user entry detection on the AP.

```
[AP] dhcp enable
[AP] dhcp relay detect enable
[AP] interface vlanif 101
[AP-Vlanif101] dhcp select relay
[AP-Vlanif101] dhcp relay server-ip 11.1.1.1
[AP-Vlanif101] quit
```

Configure the Router as a DHCP server to allocate IP addresses to STAs.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] ip pool sta
[Router-ip-pool-sta] gateway-list 10.10.10.1
[Router-ip-pool-sta] network 10.10.10.0 mask 24
[Router-ip-pool-sta] quit
[Router] vlan batch 102
[Router] interface vlanif 102
[Router-Vlanif102] ip address 11.1.1.1 24
[Router-Vlanif102] dhcp select global
[Router-Vlanif102] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.10.10.0 24 11.1.1.2
```

Step 4 Configure an AAA domain to which a RADIUS server template is applied.

1. Configure a RADIUS server template, an AAA authentication scheme, and domain information.

NOTE

Ensure that the AP and RADIUS server have the same shared key.

```
[AP] radius-server template radius_huawei
[AP-radius-radius_huawei] radius-server authentication 12.1.1.1 1812
[AP-radius-radius_huawei] radius-server shared-key cipher 123456
[AP-radius-radius_huawei] quit
[AP] aaa
[AP-aaa] authentication-scheme radius_huawei
[AP-aaa-authen-radius_huawei] authentication-mode radius
[AP-aaa-authen-radius_huawei] quit
[AP-aaa] domain huawei.com
[AP-aaa-domain-huawei.com] authentication-scheme radius_huawei
[AP-aaa-domain-huawei.com] radius-server radius_huawei
[AP-aaa-domain-huawei.com] quit
[AP-aaa] quit
```

NOTE

After domain **huawei.com** is configured, the domain name is added to the authentication user name.

2. Test whether a STA can be authenticated using RADIUS authentication. A user name **test@huawei.com** and password **123456** have been configured on the RADIUS server.

```
[AP] test-aaa test@huawei.com 123456 radius-template radius_huawei
Info: Account test succeed.
```

Step 5 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 6 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 7 Enable 802.1x authentication on the WLAN-BSS interface.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] dot1x enable
[AP-Wlan-Bss1] dot1x authentication-method eap
[AP-Wlan-Bss1] force-domain name huawei.com
[AP-Wlan-Bss1] permit-domain name huawei.com
[AP-Wlan-Bss1] quit
```

Step 8 Configure a WPA security policy.

```
[AP] wlan
[AP-wlan-view] security-profile name security
[AP-wlan-sec-prof-security] security-policy wpa
[AP-wlan-sec-prof-security] wpa authentication-method dot1x encryption-method ccmp
[AP-wlan-sec-prof-security] quit
[AP-wlan-view] quit
```

Step 9 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 10 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- The wireless PC obtains an IP address after it associates with the WLAN.
- Use the 802.1x authentication client on a STA and enter the correct user name and password. The STA is authenticated and can access the WLAN. You must configure the client for PEAP authentication.
  - Configuration on the Windows XP operating system:
    1. On the **Association** tab page of the **Wireless network properties** dialog box, add SSID **test**, set the authentication mode to WPA, encryption mode to CCMP, and encryption algorithm to AES.
    2. On the **Authentication** tab page, set EAP type to PEAP and click **Properties**. In the **Protected EAP Properties** dialog box, deselect **Validate server certificate** and click **Configure**. In the displayed dialog box, deselect **Automatically use my Windows logon name and password** and click **OK**.
  - Configuration on the Windows 7 operating system:
    1. Access the **Manage wireless networks** page, click **Add**, and select **Manually create a network profile**. Add SSID **test**. Set the authentication mode to **WPA-Enterprise**, the encryption mode to CCMP, and the algorithm to AES. Click **Next**.
    2. Scan SSIDs and double-click SSID **test**. On the **Security** tab page, set EAP type to PEAP and click **Settings**. In the displayed dialog box, deselect **Validate server**

certificate and click **Configure**. In the displayed dialog box, deselect **Automatically use my Windows logon name and password** and click **OK**.

----End

Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 101 to 103
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 103
#
return
```

- Configuration file of Router

```
#
sysname Router
#
 vlan batch 102
#
dhcp enable
#
ip pool sta
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
#
interface Vlanif102
 ip address 11.1.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 102
#
ip route-static 10.10.10.0 24 11.1.1.2
#
return
```

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101 to 103
#
dhcp enable
#
dhcp relay detect enable
#
radius-server template radius_huawei
 radius-server authentication 12.1.1.1 1812 weight 80
 radius-server shared-key cipher %@%@hH67%f}f8X"AE&Pw`wS~{:;0%@%@
#
```

```
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 domain huawei.com
  authentication-scheme radius_huawei
  radius-server radius_huawei
#
interface Vlanif101
 ip address 10.10.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 11.1.1.1
#
interface Vlanif102
 ip address 11.1.1.2 255.255.255.0
#
interface Vlanif103
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 dot1x enable
 dot1x authentication-method eap
 permit-domain name huawei.com
 force-domain name huawei.com
#
ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
  security-policy wpa
  wpa authentication-method dot1x encryption-method ccmp
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

7.2.7.2 Example for Configuring MAC Address Authentication

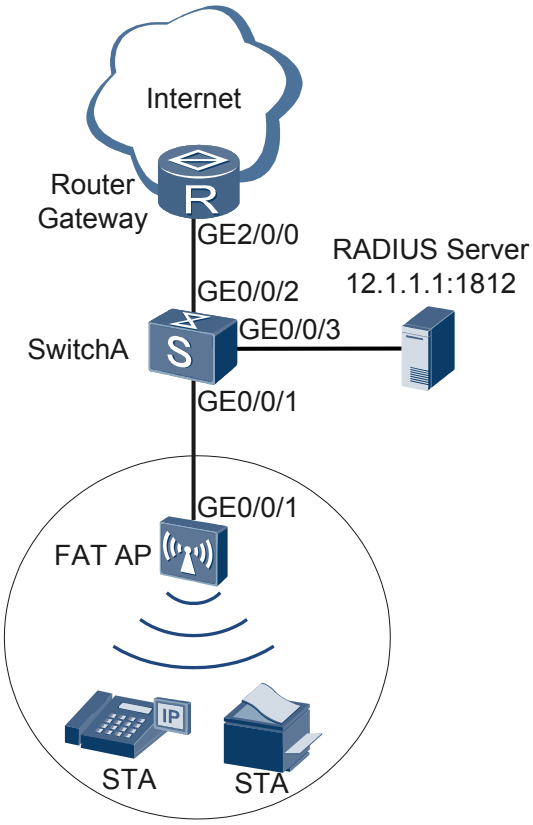
Networking Requirements

As shown in **Figure 7-33**, the enterprise's AP connects to the egress gateway (Router) and RADIUS server. The WLAN with the SSID of **test** is available for wireless users and terminals to access network resources. The gateway also functions as a DHCP server to provide IP addresses on the 10.10.10.0/24 network segment for STAs. The AP controls and manages STAs.

The WLAN authentication client cannot be installed on wireless devices providing public services, such as wireless printers and phones, so use MAC address authentication. The RADIUS

server authenticates wireless devices using their MAC addresses. No authentication is required when STAs access the WLAN, facilitating the use of WLAN services.

Figure 7-33 Networking diagram for configuring MAC address authentication on the wireless side



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.
2. Configure a RADIUS server template and apply it to an AAA domain.
3. Configure MAC address authentication on the WLAN-BSS interface to authenticate STAs.

Table 7-26 Data plan

Configuration Item	Data
WLAN service	Open system authentication+non-encryption
Service VLAN	VLAN 101
Service set	SSID: test
SwitchA VLAN	VLAN 101, VLAN 102, VLAN 103

Configuration Item	Data
DHCP server	IP addresses that Router assigns to STAs: 10.10.10.2 to 10.10.10.254/24
Gateway for STAs	VLANIF 101: 10.10.10.1/24
RADIUS authentication parameters	● IP address: 12.1.1.1 ● Port number: 1812 ● Shared key: huawei ● AAA domain: huawei.com
MAC address of a STA	0011-2233-4455

Procedure

Step 1 Configure SwitchA and the AP can communicate with the upstream device.

Add GE0/0/1 that connects SwitchA to the AP to VLAN 101, VLAN 102, and VLAN 103. Add GE0/0/2 that connects SwitchA to the router to VLAN 102. Add GE0/0/3 that connects SwitchA to the RADIUS server to VLAN 103.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 101 102 103
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 102
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 103
[SwitchA-GigabitEthernet0/0/3] quit
```

Step 2 Configure the AP to communicate with the upstream device.

Configure VLANIF 101 (service VLAN), VLANIF 102, and VLANIF 103.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101 102 103
[AP] interface vlanif 101
[AP-Vlanif101] ip address 10.10.10.1 24
[AP-Vlanif101] quit
[AP] interface vlanif 102
[AP-Vlanif102] ip address 11.1.1.2 24
[AP-Vlanif102] quit
[AP] interface vlanif 103
[AP-Vlanif103] ip address 12.1.1.2 24
[AP-Vlanif103] quit
```

Add GE0/0/1 that connects the AP to the SwitchA to VLAN 101, VLAN 102, and VLAN 103.

```
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
```

```
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103
[AP-GigabitEthernet0/0/1] quit
```

On the AC, configure a static route.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
```

Step 3 Configure the AP and the Router to assign IP addresses to STAs.

Configure the AP as the DHCP relay agent and enable user entry detection on the AP.

```
[AP] dhcp enable
[AP] dhcp relay detect enable
[AP] interface vlanif 101
[AP-Vlanif101] dhcp select relay
[AP-Vlanif101] dhcp relay server-ip 11.1.1.1
[AP-Vlanif101] quit
```

Configure the Router as a DHCP server to allocate IP addresses to STAs.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] ip pool sta
[Router-ip-pool-sta] gateway-list 10.10.10.1
[Router-ip-pool-sta] network 10.10.10.0 mask 24
[Router-ip-pool-sta] quit
[Router] vlan batch 102
[Router] interface vlanif 102
[Router-Vlanif102] ip address 11.1.1.1 24
[Router-Vlanif102] dhcp select global
[Router-Vlanif102] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.10.10.0 24 11.1.1.2
```

Step 4 Configure RADIUS authentication.

1. Configure a RADIUS server template, an AAA authentication scheme, and domain information.

   NOTE

   The STA sends its MAC address as the user name to the RADIUS server for authentication, so the AC needs to be disabled from adding a domain name to the user name.

   ```
   [AP] radius-server template radius_huawei
   [AP-radius-radius_huawei] radius-server authentication 12.1.1.1 1812
   [AP-radius-radius_huawei] radius-server shared-key cipher huawei
   [AP-radius-radius_huawei] undo radius-server user-name domain-included
   [AP-radius-radius_huawei] quit
   [AP] aaa
   [AP-aaa] authentication-scheme radius_huawei
   [AP-aaa-authen-radius_huawei] authentication-mode radius
   [AP-aaa-authen-radius_huawei] quit
   [AP-aaa] domain huawei.com
   [AP-aaa-domain-huawei.com] authentication-scheme radius_huawei
   [AP-aaa-domain-huawei.com] radius-server radius_huawei
   [AP-aaa-domain-huawei.com] quit
   [AP-aaa] quit
   ```

2. Globally configure user names in MAC address authentication without the delimiter "-".

   ```
   [AP] mac-authen username macaddress format without-hyphen
   ```

3. Test whether a STA can be authenticated using RADIUS authentication. In MAC address authentication, STA's MAC address is used as the user name and password.

```
[AP] test-aaa 001122334455 001122334455 radius-template radius_huawei
Info: Account test succeed.
```

Step 5 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 6 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 7 Configure MAC address authentication on the WLAN-BSS interface.

```
[AP] mac-authen
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] mac-authen
[AP-Wlan-Bss1] force-domain name huawei.com
[AP-Wlan-Bss1] permit-domain name huawei.com
[AP-Wlan-Bss1] quit
```

Step 8 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
```

```
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 9 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- After the WLAN function is enabled on wireless devices, they can access the WLAN and provide public services.
- After the STA connects to the WLAN, authentication is performed automatically. You can directly access the WLAN.

----End

Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 101 to 103
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 103
#
return
```

- Configuration file of Router

```
#
sysname Router
#
 vlan batch 102
#
dhcp enable
#
ip pool sta
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
#
interface Vlanif102
 ip address 11.1.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 102
#
ip route-static 10.10.10.0 24 11.1.1.2
#
return
```

- Configuration file of the AP

```
#
 sysname AP
#
```

```
vlan batch 101 to 103
#
mac-authen
#
dhcp enable
#
dhcp relay detect enable
#
radius-server template radius_huawei
 radius-server authentication 12.1.1.1 1812
 radius-server shared-key cipher %@%@hH67%f}f8X"AE&Pw`wS~{:;0%@%@
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 domain huawei.com
  authentication-scheme radius_huawei
  radius-server radius_huawei
#
 mac-authen username macaddress format without-hyphen
#
interface Vlanif101
 ip address 10.10.10.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 11.1.1.1
#
interface Vlanif102
 ip address 11.1.1.2 255.255.255.0
#
interface Vlanif103
 ip address 12.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 103
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 mac-authen
 permit-domain name huawei.com
 force-domain name huawei.com
#
ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

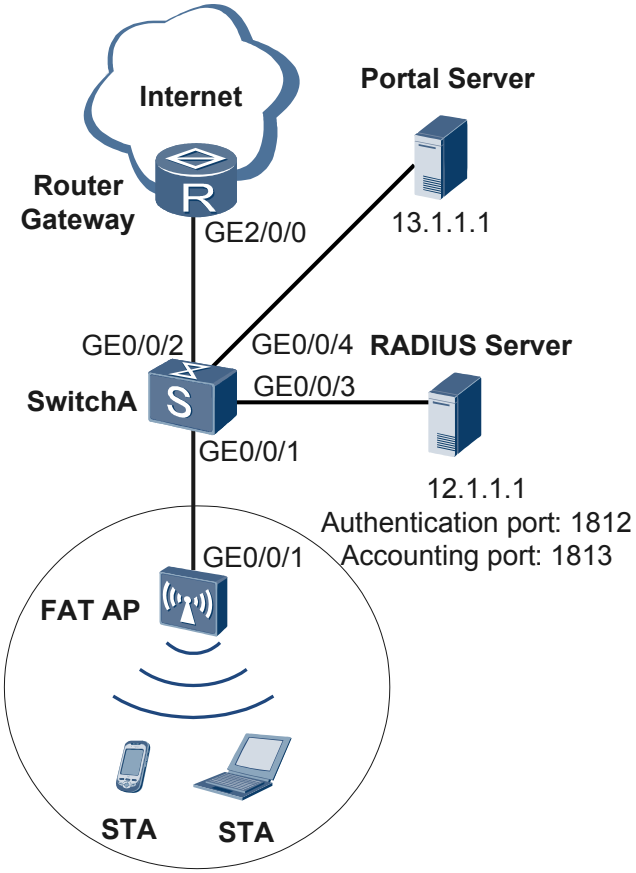
7.2.7.3 Example for Configuring Portal Authentication

Networking Requirements

As shown in **Figure 7-34**, the AP is deployed in an open place connects to the egress gateway (Router), RADIUS server, and Portal server. The WLAN with the SSID of **test** is available for users to access network resources. The gateway also functions as a DHCP server to provide IP addresses on the 10.10.10.0/24 network segment for STAs. The AP controls and manages STAs.

Because the WLAN is open to users, there are potential security risks. To facilitate access to the WLAN, use the default security policy on the AP. STAs are not authenticated and data is not encrypted. To uniformly manage STAs and allow only paid users to access the Internet, configure Portal authentication on the AP. Any user who attempts to access the Internet is redirected to the Portal authentication web page. A paid user connects to the Internet after entering the user name and password, and the RADIUS server starts accounting. An unpaid user must pay for the WLAN service and use the obtained user name and password to complete Portal authentication. Generally, the Portal authentication web page provides the paying function.

Figure 7-34 Networking diagram for configuring Portal authentication on the wireless side



Configuration Roadmap

1. Configure WLAN basic services so that STAs can access the WLAN. This example uses default configurations.

2. Configure a RADIUS server template, apply it to an AAA domain, and use a RADIUS server to authenticate STAs' identities and perform accounting.
3. Configure Portal authentication. Hypertext Transfer Protocol (HTTP) request packets from a user are redirected to the web page of the Portal server. After the user enters identity information, the STA sends the user identity information to the RADIUS server.

Table 7-27 Data plan

Configuration Item	Data
WLAN service	Open system authentication+non-encryption
Service VLAN	VLAN 101
Service set	SSID: test
SwitchA VLAN	VLAN 101, VLAN 102, VLAN 103
DHCP server	IP addresses that Router assigns to STAs: 10.10.10.2 to 10.10.10.254/24
Gateway for STAs	VLANIF101: 10.10.10.1/24
RADIUS server parameters	● Server IP address: 12.1.1.1 ● Authentication port number: 1812 ● Accounting port number: 1813 ● Shared key: huawei ● AAA domain: huawei.com
User name and password of STAs	● User name: test@huawei.com ● Password: 123456
Portal server parameters	● Server IP address: 13.1.1.1 ● Authentication port number: 50100 ● Shared key: huawei

Procedure

Step 1 Configure SwitchA and the AP can communicate with the upstream device.

Add GE0/0/1 that connects SwitchA to the AP to VLAN 101, VLAN 102, VLAN 103, and VLAN 104. Add GE0/0/2 that connects SwitchA to the router to VLAN 102. Add GE0/0/3 that connects SwitchA to the RADIUS server to VLAN 103. Add GE0/0/4 that connects SwitchA to the portal server to VLAN 104.

```
<Quidway> system-view
[Quidway] sysname SwitchA
[SwitchA] vlan batch 101 102 103 104
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitethernet 0/0/2
```

```
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 102
[SwitchA-GigabitEthernet0/0/2] quit
[SwitchA] interface gigabitethernet 0/0/3
[SwitchA-GigabitEthernet0/0/3] port link-type trunk
[SwitchA-GigabitEthernet0/0/3] port trunk allow-pass vlan 103
[SwitchA-GigabitEthernet0/0/3] quit
[SwitchA] interface gigabitethernet 0/0/4
[SwitchA-GigabitEthernet0/0/4] port link-type trunk
[SwitchA-GigabitEthernet0/0/4] port trunk allow-pass vlan 104
[SwitchA-GigabitEthernet0/0/4] quit
```

Step 2 Configure the AP to communicate with the upstream device.

Configure VLANIF 101 (service VLAN), VLANIF 102, VLANIF 103, and VLANIF 104.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101 102 103 104
[AP] interface vlanif 101
[AP-Vlanif101] ip address 10.10.10.1 24
[AP-Vlanif101] quit
[AP] interface vlanif 102
[AP-Vlanif102] ip address 11.1.1.2 24
[AP-Vlanif102] quit
[AP] interface vlanif 103
[AP-Vlanif103] ip address 12.1.1.2 24
[AP-Vlanif103] quit
[AP] interface vlanif 104
[AP-Vlanif104] ip address 13.1.1.2 24
[AP-Vlanif104] quit
```

Add GE0/0/1 that connects the AP to the SwitchA to VLAN 101, VLAN 102, VLAN 103, and VLAN 104.

```
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102 103 104
[AP-GigabitEthernet0/0/1] quit
```

On the AP, configure a static route.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
```

Step 3 Configure the AP and the Router to assign IP addresses to STAs.

Configure the AP as the DHCP relay agent and enable user entry detection on the AP.

```
[AP] dhcp enable
[AP] dhcp relay detect enable
[AP] interface vlanif 101
[AP-Vlanif101] dhcp select relay
[AP-Vlanif101] dhcp relay server-ip 11.1.1.1
[AP-Vlanif101] quit
```

Configure the Router as a DHCP server to allocate IP addresses to STAs.

```
<Huawei> system-view
[Huawei] sysname Router
[Router] dhcp enable
[Router] ip pool sta
[Router-ip-pool-sta] gateway-list 10.10.10.1
[Router-ip-pool-sta] network 10.10.10.0 mask 24
[Router-ip-pool-sta] quit
[Router] vlan batch 102
[Router] interface vlanif 102
[Router-Vlanif102] ip address 11.1.1.1 24
```

```
[Router-Vlanif102] dhcp select global
[Router-Vlanif102] quit
[Router] interface gigabitethernet 0/0/1
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[Router-GigabitEthernet0/0/1] quit
[Router] ip route-static 10.10.10.0 24 11.1.1.2
```

Step 4 Configure RADIUS authentication and accounting.

Configure a RADIUS server template, an AAA authentication scheme, an AAA accounting scheme, and domain information.

```
[AP] radius-server template radius_huawei
[AP-radius-radius_huawei] radius-server authentication 12.1.1.1 1812
[AP-radius-radius_huawei] radius-server accounting 12.1.1.1 1813
[AP-radius-radius_huawei] radius-server shared-key simple huawei
[AP-radius-radius_huawei] quit
[AP] aaa
[AP-aaa] authentication-scheme radius_huawei
[AP-aaa-authen-radius_huawei] authentication-mode radius
[AP-aaa-authen-radius_huawei] quit
[AP-aaa] accounting-scheme radius_huawei
[AP-aaa-accounting-radius_huawei] accounting-mode radius
[AP-aaa-accounting-radius_huawei] quit
[AP-aaa] domain huawei.com
[AP-aaa-domain-huawei.com] authentication-scheme radius_huawei
[AP-aaa-domain-huawei.com] accounting-scheme radius_huawei
[AP-aaa-domain-huawei.com] radius-server radius_huawei
[AP-aaa-domain-huawei.com] quit
[AP-aaa] quit
```

Test whether a STA can be authenticated using RADIUS authentication.

```
[AP] test-aaa test@huawei.com 123456 radius-template radius_huawei
Info: Account test succeed.
```

Step 5 Configure Portal authentication.

Configuring Portal server parameters.

```
[AP] web-auth-server test
[AP-web-auth-server-test] server-ip 13.1.1.1
[AP-web-auth-server-test] port 50100
[AP-web-auth-server-test] shared-key simple huawei
[AP-web-auth-server-test] url http://13.1.1.1
[AP-web-auth-server-test] quit
```

Bind VLAN 101 to the Portal server.

```
[AP] interface vlanif 101
[AP-Vlanif101] web-auth-server test direct
[AP-Vlanif101] quit
```

Step 6 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 7 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 8 Configure Portal authentication on the WLAN-BSS interface.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] force-domain name huawei.com
[AP-Wlan-Bss1] permit-domain name huawei.com
[AP-Wlan-Bss1] quit
```

Step 9 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 10 Verify the configuration.

- The WLAN with SSID **test** is available for STAs connected to the AP.
- The wireless PC obtains an IP address after it associates with the WLAN.
- Open a browser on the STA to access the Internet. The Portal authentication web page is automatically displayed. Enter the user name and password. The STA is authenticated and can access the WLAN.

----End

Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 101 to 104
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 104
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet0/0/3
 port link-type trunk
 port trunk allow-pass vlan 103
#
interface GigabitEthernet0/0/4
 port link-type trunk
 port trunk allow-pass vlan 104
#
return
```

- Configuration file of Router

```
#
sysname Router
#
 vlan batch 102
#
dhcp enable
#
ip pool sta
 gateway-list 10.10.10.1
 network 10.10.10.0 mask 255.255.255.0
#
interface Vlanif102
 ip address 11.1.1.1 255.255.255.0
 dhcp select global
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk allow-pass vlan 102
#
ip route-static 10.10.10.0 24 11.1.1.2
#
return
```

- Configuration file of the AP

```
#
 sysname AP
#
 vlan batch 101 to 104
#
dhcp enable
#
dhcp relay detect enable
#
radius-server template radius_huawei
 radius-server authentication 12.1.1.1 1812 weight 80
 radius-server accounting 12.1.1.1 1813 weight 80
 radius-server shared-key cipher %@%@hH67%f}f8X"AE&Pw`wS~{:;0%@%@
#
web-auth-server test
 server-ip 13.1.1.1
```

```
 port 50100
 shared-key cipher %@%@w^y1$5h,lGXtWH(R+B'0{GM{%@%@
 url http://13.1.1.1
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 accounting-scheme radius_huawei
  accounting-mode radius
 domain huawei.com
  authentication-scheme radius_huawei
  accounting-scheme radius_huawei
  radius-server radius_huawei
#
interface Vlanif101
 ip address 10.10.10.1 255.255.255.0
 web-auth-server test direct
 dhcp select relay
 dhcp relay server-ip 11.1.1.1
#
interface Vlanif102
 ip address 11.1.1.2 255.255.255.0
#
interface Vlanif103
 ip address 12.1.1.2 255.255.255.0
#
interface Vlanif104
 ip address 13.1.1.2 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101 to 104
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 permit-domain name huawei.com
 force-domain name huawei.com
#
ip route-static 0.0.0.0 0.0.0.0 11.1.1.1
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

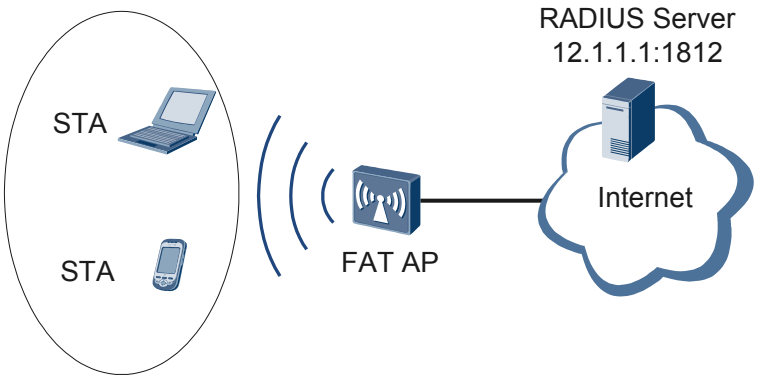
7.2.7.4 Example for Configuring Built-in Portal Authentication

Networking Requirements

As shown in **Figure 7-35**, a Fat AP of an enterprise provides wireless Internet access service and functions as a DHCP server to allocate IP addresses to users.

MAC address authentication controls the network access permission of a user based on the access interface and MAC address of the user. The user does not need to install any client software. After detecting the MAC address of a user for the first time, the AP starts authenticating the user. During the authentication, the user does not need to enter the user name or password. The administrator wants to use MAC address authentication to control STAs.

Figure 7-35 Networking of built-in Portal authentication



Configuration Roadmap

1. Create and configure a RADIUS server template, an authentication scheme, and a domain, and bind the RADIUS server template and authentication scheme to the domain, so that the AP can exchange information with the RADIUS server.
2. Configure basic WLAN services so that STAs can connect to the WLAN. This example uses default configuration parameters.
3. Configure built-in Portal authentication.
   a. Configure the IP address of the built-in Portal server so that the Fat AP can exchange information with the built-in Portal server.
   b. Enable Portal authentication to authenticate access users.

NOTE

- Ensure that the Fat AP, RADIUS server, and Portal server have reachable routes to each other.
- Ensure that the RADIUS server IP address, port number, and shared key are configured correctly and are the same as those on the RADIUS server.

Procedure

Step 1 Create and configure a RADIUS server template, an authentication scheme, and a domain.

Create and configure a RADIUS server template **radius_huawei**.

```
[FAT AP] radius-server template radius_huawei
[FAT AP-radius-radius_huawei] radius-server authentication 12.1.1.1 1812
[FAT AP-radius-radius_huawei] radius-server shared-key cipher huawei@1234
[FAT AP-radius-radius_huawei] quit
```

Create an authentication scheme **radius_huawei** in which the authentication mode is RADIUS.

```
[FAT AP] aaa
[FAT AP-aaa] authentication-scheme radius_huawei
[FAT AP-aaa-authen-radius_huawei] authentication-mode radius
[FAT AP-aaa-authen-radius_huawei] quit
```

Create a domain **huawei.com**, and bind the authentication and accounting schemes **radius_huawei** and RADIUS server template **radius_huawei** to the domain.

```
[FAT AP-aaa] domain huawei.com
[FAT AP-aaa-domain-huawei.com] authentication-scheme radius_huawei
[FAT AP-aaa-domain-huawei.com] radius-server radius_huawei
[FAT AP-aaa-domain-huawei.com] quit
[FAT AP-aaa] quit
```

Check whether a user can be authenticated using RADIUS authentication. The test user **test@huawei.com** and password **123456** have been configured on the RADIUS server.

```
[FAT AP] test-aaa test@huawei.com 123456 radius-template radius_huawei
Info: FAT APcount test succeed.
```

Configure authentication in the domain **huawei.com** for STAs.

```
[FAT AP] interface wlan-bss 1
[FAT AP-Wlan-Bss1] permit-domain name huawei.com
[FAT AP-Wlan-Bss1] force-domain name huawei.com
[FAT AP-Wlan-Bss1] quit
```

Step 2 Configure basic WLAN services.

1. Configure basic Fat AP functions.

   # Configure the country code for the Fat AP.

   ```
   <Huawei> system-view
   [Huawei] sysname FAT AP
   [FAT AP] wlan global country-code cn
   ```

   # Create the VLANIF 100 and an IP address, and configure the VLANIF 100 to allocate IP addresses to STAs from an IP address pool.

   ```
   [FAT AP] vlan batch 100
   [FAT AP] dhcp enable
   [FAT AP] interface vlanif 100
   [FAT AP-Vlanif100] ip address 192.168.10.1 24
   [FAT AP-Vlanif100] dhcp select interface
   [FAT AP-Vlanif100] quit
   ```

2. Configure WLAN service parameters.

   # Create a WMM profile **wmm**.

   ```
   [FAT AP-wlan-view] wmm-profile name wmm id 1
   [FAT AP-wlan-wmm-prof-wmm] quit
   ```

   # Create a radio profile **radio** and bind the WMM profile **wmm** to the radio profile.

   ```
   [FAT AP-wlan-view] radio-profile name radio id 1
   [FAT AP-wlan-radio-prof-radio] wmm-profile name wmm
   [FAT AP-wlan-radio-prof-radio] quit
   [FAT AP-wlan-view] quit
   ```

   # Bind the radio profile **radio** to a radio interface.

   ```
   [FAT AP] interface wlan-radio 0/0/0
   [FAT AP-Wlan-Radio0/0/0] radio-profile name radio
    Warning: Modify the Radio type may cause some parameters of Radio resume
   defaul
   t value, are you sure to continue?[Y/N]: y
   [FAT AP-Wlan-Radio0/0/0] quit
   ```

   # Configure a WLAN-BSS interface so that radio packets sent from users can be sent to the WLAN service processing module after reaching the AP.

```
[FAT AP] interface wlan-bss 1
[FAT AP-Wlan-Bss1] port hybrid pvid vlan 100
[FAT AP-Wlan-Bss1] port hybrid untagged vlan 100
[FAT AP-Wlan-Bss1] quit
```

Create a security profile **security**.

```
[FAT AP] wlan
[FAT AP-wlan-view] security-profile name security id 1
[FAT AP-wlan-sec-prof-security] quit
```

Create a traffic profile **traffic**.

```
[FAT AP-wlan-view] traffic-profile name traffic id 1
[FAT AP-wlan-traffic-prof-traffic] quit
```

Create a service set **test** and bind it to the WLAN-BSS interface, security profile, and traffic profile.

```
[FAT AP-wlan-view] service-set name test id 1
[FAT AP-wlan-service-set-test] ssid test
[FAT AP-wlan-service-set-test] wlan-bss 1
[FAT AP-wlan-service-set-test] security-profile name security
[FAT AP-wlan-service-set-test] traffic-profile name traffic
[FAT AP-wlan-service-set-test] quit
[FAT AP-wlan-view] quit
```

Bind the service set **test** to the radio interface.

```
[FAT AP] interface wlan-radio 0/0/0
[FAT AP-Wlan-Radio0/0/0] service-set name test
[FAT AP-Wlan-Radio0/0/0] quit
```

Step 3 Configure built-in Portal authentication.

Configure SSL policy sslserver and load a digital certificate.

For details, see **7.9.5.1 Example for Configuring a Server SSL Policy**.

Create a loopback interface and assign an IP address to the loopback interface.

```
[FAT AP] interface loopback 1
[FAT AP-LoopBack1] ip address 192.168.1.30 32
[FAT AP-LoopBack1] quit
```

Configured the IP address for the built-in Portal server.

```
[FAT AP] portal local-server ip 192.168.1.30
```

Enable built-in Portal authentication.

```
[FAT AP] portal local-server https ssl-policy sslserver
[FAT AP] portal local-server enable interface
```

Step 4 Verify the configuration.

- The WLAN with the SSID **test** is available for STAs after the configuration is complete.
- The STAs obtain IP addresses when they successfully associate with the WLAN.
- When a user opens the browser, the user is redirected to the Portal authentication page. After the user enters the correct user name and password and is successfully authenticated, the user can access the Internet.

----End

Configuration Files

- Configuration file of the Fat AP

```
#
 sysname FAT AP
#
 vlan batch 100 to 101
#
portal local-server ip 192.168.1.30
portal local-server https ssl-policy sslserver
#
dhcp enable
#
pki entity abc
 common-name hello
 country CN
#
radius-server template radius_huawei
 radius-server shared-key cipher %@%@4!ifTd`rATPg!lDdFh2GFuG7%@%@
 radius-server authentication 12.1.1.1 1812 weight 80
 radius-server accounting 12.1.1.1 1813 weight 80
#
pki realm admin
 entity abc
 ca id ca_root
 enrollment-url http://3.1.1.1:8080/certsrv/mscep/mscep.dll ra
 fingerprint sha1 7A34D94624B1C1BCBF6D763C4A67035D5B578EAF
#
ssl policy huawei type server
 pki-realm admin
 session cachesize 20 timeout 7200
#
aaa
 authentication-scheme radius_huawei
  authentication-mode radius
 accounting-scheme radius_huawei
  accounting-mode radius
 domain huawei.com
  authentication-scheme radius_huawei
  accounting-scheme radius_huawei
  radius-server radius_huawei
#
interface Vlanif100
 ip address 192.168.10.1 255.255.255.0
 dhcp select interface
#
interface Wlan-Bss1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 portal local-server enable
 permit-domain name default
 force-domain name default
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
```

```
 service-set id 1 wlan 1
#
return
```

7.2.8 References

The following table lists the references of this document.

Document	Description	Remarks
RFC3748	Extensible Authentication Protocol (EAP)	-
Portal 2.0	Portal protocol standard for Huawei broadband products (V2.01)	-

7.3 ACL Configuration

An access control list (ACL) is a set of rules that classify packets into different types. This chapter explains how to configure an ACL on a AP to filter packets.

7.3.1 Overview

This section describes the definition and functions of ACL.

Definition

An Access Control List (ACL) is composed of a list of rules. ACL rules classify packets so that the device processes classified packets in different manners.

Purpose

Devices need to communicate with each other on stable networks with reliable data transmission. Example:

- Defend against various network attacks, such as Internet Protocol (IP), Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP) packet attacks.
- Control network access. For example, control the access of enterprise network users to external networks, specific network resources that users can access, and time ranges in which users can access networks.
- Limit network traffic and improve network performance. For example, limit bandwidth for upstream and downstream traffic, charge for the bandwidth that users have applied for, and make full use of high-bandwidth network resources.

The ACL solves the preceding problems and ensures stability and reliability of network transmission.

7.3.2 Principles

This section describes the implementation of ACL.

7.3.2.1 Principles of ACLs

An ACL manages all configured rules and provides the matching algorithm for packets.

ACL Rule Management

An ACL can contain multiple rules. A rule is identified by a rule ID, which can be set by a user or automatically generated based on the ACL step. All rules in an ACL are arranged in ascending order of rule IDs.

There is an ACL step between rule IDs. For example, if an ACL step is set to 5, rules are numbered 5, 10, 15, and so on. If an ACL step is set to 2 and rule IDs are configured to be automatically generated, the system automatically generates rule IDs starting from 2. The step makes it possible to add a new rule between existing rules.

ACL Rule Matching

When a packet reaches a device, the search engine retrieves information from the packet to constitute the key value and matches it with ACL rules. Once a matching rule is found, the system stops matching. If no rule matches the packet, the system does not process the packet.

ACL rules can be classified into permit rules and deny rules.

In summary, the ACL classifies packets into the following types:

- Packets matching permit rules.
- Packets matching deny rules.
- Packets that do not match rules.

Different features have different manners to process the three types of packets. For details, see feature manuals.

7.3.2.2 ACL Classification

ACLs can be classified into different types according to different rules.

- ACLs can be classified into numbered ACLs and named ACLs according to the ACL naming mode.
  - A numbered ACL is identified by a number.

    NOTE

    The number is the identifier of the ACL. For example, the ACL with the number ranging from 2000 to 2999 is a basic ACL, and the ACL with the number ranging from 3000 to 3999 is an advanced ACL.
  - A named ACL is identified by a name.
- The **Table 7-28** lists the ACL classification.

Table 7-28 ACL classification

Category	IP Version	Function	Note
Basic ACL	IPv4	A basic ACL matches packets only based on the source IP address, fragment flag, and time range.	A basic IPv4 ACL is also called a basic ACL. Basic ACLs are numbered from 2000 to 2999.
Advanced ACL	IPv4	An advanced ACL matches packets based on the source IPv4 address, destination IPv4 address, IP precedence, Type of Service (ToS), DiffServ Code Point (DSCP) priority, IP protocol type, Internet Control Message Protocol (ICMP) type, TCP source/ destination port, and User Datagram Protocol (UDP) source/ destination port.	An advanced IPv4 ACL is also called an advanced ACL. Advanced ACLs are numbered from 3000 to 3999.
Layer 2 ACL	IPv4	A Layer 2 ACL matches packets based on Layer 2 information in packets, such as source and destination Media Access Control (MAC) addresses, and Layer 2 protocol types.	The number of a Layer 2 ACL ranges from 4000 to 4999.
User ACL	IPv4	An user ACL matches packets based on the source IPv4 address or user group, destination IPv4 address or user group, IP precedence, Type of Service (ToS), DiffServ Code Point (DSCP) priority, IP protocol type, Internet Control Message Protocol (ICMP) type, TCP source/ destination port, and User Datagram Protocol (UDP) source/ destination port.	The number of a user ACL ranges from 6000 to 6999.

7.3.2.3 ACL Naming

You can specify a unique name to an ACL. Each ACL has only one name. A named ACL is identified by the name, which can be specified to reference the ACL.

You can choose whether to specify a name when an ACL is created. After the ACL is created, you cannot modify or delete the ACL name, or specify names to unnamed ACLs.

You can configure a number for a named ACL. If no ACL number is specified for a named ACL, the system allocates an ACL number to the named ACL.

NOTE

A basic ACL and a basic ACL6 or an advanced ACL and an advanced ACL6 can use the same number.

7.3.2.4 Setting the Step Value for an ACL

Definition

The step is the difference between rule IDs when the system automatically assigns rule IDs. For example, if the step is set to 5, the rule IDs are multiples of 5 (beginning with 5), such as 5, 10, and 15.

- If the step value is changed, ACL rule IDs are arranged automatically. For example, the original rule numbers 5, 10, 15, and 20 will become 2, 4, 6, and 8 if you change the ACL step to 2.
- When the step restores to the default value, the device arranges ACL rule IDs using the default step value. For example, ACL rule group 3001 contains four rules with IDs being 2, 4, 6, and 8, and the step is 2. After the ACL rule restores to the default value, the ACL rule IDs become 5, 10, 15, and 20 and the step value is 5.

Function

The step value can be used to add a new rule between existing rules so that the matching order of ACL rules is configured. For example, four rules are configured in the ACL rule group: rules 5, 10, 15, and 20. To insert a new rule after rule 5 (the first rule), run the command to insert rule 7 between rule 5 and rule 10.

In addition, you do not need to specify a rule ID for an ACL rule. In this case, the system allocates the rule ID which is the sum of the current maximum ID and a step value. For example, the current maximum rule ID is 25 and the step value is 5, the system allocates the rule ID 30 to a new rule.

7.3.2.5 Matching Order of ACL Rules

An ACL is composed of a list of rules. Each rule contains a permit or deny clause. These rules may overlap or conflict. One rule can contain another rule, but the two rules must be different.

The device supports two types of matching order: configuration order and automatic order. The matching order determines the priorities of the rules in an ACL. Rule priorities resolve the conflict between overlapping rules.

Configuration Order

The configuration order indicates that ACL rules are matched in ascending order of rule IDs. The rule with the smallest rule ID is matched first. The configuration order is used by default.

Automatic Order

The automatic order follows the depth first principle.

ACL rules are arranged in sequence based on rule precision. Stricter conditions (such as the protocol type, source IP address range, or destination IP address range), the stricter in an ACL rule makes the rule more precise. For example, an ACL rule can be configured based on the wildcard of IP addresses. A smaller wildcard identifies a narrower network segment and therefore makes a stricter ACL rule.

If the ACL rules have the same priority according the depth first principle, they are matched based on rule IDs in ascending order.

NOTE

Similar to inverse mask, a wildcard mask is in dotted decimal notation. In a binary wildcard mask, the value 0 indicates that the bit in the IP address needs to be matched and the value 1 indicates that the bit in the IP address does not need to be matched. The value 0 and 1 in a wildcard mask can be discontinuous. For example, if the IP address is 192.168.1.169 and the wildcard mask is 0.0.0.172, the address is 192.168.1.x0x0xx01. The value x can be 0 or 1.

Table 7-29 lists the matching rules according to the depth first principle.

Table 7-29 Depth first principle

ACL Type	Matching rules
Basic ACL	1. The rule that defines the smallest source IP address range is matched first. The mask with the most 1 bits identifies the smallest source IP address range. 2. If the source IP address ranges are the same, the rule with the smallest ID is matched first.
Advanced ACL	1. The rule that defines a protocol type is matched first. 2. If the protocol types are the same, the rule that defines the smallest source IP address range is matched first. The mask with the most 1 bits identifies the smallest source IP address range. 3. If the protocol types and source IP address ranges are the same, the rule that defines the smallest destination IP address range is matched first. The mask with the most 1 bits identifies the smallest destination IP address range. 4. If the protocol types, source IP address ranges, and destination IP address ranges are the same, the rule that defines the smallest Layer 4 port number (TCP/UDP port number) range is matched first. 5. If the preceding ranges are all the same, the rule with the smallest ID is matched first.
Layer 2 ACL	1. The rule with the largest protocol type wildcard (with the most "1"s in the mask) is matched first. 2. The rule that defines the smallest source MAC address range is matched first. The mask with the most 1 bits identifies the smallest source MAC address range. 3. If the source MAC address ranges are the same, the rule that defines the smallest destination MAC address range is matched first. The mask with the most 1 bits identifies the smallest destination MAC address range. 4. If the source and destination MAC address ranges are the same, the rule with the smallest ID is matched first.

ACL Type	Matching rules
User ACL	1. The rule that defines a protocol type is matched first. 2. If the protocol types are the same, the rule that defines the smallest source IP address range is matched first. The mask with the most 1 bits identifies the smallest source IP address range. 3. If the protocol types and source IP address ranges are the same, the rule that defines the smallest destination IP address range is matched first. The mask with the most 1 bits identifies the smallest destination IP address range. 4. If the protocol types, source IP address ranges, and destination IP address ranges are the same, the rule that defines the smallest Layer 4 port number (TCP/UDP port number) range is matched first. 5. If the preceding ranges are all the same, the rule with the smallest ID is matched first.

7.3.2.6 Packet Fragmentation Supported by ACLs

The AP can filter fragmented packets. It can match all Layer 3 IP packets with Layer 3 filtering rules.

- If **fragment** is not specified in an ACL rule, the device matches non-fragmented packets and fragmented packets.
- If **fragment** is specified in the ACL rule, the device matches fragmented packets only.

When attackers construct fragmented packets to attack the network, you can specify **fragment** in an ACL rule to enable the device to filter non-initial fragmented packets only. This prevents the device from filtering other non-fragmented packets to protect normal service transmission.

7.3.2.7 Time Range of an ACL

A time range specifies a period of time. In practice, some ACL rules are required to be valid during a certain period of time, and invalid outside of that period of time, meaning that ACL rules are used to filter packets based on the time range. For example, if staff members are prohibited from browsing entertainment websites during business hours but are allowed to visit these entertainment websites during after-hours using a specified device, a time range must be defined for an ACL to execute these conditions. To implement this function, configure one or more time ranges, and reference time ranges using commands.

If no time range referenced by the rule is configured, the rule does not take effect until the referenced time range is specified and the system time is within the specified time range.

7.3.3 Default Configuration

This section describes the default ACL configurations.

Table 7-30 describes default configurations of the ACL.

Table 7-30 Default ACL configuration

Parameter	Default Value
Step	5
Matching order	Configuration order

7.3.4 Configuring ACL

This section describes the procedures for configuring ACL.

7.3.4.1 Configuring a Basic ACL

A basic ACL classifies IPv4 packets based on information such as source IP addresses.

7.3.4.1.1 (Optional) Configuring the Validity Time Range of a Rule

Context

Some services or functions are restricted within a specified period of time, for example, Quality of Service (QoS) is started only during peak hours. You can create a time range and reference the time range in an ACL applied to these services or functions so that the ACL takes effect only in the time range. The services or functions that reference the ACL is also started in the specified time range.

NOTICE

The deletion of ACL validity time range may cause invalidity of some ACLs. Therefore, use this command with caution.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
time-range time-name { start-time to end-time { days } &<1-7> | from time1 date1
[ to time2 date2 ] }
```

A time range is created.

To configure multiple time ranges with the same name on the AP, run the preceding command with the same value of *time-name* repeatedly.

NOTE

If multiple time ranges are configured using the same *time-name* value, the system takes the union of periodic time ranges and the union of absolute time ranges, and then takes the intersection of the two unions as the final time range. In this example, the name **test** is used to configure the following time ranges:

- Time range 1: 01.01.2010 00:00 to 31.12.2010 23:59 (absolute time range)
- Time range 2: 8:00 to 18:00 from Monday to Friday (periodic time range)
- Time range 3: 14:00 to 18:00 on Saturday and Sunday (periodic time range)

The time range **test** includes 8:00-18:00 on Monday to Friday and 14:00-18:00 on Saturday and Sunday in 2010.

You are advised to configure the Network Time Protocol (NTP) to ensure that devices on the network use the same system time. For the NTP configuration, see **9.5.4.1 Configuring Basic NTP Functions** in the *Huawei Wireless Access Points Configuration Guide - Network Management*.

----End

7.3.4.1.2 Creating a Basic ACL

Context

Basic ACLs classify IPv4 packets based on source IP addresses, fragment flags, and time ranges in the packets.

Before configuring a basic ACL, you need to create a basic ACL.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

A numbered basic ACL is created and the basic ACL view is displayed.

Or run:

```
acl name acl-name { basic | acl-number } [ match-order { auto | config } ]
```

A named basic ACL is created and the basic ACL view is displayed.

acl-number specifies the number of a basic ACL. The value ranges from 2000 to 2999.

By default, no ACL is created.

Step 3 (Optional) Run:

```
step step
```

The ACL step is configured.

By default, the step between ACL rule IDs is 5.

Step 4 (Optional) Run:

```
description text
```

The ACL description is configured.

By default, no description is configured for an ACL.

----End

7.3.4.1.3 Configuring a Basic ACL Rule

Context

A basic ACL classifies packets by matching packet information with its rules. After a basic ACL is created, configure rules in the basic ACL.

Adding new rules to an ACL will not affect the existing rules. If the new rule conflicts with an existing rule, the new rule takes effect. To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect. If different rules are ANDed or ORed, configure a correct matching order to prevent incorrect configurations.

NOTE

When the device receives a packet, it matches the packet with ACL rules one by one based on the matching order. Once the packet matches a rule, the device stops the matching process and performs the action specified in the matching rule on the packet.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

A numbered basic ACL is created and the basic ACL view is displayed.

Or run:

```
acl name acl-name { basic | acl-number } [ match-order { auto | config } ]
```

A named basic ACL is created and the basic ACL view is displayed.

acl-number specifies the number of a basic ACL. The value ranges from 2000 to 2999.

By default, no ACL is created.

Step 3 Run:

```
rule [ rule-id ] { deny | permit } [ source { source-address source-wildcard |
any } | fragment | time-range time-name ] *
```

A basic ACL rule is configured. To configure multiple rules, repeat this step.

NOTE

After the first rule is configured in an ACL, the device uses the step value as the number of this rule if the *rule-id* parameter is not specified. If the *rule-id* parameter is not specified for the later rules, the device uses the multiples of the next step of the last rule ID to number the rules. For example, if an ACL includes rule 7 and the step is 5, the system assigns 10 to a new rule without *rule-id* specified.

When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.

Step 4 (Optional) Run:

rule *rule-id* **description** *description*

The description of a basic ACL rule is configured.

The device only supports the description configured for the rules with rule IDs. You are not allowed to configure the description for a rule that has not been created.

----End

7.3.4.1.4 Applying the ACL to the AP

Context

An ACL is a set of rules that differentiate packets and determines whether packets are permitted and denied. The device then processes the permitted packets and discards the denied packets.

Procedure

- Apply the ACL.

  ACL can be applied to many features. For example, to process different types of traffic, you can use basic ACLs, advanced ACLs, Layer 2 ACLs to perform traffic policing, or traffic classification on the traffic that matches the ACL rules.

  NOTE

  ACL can be applied to different services, and devices running these services process the classified packets according to service requirements. For details about the services referencing ACLs, see the configuration guide.

----End

7.3.4.1.5 Checking the Configuration

Procedure

- Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } command to view the configuration about a specific ACL or all ACLs.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

----End

7.3.4.2 Configuring an Advanced ACL

Advanced ACLs classify IPv4 packets based on information such as source and destination IP addresses, source and destination port numbers, packet priorities, and time ranges.

7.3.4.2.1 (Optional) Configuring the Validity Time Range of a Rule

Context

Some services or functions are restricted within a specified period of time, for example, Quality of Service (QoS) is started only during peak hours. You can create a time range and reference the time range in an ACL applied to these services or functions so that the ACL takes effect only

in the time range. The services or functions that reference the ACL is also started in the specified time range.

NOTICE

The deletion of ACL validity time range may cause invalidity of some ACLs. Therefore, use this command with caution.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
time-range time-name { start-time to end-time { days } &<1-7> | from time1 date1
[ to time2 date2 ] }
```

A time range is created.

To configure multiple time ranges with the same name on the AP, run the preceding command with the same value of *time-name* repeatedly.

NOTE

If multiple time ranges are configured using the same *time-name* value, the system takes the union of periodic time ranges and the union of absolute time ranges, and then takes the intersection of the two unions as the final time range. In this example, the name **test** is used to configure the following time ranges:

- Time range 1: 01.01.2010 00:00 to 31.12.2010 23:59 (absolute time range)
- Time range 2: 8:00 to 18:00 from Monday to Friday (periodic time range)
- Time range 3: 14:00 to 18:00 on Saturday and Sunday (periodic time range)

The time range **test** includes 8:00-18:00 on Monday to Friday and 14:00-18:00 on Saturday and Sunday in 2010.

You are advised to configure the Network Time Protocol (NTP) to ensure that devices on the network use the same system time. For the NTP configuration, see **9.5.4.1 Configuring Basic NTP Functions** in the *Huawei Wireless Access Points Configuration Guide - Network Management*.

----End

7.3.4.2.2 Creating an Advanced ACL

Context

Advanced ACLs classify IPv4 packets based on the source IP address, destination IP address, IP precedence, Type of Service (ToS), DiffServ Code Point (DSCP) priority, IP protocol type, Internet Control Message Protocol (ICMP) type, TCP source/destination port number, and User Datagram Protocol (UDP) source/destination port.

Before configuring an advanced ACL, you need to create an advanced ACL.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

A numbered advanced ACL is created and the advanced ACL view is displayed.

Or run:

```
acl name acl-name { advance | acl-number } [ match-order { auto | config } ]
```

A named advanced ACL is created and the advanced ACL view is displayed.

acl-number specifies the number of an advanced ACL. The value ranges from 3000 to 3999.

By default, no ACL is created.

Step 3 (Optional) Run:

```
step step
```

The ACL step is configured.

By default, the step between ACL rule IDs is 5.

Step 4 (Optional) Run:

```
description text
```

The ACL description is configured.

By default, no description is configured for an ACL.

----End

7.3.4.2.3 Configuring an Advanced ACL Rule

Context

An advanced ACL classifies packets by matching packet information with its rules. After an advanced ACL is created, configure rules in the advanced ACL.

Adding new rules to an ACL will not affect the existing rules. If the new rule conflicts with an existing rule, the new rule takes effect. To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect. If different rules are ANDed or ORed, configure a correct matching order to prevent incorrect configurations.

NOTE

When the device receives a packet, it matches the packet with ACL rules one by one based on the matching order. Once the packet matches a rule, the device stops the matching process and performs the action specified in the matching rule on the packet.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

A numbered advanced ACL is created and the advanced ACL view is displayed.

Or run:

```
acl name acl-name { advance | acl-number } [ match-order { auto | config } ]
```

A named advanced ACL is created and the advanced ACL view is displayed.

acl-number specifies the number of an advanced ACL. The value ranges from 3000 to 3999.

By default, no ACL is created.

Step 3 Configure an advanced ACL rule based on the IP protocol version or the protocol type over IP.

- Configure an advanced ACL rule based on the IP protocol version. When IPv4 is used, run:

  rule [*rule-id*] { **deny** | **permit** } **ip** [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- Configure an advanced ACL rule based on the protocol type over IP.
  - When the ICMP protocol is used, run:

    rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

  - When the TCP protocol is used, run:

    rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

  - When the UDP protocol is used, run:

    rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

  - When the parameter *protocol* is specified as another protocol rather than TCP, UDP, or ICMP, run:

    rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

To configure multiple rules, repeat this step.

NOTE

To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.

The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set simultaneously for the same rule.

The **dscp** *dscp* and **tos** *tos* parameters cannot be set simultaneously for the same rule.

After the first rule is configured in an ACL, the device uses the step value as the number of this rule if the *rule-id* parameter is not specified. If the *rule-id* parameter is not specified for the later rules, the device uses the multiples of the next step of the last rule ID to number the rules. For example, if an ACL includes rule 7 and the step is 5, the system assigns 10 to a new rule without *rule-id* specified.

When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.

Step 4 (Optional) Run:

```
rule rule-id description description
```

The description of an advanced ACL rule is configured.

----End

7.3.4.2.4 Applying the ACL to the AP

Context

An ACL is a set of rules that differentiate packets and determines whether packets are permitted and denied. The device then processes the permitted packets and discards the denied packets.

Procedure

- Apply the ACL.

  ACL can be applied to many features. For example, to process different types of traffic, you can use basic ACLs, advanced ACLs, Layer 2 ACLs to perform traffic policing, or traffic classification on the traffic that matches the ACL rules.

  NOTE

  ACL can be applied to different services, and devices running these services process the classified packets according to service requirements. For details about the services referencing ACLs, see the configuration guide.

----End

7.3.4.2.5 Checking the Configuration

Procedure

- Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } command to view the configuration about a specific ACL or all ACLs.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

----End

7.3.4.3 Configuring a Layer 2 ACL

A Layer 2 ACL classifies data packets according to the link layer information, including the source MAC address, VLAN ID, Layer 2 protocol type, and destination MAC address.

7.3.4.3.1 (Optional) Configuring the Validity Time Range of a Rule

Context

Some services or functions are restricted within a specified period of time, for example, Quality of Service (QoS) is started only during peak hours. You can create a time range and reference the time range in an ACL applied to these services or functions so that the ACL takes effect only in the time range. The services or functions that reference the ACL is also started in the specified time range.

NOTICE

The deletion of ACL validity time range may cause invalidity of some ACLs. Therefore, use this command with caution.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
time-range time-name { start-time to end-time { days } &<1-7> | from time1 date1
[ to time2 date2 ] }
```

A time range is created.

To configure multiple time ranges with the same name on the AP, run the preceding command with the same value of *time-name* repeatedly.

NOTE

If multiple time ranges are configured using the same *time-name* value, the system takes the union of periodic time ranges and the union of absolute time ranges, and then takes the intersection of the two unions as the final time range. In this example, the name **test** is used to configure the following time ranges:

- Time range 1: 01.01.2010 00:00 to 31.12.2010 23:59 (absolute time range)
- Time range 2: 8:00 to 18:00 from Monday to Friday (periodic time range)
- Time range 3: 14:00 to 18:00 on Saturday and Sunday (periodic time range)

The time range **test** includes 8:00-18:00 on Monday to Friday and 14:00-18:00 on Saturday and Sunday in 2010.

You are advised to configure the Network Time Protocol (NTP) to ensure that devices on the network use the same system time. For the NTP configuration, see **9.5.4.1 Configuring Basic NTP Functions** in the *Huawei Wireless Access Points Configuration Guide - Network Management*.

----End

7.3.4.3.2 Creating a Layer 2 ACL

Context

A Layer 2 ACL classifies packets based on the source MAC address, destination MAC address, and Layer 2 protocol type in the packet.

Before configuring a Layer 2 ACL, you need to create a Layer 2 ACL.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

A numbered Layer 2 ACL is created and the Layer 2 ACL view is displayed.

Or run:

```
acl name acl-name { link | acl-number } [ match-order { auto | config } ]
```

A named Layer 2 ACL is created and the Layer 2 ACL view is displayed.

acl-number specifies the number of a Layer 2 ACL. The value ranges from 4000 to 4999.

By default, no ACL is created.

Step 3 (Optional) Run:

```
step step
```

The ACL step is configured.

By default, the step between ACL rule IDs is 5.

Step 4 (Optional) Run:

```
description text
```

The ACL description is configured.

By default, no description is configured for an ACL.

----End

7.3.4.3.3 Configuring a Layer 2 ACL Rule

Context

ACLs classify packets by matching packet information with its rules. After an ACL is created, configure rules in the ACL.

Adding new rules to an ACL will not affect the existing rules. If the new rule conflicts with an existing rule, the new rule takes effect. To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect. If different rules are ANDed or ORed, configure a correct matching order to prevent incorrect configurations.

NOTE

When the device receives a packet, it matches the packet with ACL rules one by one based on the matching order. Once the packet matches a rule, the device stops the matching process and performs the action specified in the matching rule on the packet.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

A numbered Layer 2 ACL is created and the Layer 2 ACL view is displayed.

Or run:

```
acl name acl-name { link | acl-number } [ match-order { auto | config } ]
```

A named Layer 2 ACL is created and the Layer 2 ACL view is displayed.

acl-number specifies the number of a Layer 2 ACL. The value ranges from 4000 to 4999.

By default, no ACL is created.

Step 3 Run:

```
rule [ rule-id ] { permit | deny } [ l2-protocol type-value [ type-mask ] |
destination-mac dest-mac-address [ dest-mac-mask ] | source-mac source-mac-address
[ source-mac-mask ] | vlan-id vlan-id [ vlan-id-mask ] | 8021p 802.1p-value ] *
[ time-range time-name ]
```

A Layer 2 ACL rule is configured.

To configure multiple rules, repeat this step.

NOTE

After the first rule is configured in an ACL, the device uses the step value as the number of this rule if the *rule-id* parameter is not specified. If the *rule-id* parameter is not specified for the later rules, the device uses the multiples of the next step of the last rule ID to number the rules. For example, if an ACL includes rule 7 and the step is 5, the system assigns 10 to a new rule without *rule-id* specified.

When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.

Step 4 (Optional) Run:

```
rule rule-id description description
```

The description of a Layer 2 ACL rule is configured.

The device only supports the description configured for the rules with rule IDs. You are not allowed to configure the description for a rule that has not been created.

----End

7.3.4.3.4 Applying the ACL to the AP

Context

An ACL is a set of rules that differentiate packets and determines whether packets are permitted and denied. The device then processes the permitted packets and discards the denied packets.

Procedure

- Apply the ACL.

  ACL can be applied to many features. For example, to process different types of traffic, you can use basic ACLs, advanced ACLs, Layer 2 ACLs to perform traffic policing, or traffic classification on the traffic that matches the ACL rules.

  NOTE

  ACL can be applied to different services, and devices running these services process the classified packets according to service requirements. For details about the services referencing ACLs, see the configuration guide.

----End

7.3.4.3.5 Checking the Configuration

Procedure

- Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } command to view the configuration about a specific ACL or all ACLs.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

----End

7.3.4.4 Configuring an User ACL

User ACLs classify IPv4 packets based on information such as source and destination IP addresses or user groups, source and destination port numbers, packet priorities, and time ranges.

7.3.4.4.1 (Optional) Configuring the Validity Time Range of a Rule

Context

Some services or functions are restricted within a specified period of time, for example, Quality of Service (QoS) is started only during peak hours. You can create a time range and reference the time range in an ACL applied to these services or functions so that the ACL takes effect only in the time range. The services or functions that reference the ACL is also started in the specified time range.

NOTICE

The deletion of ACL validity time range may cause invalidity of some ACLs. Therefore, use this command with caution.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
time-range time-name { start-time to end-time { days } &<1-7> | from time1 date1
[ to time2 date2 ] }
```

A time range is created.

To configure multiple time ranges with the same name on the AP, run the preceding command with the same value of *time-name* repeatedly.

NOTE

If multiple time ranges are configured using the same *time-name* value, the system takes the union of periodic time ranges and the union of absolute time ranges, and then takes the intersection of the two unions as the final time range. In this example, the name **test** is used to configure the following time ranges:

- Time range 1: 01.01.2010 00:00 to 31.12.2010 23:59 (absolute time range)
- Time range 2: 8:00 to 18:00 from Monday to Friday (periodic time range)
- Time range 3: 14:00 to 18:00 on Saturday and Sunday (periodic time range)

The time range **test** includes 8:00-18:00 on Monday to Friday and 14:00-18:00 on Saturday and Sunday in 2010.

You are advised to configure the Network Time Protocol (NTP) to ensure that devices on the network use the same system time. For the NTP configuration, see **9.5.4.1 Configuring Basic NTP Functions** in the *Huawei Wireless Access Points Configuration Guide - Network Management*.

----End

7.3.4.4.2 Creating an User ACL

Context

User ACLs classify IPv4 packets based on the source IP address or user group, destination IP address or user group, IP precedence, Type of Service (ToS), DiffServ Code Point (DSCP) priority, IP protocol type, Internet Control Message Protocol (ICMP) type, TCP source/destination port number, and User Datagram Protocol (UDP) source/destination port.

Before configuring an user ACL, you need to create an user ACL. *acl-number* specifies the number of an user ACL. The value ranges from 6000 to 6999.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
acl [ number ] acl-number [ match-order { auto | config } ]
```

A numbered user ACL is created and the user ACL view is displayed.

Step 3 (Optional) Run:

step *step*

The ACL step is configured.

Step 4 (Optional) Run:

description *text*

The ACL description is configured.

----End

7.3.4.4.3 Configuring an User ACL Rule

Context

An user ACL classifies packets by matching packet information with its rules. After an user ACL is created, configure rules in the user ACL.

Adding new rules to an ACL will not affect the existing rules. If the new rule conflicts with an existing rule, the new rule takes effect. To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect. If different rules are ANDed or ORed, configure a correct matching order to prevent incorrect configurations.

NOTE

When the device receives a packet, it matches the packet with ACL rules one by one based on the matching order. Once the packet matches a rule, the device stops the matching process and performs the action specified in the matching rule on the packet.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

acl [**number**] *acl-number* [**match-order** { **auto** | **config** }]

A numbered user ACL is created and the user ACL view is displayed.

Step 3 Configure an user ACL rule based on the IP protocol version or the protocol type over IP.

- Configure an user ACL rule based on the IP protocol version. When IPv4 is used, run:

  rule [*rule-id*] { **deny** | **permit** } **ip** [**destination** { { *destination-address destination-wildcard* | **any** } | **user-group** { **name** *destination-group-name* |**any** } } | **source** { { *source-address source-wildcard* | **any** } | **user-group** { **name** *source-group-name* |**any** } } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- Configure an user ACL rule based on the protocol type over IP.
  - When the ICMP protocol is used, run:

    rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { { *destination-address destination-wildcard* | **any** } | **user-group** { **name** *destination-group-name* | **any** } } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { { *source-address source-wildcard* | **any** } | **user-group** { **name** *source-group-name* |**any** } } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the TCP protocol is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { { *destination-address destination-wildcard* | **any** } | **user-group** { **name** *destination-group-name* | **any** } } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { { *source-address source-wildcard* | **any** } | **user-group** { **name** *source-group-name* |**any** } } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the UDP protocol is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { { *destination-address destination-wildcard* | **any** } | **user-group** { **name** *destination-group-name* | **any** } } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { { *source-address source-wildcard* | **any** } | **user-group** { **name** *source-group-name* |**any** } } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the parameter *protocol* is specified as another protocol rather than TCP, UDP, or ICMP, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ipinip** | **ospf** } [**destination** { { *destination-address destination-wildcard* | **any** } | **user-group** { **name** *destination-group-name* |**any** } } | **source** { { *source-address source-wildcard* | **any** } | **user-group** { **name** *source-group-name* |**any** } } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

To configure multiple rules, repeat this step.

NOTE

To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.

The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set simultaneously for the same rule.

The **dscp** *dscp* and **tos** *tos* parameters cannot be set simultaneously for the same rule.

After the first rule is configured in an ACL, the device uses the step value as the number of this rule if the *rule-id* parameter is not specified. If the *rule-id* parameter is not specified for the later rules, the device uses the multiples of the next step of the last rule ID to number the rules. For example, if an ACL includes rule 7 and the step is 5, the system assigns 10 to a new rule without *rule-id* specified.

When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.

If the user group information is specified in the rule, you cannot run the **acl-id (user group view)** command to bind the user group to the ACL. If the user group has been bound to the ACL, the user group information cannot be specified in the rules of user ACLs.

Step 4 (Optional) Run:

```
rule rule-id description description
```

The description of an user ACL rule is configured.

----End

7.3.4.4.4 Applying the ACL to the AP

Context

An ACL is a set of rules that differentiate packets and determines whether packets are permitted and denied. The device then processes the permitted packets and discards the denied packets.

Procedure

- Apply the ACL.

  ACL can be applied to many features. For example, to process different types of traffic, you can use basic ACLs, advanced ACLs, Layer 2 ACLs to perform traffic policing, or traffic classification on the traffic that matches the ACL rules.

  NOTE

  ACL can be applied to different services, and devices running these services process the classified packets according to service requirements. For details about the services referencing ACLs, see the configuration guide.

----End

7.3.4.4.5 Checking the Configuration

Procedure

- Run the **display acl** { *acl-number* | **name** *acl-name* | **all** } command to view the configuration about a specific ACL or all ACLs.
- Run the **display time-range** { **all** | *time-name* } command to view information about the time range.

----End

7.3.5 Maintaining an ACL

The section describes how to maintain an ACL.

7.3.5.1 Displaying ACL Resources

Context

If an ACL fails to be created, the available ACL resources in the system may be insufficient.

You can view ACL resource usage in the system to check whether the ACL resources have been used up.

Procedure

- Run the **display acl resource** command in any view to check information about ACL resources.

----End

7.3.6 References

This section lists references of ACL.

The following table lists the references of this document.

Document	Description	Remarks
RFC 4314	Defines several new access control rights and clarifies which rights are required for different IMAP (Internet Message Access Protocol) commands.	-

7.4 Local Attack Defense Configuration

Local attack defense limits the rate of packets sent to the CPU, ensuring device security and uninterrupted services when attacks occur.

7.4.1 Local Attack Defense Overview

Local attack defense prevents the CPU from being attacked by a large number of packets or malicious packets.

Definition

A large number of packets including malicious attack packets are sent to the Central Processing Unit (CPU) on a network. If malicious attack packets are sent to the CPU, the CPU is busy with processing these attack packets for a long period. Services are interrupted and even the system fails. If a large number of packets are sent to the CPU, the CPU usage becomes high and CPU performance deteriorates. In this case, services cannot be processed in a timely manner.

To protect the CPU and ensure that the CPU can process services, the device provides local attack defense. Local attack defense protects the device against attacks. When an attack occurs, this function ensures uninterrupted services and minimizes the impact on network services.

Basic Principles

The device can limit the rate of all packets sent to the CPU to protect the CPU.

- The device provides hierarchical device protection:
  - Level 1: The device limits the rate of packets sent to the CPU based on the protocol type to prevent excess packets of a protocol from being sent to the CPU.
  - Level 2: The device schedules packets sent to the CPU based on priorities of protocol packets to ensure that packets with higher protocol priorities are processed first.
  - Level 3: The device uniformly limits the rate of packets with the same priority sent to the CPU and randomly discards the excess packets to protect the CPU.

- When the device detects setup of an FTP session, ALP is enabled to protect the session. The packets matching characteristics of the session are sent at a high rate; therefore, reliability and stability of session-related services are ensured.

7.4.2 Default Configuration

This section provides the default configuration of local attack defense. You can change the configuration as required.

Table 7-31 list the default configuration of local attack defense.

Table 7-31 Default configuration of CPU attack defense

Parameter	Default Setting
CPU attack defense policy	CPU attack defense policy named **default**
Rate limit	500pps
Rate limit after ALP is enabled	During setup of an FTP connection, if the **application-apperceive** command is not used, the default rate limit specified by **application-apperceive** is applied to FTP packets. - FTP: 1024 pps

7.4.3 Configuring Local Attack Defense

This section describes the procedures for configuring local attack defense.

7.4.3.1 Configuring CPU Attack Defense

With the CPU attack defense function, the device limits the rate of packets sent to the CPU to protect the CPU.

Pre-configuration Tasks

Before configuring CPU attack defense, complete the following task:

- Connecting interfaces and setting physical parameters for the interfaces to ensure that the physical status of the interfaces is Up

Configuration Process

Before configuring CPU attack defense, create an attack defense policy first. The other tasks are performed in any sequence and can be selected as required. An attack defense policy takes effect only after it is applied to an object. There is no limitation on when the attack defense policy is applied.

7.4.3.1.1 Creating an Attack Defense Policy

Context

Before configuring local attack defense in an attack defense policy, you must create an attack defense policy.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
cpu-defend policy policy-name
```

An attack defense policy is created and the attack defense policy view is displayed.

The device supports a maximum of 19 attack defense policies, including the **default** attack defense policy. The **default** attack defense policy is generated in the system by default and is applied to the device. The **default** attack defense policy cannot be deleted or modified. The other 18 policies can be created, modified and deleted.

Step 3 (Optional) Run:

```
description text
```

The description of the attack defense policy is configured.

By default, no description is configured for an attack defense policy.

----End

7.4.3.1.2 Configuring the Rate Limit for Packets Sent to the CPU

Context

The device applies different rate limits to packets of different types or discards packets of a specified type to protect the CPU.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
cpu-defend policy policy-name
```

The attack defense policy view is displayed.

Step 3 Configure a rate limit for packets sent to the CPU.

- Run:

  ```
  packet-type packet-type rate-limit rate-value { wired | wireless }
  ```

The rate limit for packets sent to the CPU is set. Excess packets are discarded.

- Run:
  deny packet-type *packet-type* { **wired** | **wireless** }

  The device is configured to discard packets of a specified type sent to the CPU. That is, the rate limit for packets sent to the CPU is 0.

By default, the device applies the rate limit defined in the **default** attack defense policy to limit the packets sent to the CPU.

----End

7.4.3.1.3 Setting the Priority for Packets of a Specified Protocol

Context

After an attack defense policy is created, set priorities of protocol packets in the attack defense policy so that packets with higher priorities are processed first.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:
cpu-defend policy *policy-name*

The attack defense policy view is displayed.

Step 3 Run:
packet-type *packet-type* **priority** *priority-level* { **wired** | **wireless** }

The priority for packets of a specified protocol sent to the CPU is set.

By default, the priority defined in the **default** attack defense policy is used for packets of a specified protocol sent to the CPU.

----End

7.4.3.1.4 Configuring ALP

Context

Active link protection (ALP) protects session-based application layer data, including data of FTP sessions to ensure uninterrupted services when attacks occur.

The rate limit for packets after ALP is enabled can be set in the attack defense policy view. The **cpu-defend application-apperceive** command enables the ALP function.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:

```
cpu-defend policy policy-name
```

The attack defense policy view is displayed.

Step 3 Run:

```
application-apperceive packet-type ftp rate-limit rate-value
```

The rate limit for FTP packets is set.

By default, the rate limit for FTP packets is 1024 pps.

NOTE

During setup of an FTP connection, if the **application-apperceive** command is not used, the default rate limit specified by **application-apperceive** is applied to FTP packets.

After ALP is configured for FTP packets, it also takes effect for TFTP packets.

Step 4 Run:

```
quit
```

Return to the system view.

Step 5 Run:

```
cpu-defend application-apperceive [ ftp ] enable
```

ALP is enabled.

By default, ALP is enabled for FTP packets.

----End

7.4.3.1.5 Configuring the Rate Limit for All Packets Sent to the CPU

Context

After an attack defense policy is created, set the rate limit for all packets sent to the CPU in the attack defense policy. The device uniformly limits the rate of packets with the same priority sent to the CPU and randomly discards the excess packets to protect the CPU.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
cpu-defend policy policy-name
```

The attack defense policy view is displayed.

Step 3 Run:

```
rate-limit all-packets pps pps-value
```

The rate limit for all packets sent to the CPU is set.

By default, the rate limit is 500pps.

----End

7.4.3.1.6 Applying an Attack Defense Policy

Context

After an attack defense policy is created, you must apply the attack defense policy to the device in the system view. Otherwise, the attack defense policy does not take effect.

Only one attack defense policy can be applied to the device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
cpu-defend-policy policy-name
```

The attack defense policy is applied.

----End

7.4.3.1.7 Checking the Configuration

Procedure

- Run the **display cpu-defend policy** [*policy-name*] command to check the attack defense policy.
- Run the **display cpu-defend statistics** [**packet-type** *packet-type*] { **wired** | **wireless** } command to check statistics on packets sent to the CPU.
- Run the **display cpu-defend configuration** [**packet-type** *packet-type*] { **wired** | **wireless** } command to check the rate limits for protocol packets sent to the CPU.

----End

7.4.4 Maintaining Local Attack Defense

This section describes how to maintain local attack defense, including clearing statistics on packets sent to the CPU. This helps check whether the attack is eliminated.

7.4.4.1 Clearing Statistics About Packets Sent to the CPU

Context

Before recollecting statistics on packets sent to the CPU, run the following command in the user view to clear the existing statistics.

NOTICE

The cleared statistics cannot be restored. Exercise caution when you use the command.

Procedure

Step 1 Run the **reset cpu-defend statistics** [**packet-type** *packet-type*] { **wired** | **wireless** } command to clear statistics about packets sent to the CPU.

----End

7.5 Attack Defense Configuration

Attack defense is a network security feature. Attack defense allows the device to identify various types of network attacks and protect itself and the connected network against malicious attacks to ensure device and network operation.

7.5.1 Overview

This section describes the definition and functions of Attack defense.

Definition

Attack defense is a network security feature. This feature enables the device to analyze the content and behavior of packets sent to the CPU for processing, check whether packets are attack packets, and take measures for attack packets.

Attack defense is classified into malformed packet attack defense, packet fragment attack defense, and flood attack defense.

Purpose

Due to defects of communications protocols and network deployment problems, increasing network attacks have great impact on networks. In particular, attacks to a network device cause the device or network to crash.

The attack defense feature enables the device to discard or limit the rate of different types of attack packets sent to the CPU, protecting the device and ensuring normal services.

7.5.2 Principles

This section describes the implementation of Attack defense.

7.5.2.1 Defense Against Malformed Packet Attacks

The malformed packet attack is to send malformed IP packets to the system. If such an attack occurs, the system may break down when processing the malformed IP packets. Defense against malformed packet attacks allows the device to detect malformed packets in real time and discard them to protect the device.

Malformed packet attacks are classified into the following types.

Flood Attacks From IP Null Payload Packets

An IP packet with a 20-byte IP header only is considered as an IP null payload packet. An attacker often constructs IP packets with the IP header only and without any high-layer data. When the device processes these packets, errors may occur or the device may break down.

After defense against malformed packet attacks is enabled, the device directly discards the received IP packets without payloads.

Attacks from IGMP Null Payload Packets

An IGMP packet consists of a 20-byte IP header and a 8-byte IGMP body. The device considers IGMP packets with less than 28 bytes as IGMP null payload packets. When the device processes IGMP null payload packets, errors may occur or the device may break down.

After defense against malformed packet attacks is enabled, the device directly discards the received IGMP null payload packets.

LAND Attacks

Because of defects in the three-way handshake mechanism of TCP, a LAND attacker sends SYN packets of which the source address and port of a device are the same as the destination address and port respectively. After receiving the SYN packet, the target host creates a null TCP connection with the source and destination addresses as the address of the target host. The connection is kept until expiration. The target host will create many null TCP connections, wasting many resources or causing device breakdown.

After defense against malformed packet attacks is enabled, the device checks source and destination addresses in TCP SYN packets to prevent LAND attacks. The device considers TCP SYN packets with the same source and destination addresses as malformed packets and discards them.

Smurf Attack

An attacker sends an ICMP Request packets of which the source address is the target host address and the destination address is the broadcast address of the target network. After all hosts of the target network receive the ICMP request packet, they send ICMP Reply packets to the target host. The target host receives excess packets and consumes many resources, causing device breakdown or network blocking.

After defense against malformed packet attacks is enabled, the device checks whether the destination address in ICMP Request packets is the broadcast address or subnet broadcast address to prevent Smurf attacks. When detecting the ICMP Request packets with the destination address as the broadcast address or subnet broadcast address, the device directly discards them.

Attacks from Packets with Invalid TCP Flag Bits

A TCP packet contains six flag bits: URG, ACK, PSH, RST, SYN, and FIN. Different systems respond differently to the combination of these flag bits.

- If the six flag bits are all 1s, the attack is a Christmas tree attack. When the Christmas tree attack is launched, the device may break down.
- If both the SYN and FIN are 1 and the interface is disabled, the receiver replies with an RST | ACK message. If the interface is enabled, the receiver replies with an SYN | ACK message. This method is used to detect the host (online or offline) and interface (enabled or disabled).
- The six flag bits are all 0s.
  - If the interface is disabled, the receiver replies with an RST | ACK message to detect whether the host is online or offline.
  - If the interface is enabled, Linux and UNIX operating systems do not respond but the Windows operating system replies with an RST | ACK message. This helps you learn the type of the operating system (Windows, Linux, or UNIX).

After defense against malformed packet attacks is enabled, the device checks each flag bit of TCP packets to prevent attacks from packets with invalid TCP flag bits. If any of the following condition is met, the device discards the TCP packets:

- The six flag bits are all 1s.
- The SYN and FIN bits are all 1s.
- The six flag bits are all 0s.

7.5.2.2 Defense Against Packet Fragment Attacks

If an attacker sends error packet fragments to attack the device, the device may consume a large number of CPU resources, restart, or even break down, affecting normal services. Defense against packet fragment attacks allows the device to detect packet fragments in real time and discard them or limit the rate of the packets to protect the device.

Attacks of packet fragments are classified into the following types.

Excess-Fragment Attacks

The offset of IP packets is in the unit of 8 bytes. Normally, an IP header has 20 bytes and the maximum payload of an IP packet is 65515 bytes. An IP packet can be fragmented into up to 8189 fragments. The device consumes many CPU resources to reassemble the packets with over 8189 fragments.

After defense against packet fragment attacks is enabled, the device considers a packet with over 8189 fragments malicious and discards all the fragments of the packet.

Excess-Offset Attacks

An attacker sends a fragment with a larger offset value to the target host. As a result, the target host allocates much memory space to store all fragments, consuming a large number of resources.

The maximum value of the offset is 65528. Generally, the offset value does not exceed 8190. If the offset value is 8189 multiplied by 8 and the IP header is 20, the last fragment can have only 3-byte IP payload. Therefore, the maximum value of the offset is 8189 in normal situations. The device considers packets with the offset value larger than 8190 malicious and directly discards them.

After defense against packet fragment attacks is enabled, the device checks whether the offset value multiplied by 8 is greater than 65528. If the offset value multiplied by 8 is greater than 65528, the device considers the fragments malicious and discards them.

Repeated Packet Fragment Attacks

An attacker sends repeated fragments to the target host multiple times:

- The attacker sends the same fragments to the target host multiple times, causing abnormality in CPU and memory usage of the target host.
- The attacker sends different fragments with the same offset to the target host. As a result, the target host cannot determine how to process these packet fragments and there is abnormality in CPU and memory usage of the target host.

After defense against packet fragment attacks is enabled, the device applies the rate limit to packet fragments, reserves the first fragment, and discards all the remaining repeated fragments to protect the device CPU.

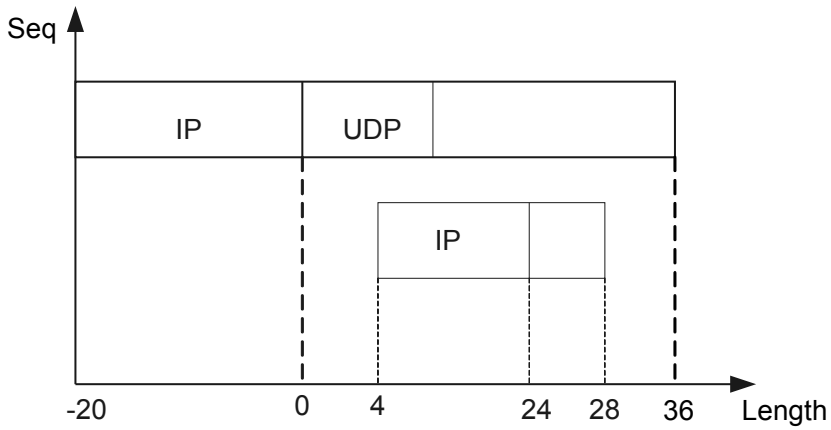
Tear Drop Attack

Tear Drop attack is the frequently used IP packet fragment attack. IP packets are incorrectly fragmented and the second fragment is contained in the first one. The offset of the second fragment is smaller than the offset of the first fragment, and the offset plus the Data field of the second fragment does not exceed the the tail of the first fragment.

As shown in **Figure 7-36**:

- In the first fragment, the IP payload is 36 bytes, the total length of the IP packet is 56 bytes, the protocol is UDP, and the UDP checksum is 0 (namely, unchecked).
- In the second fragment, the IP payload is 4 bytes, the total length of the IP packet is 24 bytes, the protocol is UDP, and the offset is 24 (this is incorrectly calculated and the correct offset is 36).

Figure 7-36 Tear Drop attack



Tear Drop attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all the fragments of Tear Drop attacks.

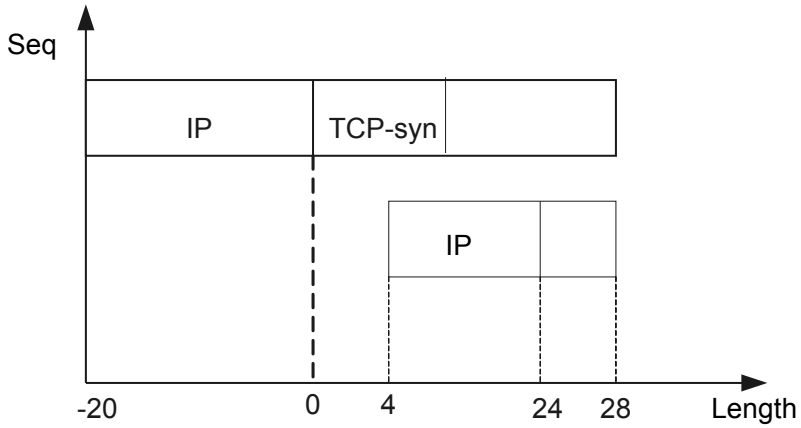
Syndrop Attack

Syndrop attack is similar to Tear Drop attack. The difference is that Syndrop attacks use TCP packets with SYN flag and IP payload.

As shown in **Figure 7-37**:

- In the first fragment, the IP payload is 28 bytes, and the IP header is 20 bytes.
- In the second fragment, the IP payload is 4 bytes, the IP header is 20 bytes, and the offset is 24 (this is incorrectly calculated and the correct offset is 28).

Figure 7-37 Syndrop attack



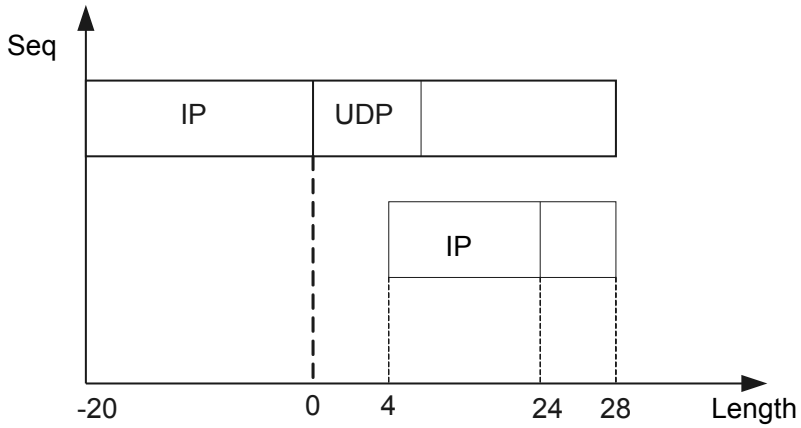
Syndrop attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all the fragments of Syndrop attacks.

Newtear Attack

NewTear attack is the attack from error fragments. As shown in **Figure 7-38**, the used protocol is UDP.

- The IP payload of the first fragment is 28 bytes including the UDP header. The UDP checksum is 0.
- The IP payload of the second fragment is 4 bytes. The offset is 24, which is incorrectly calculated. The correct offset is 28.

Figure 7-38 NewTear attack



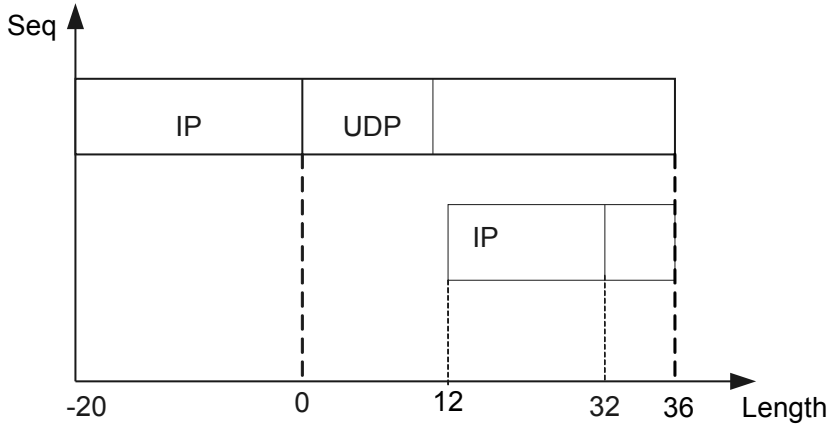
NewTear attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all the fragments of NewTear attacks.

Bonk Attack

Bonk attack is the attack from error fragments. As shown in **Figure 7-39**, the used protocol is UDP.

- The IP payload of the first fragment is 36 bytes including the UDP header. The UDP checksum is 0.
- The IP payload of the second fragment is 4 bytes. The offset is 32, which is incorrectly calculated. The correct offset is 36.

Figure 7-39 Bonk attack



Bonk attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all the fragments of Bonk attacks.

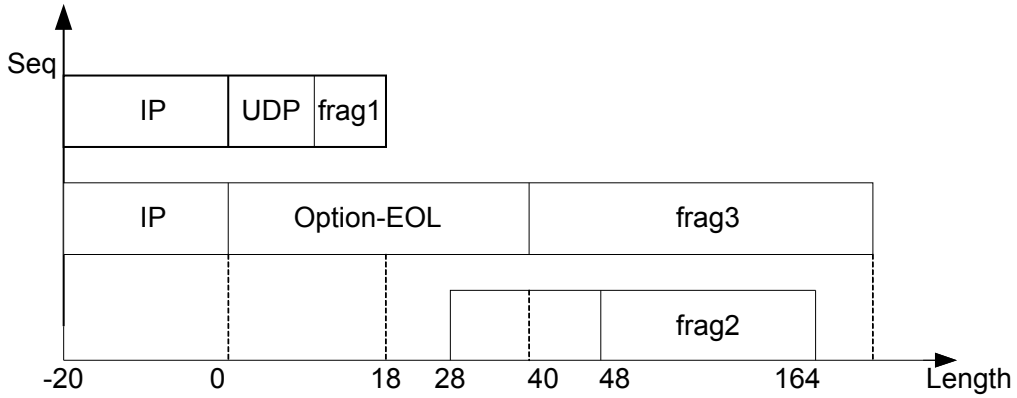
Nesta Attack

Nesta attack is the attack from error fragments. As shown in **Figure 7-40**:

- In the first fragment, the IP payload is 18 bytes, the used protocol is UDP, and the checksum is 0.

- In the second fragment, the offset is 48 and the IP payload is 116 bytes.
- In the third fragment, the offset is 0, the **more frag** is 1 (that is, there are more fragments), the **IP option** (all EOLs) is 40 bytes, and the IP payload is 224 bytes.

Figure 7-40 Nesta attack



Nesta attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all the fragments of Nesta attacks.

Rose Attack

The use protocol can be UDP or TCP.

As shown in **Figure 7-41**:

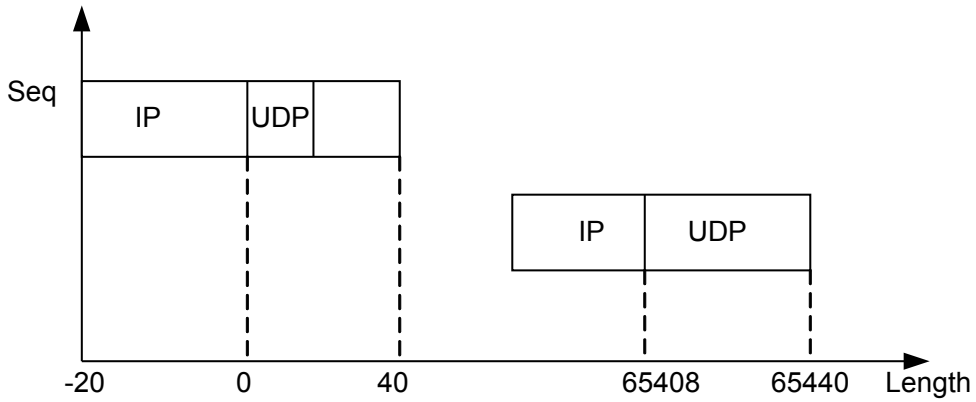
If Rose attacks use TCP:

- In the first fragment, the IP payload is 48 bytes (including the TCP header) and the length of the IP header is 20 bytes.
- In the second fragment, the IP payload is 32 bytes, the offset is 65408, and the **more frag** is 0 (last fragment).

If Rose attacks use UDP:

- In the first fragment, the IP payload is 40 bytes (including the UDP header, with UDP checksum 0), and the IP header is 20 bytes.
- In the second fragment, the IP payload is 32 bytes, the offset is 65408, and the **more frag** is 0 (last fragment).

Figure 7-41 Rose attack

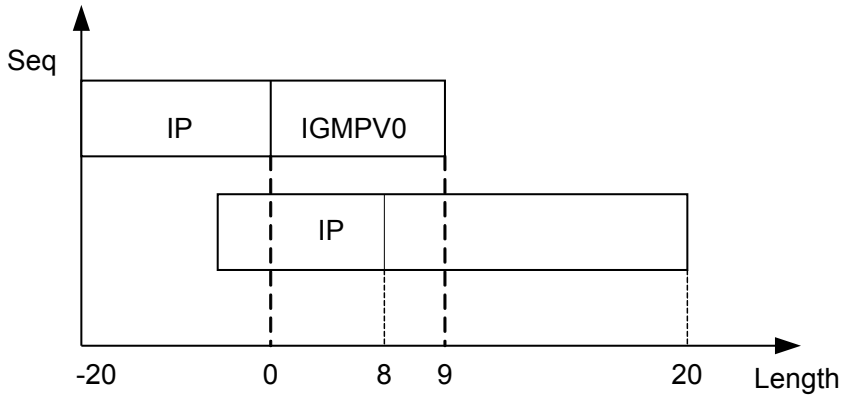


Rose attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all the fragments of Rose attacks.

Fawx Attack

Fawx attack uses error fragments of IGMP packets. As shown in **Figure 7-42**, two fragments of an IGMP packet is sent. In the first fragment, the IP payload is 9 bytes. In the second fragment, the offset is 8, and the IP payload is 16 bytes.

Figure 7-42 Fawx attack



Fawx attacks cause system breakdown or restart. After defense against packet fragment attacks is enabled, the device discards all the fragments of Fawx attacks.

Ping of Death Attack

An attacker sends ICMP packets with the Data field longer than 65507 bytes to attack the device. If the device incorrectly processes ICMP packets with the Data field longer than 65507 bytes, the protocol stack may crash.

After defense against packet fragment attacks is enabled, the device discards ICMP packets with the Data field longer than 65507 bytes.

Jolt Attack

An attacker sends packets longer than 65535 bytes to attack the device. Jolt attack uses 173 packet fragments. The IP payload of each packet fragment is 380 bytes. The total length is 65760 (173 x 380 + 20) bytes, which is greater than 65535. If the device incorrectly processes such packets, the device may stop responding, crash, or restart.

After defense against packet fragment attacks is enabled, the device discards Jolt attack packets.

7.5.2.3 Defense Against Flood Attacks

If an attacker sends a large number of bogus packets to the target host, the target host is busy with these bogus packets and cannot process normal services.

Defense against flood attacks allows the device to detect flood packets in real time and discard them or limit the rate of the packets to protect the device.

Flood attacks include TCP SYN flood attacks, UDP flood attacks, and ICMP flood attacks.

TCP SYN Flood Attack

TCP SYN flood attack uses vulnerability of TCP three-way handshake. During TCP three-way handshake, when receiving the first SYN message from a sender, the receiver sends an SYN +ACK message. When the receiver is waiting for the final ACK packet from the sender, the connection is in half-connected mode. If the receiver does not receive the ACK packet, the receiver retransmits a SYN+ACK packet to the sender. If the receiver does not receive the ACK message from the sender after many attempts, the receiver shuts down the session and then updates the session in the memory. The period from the time to send the first SYN+ACK message to the session teardown time is about 30s.

During this period, an attacker may send thousands of SYN messages to the started interfaces and does not respond to the SYN+ACK message from the receiver. The memory of the receiver is overloaded and the receiver cannot accept any new connection requests. Then the receiver disconnects all existing connections.

After defense against TCP SYN flood attacks is enabled, the device limits the rate of TCP SYN packets so that system resources are not exhausted upon attacks.

UDP Flood Attack

If an attacker sends a large number of UDP packets to the target host, the target host is busy with these UDP packets. As a result, the target host is overloaded and cannot process normal services. UDP flood attacks are classified into two types:

- Fraggle attack

  An attacker sends UDP packets of which the source address is the target host address, the destination address is the broadcast address of the target network, and the destination port number is port 7. If multiple hosts use UDP echo services on the broadcast network, the target host receives excess response packets. As a result, the system becomes busy.

  The device considers packets from UDP port 7 as attack packets and directly discards them.

- UDP diagnosis port attack

  An attacker sends many packets to the UDP diagnosis port (7-echo, 13-daytime, and 19-Chargen) simultaneously, packets are flooded and network devices cannot work properly.

The device considers packets from UDP ports 7, 13, and 19 as attack packets and directly discards them.

ICMP Flood Attack

Generally, a network administrator monitors a network and rectifies network faults with the ping tool as follows:

- The source host sends an ICMP Echo message to the destination host.
- When receiving the ICMP Echo message, the destination host sends an ICMP Echo Reply message to the source host.

If an attacker sends many ICMP Echo messages to the target host, the target host is busy with these Echo messages and cannot process other data packets. Therefore, normal services are affected.

The device limits the rate of packets of ICMP flood attacks to protect the CPU and ensure that the network can work properly.

7.5.3 Default Configuration

This section provides default settings of attack defense.

Table 7-32 describes the default settings of attack defense.

Table 7-32 Default settings of attack defense

Parameter	Default Setting
Defense against malformed packet attacks	Enabled
Defense against packet fragment attacks	Enabled
Rate at which packet fragments are sent	155000000 bit/s
Defense against TCP SYN flood attacks	Enabled
Rate at which TCP SYN flood packets are sent	155000000 bit/s
Defense against UDP flood attacks	Enabled
Defense against ICMP flood attacks	Enabled
Rate at which ICMP flood packets are sent	155000000 bit/s

7.5.4 Configuring Attack Defense

This section describes the procedures for configuring attack defense.

7.5.4.1 Configuring Defense Against Malformed Packet Attacks

Malformed packet attacks include flood attacks without IP payloads, attacks from IGMP null payload packets, LAND attacks, Smurf attacks, and attacks from packets with invalid TCP flag bits.

Context

The malformed packet attack is to send malformed IP packets to the system. If such an attack occurs, the system may break down when processing the malformed IP packets.

To prevent the system from breaking down and to ensure normal network services, enable defense against malformed packet attacks. After detecting malformed packets, the device directly discards them.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
anti-attack abnormal enable
```

Defense against malformed packet attacks is enabled.

By default, defense against malformed packet attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including malformed packets.

----End

Checking the Configuration

- Run the **display anti-attack statistics abnormal** command to check statistics on defense against malformed packet attacks.

7.5.4.2 Configuring Defense Against Packet Fragment Attacks

Packet fragment attacks include attacks from many fragments, attacks from many packets with offsets, attacks from repeated packet fragments, Tear Drop attacks, Syndrop attacks, NewTear attacks, Bonk attacks, Nesta attacks, Rose attacks, Fawx attacks, Ping of Death attacks, and Jolt attacks.

Context

If an attacker sends error packet fragments to attack the device, the device consumes a large number of resources to process the error packet fragments, affecting normal services.

To prevent the system from breaking down and to ensure normal network services, enable defense against packet fragment attacks. The device limits the rate of fragment packets to ensure that the CPU runs properly when the device is being attacked by many packet fragments.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
anti-attack fragment enable
```

Defense against packet fragment attacks is enabled.

By default, defense against packet fragment attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including packet fragments.

Step 3 Run:

```
anti-attack fragment car cir cir
```

The rate limit of packet fragments is set.

By default, the rate limit of packet fragments is 155000000 bit/s.

----End

Checking the Configuration

- Run the **display anti-attack statistics fragment** command to check statistics on defense against packet fragment attacks.

7.5.4.3 Configuring Defense Against Flood Attacks

Flood attacks include TCP SYN flood attacks, UDP flood attacks, and ICMP flood attacks.

7.5.4.3.1 Configuring Defense Against TCP SYN Flood Attacks

Context

An attacker sends a SYN packet to the target host to initiate a TCP connection but does not respond to the SYN+ACK sent from the target host. If the target host receives no ACK packet from the attacker, the device keeps waiting for the ACK packet. A half-open connection is formed. The attacker keeps sending SYN packets, so many half-open connections are set up on the target host. This wastes a large number of resources.

To prevent TCP SYN flood attacks, enable defense against TCP SYN flood attacks and set the rate limit of TCP SYN flood attack packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
anti-attack tcp-syn enable
```

Defense against TCP SYN flood attacks is enabled.

By default, defense against TCP SYN flood attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including TCP SYN flood attack packets.

Step 3 Run:

```
anti-attack tcp-syn car cir cir
```

The rate limit at which TCP SYN packets are received is set.

By default, the rate limit at which TCP SYN packets are received is 155000000 bit/s.

----End

7.5.4.3.2 Configuring Defense Against UDP Flood Attacks

Context

If an attacker sends a large number of UDP packets with specified destination port numbers to the target host in a short time, the target host is busy with these UDP packets. As a result, the target host is overloaded and cannot process normal services. To prevent UDP flood attacks,enable defense against UDP flood attacks.

The device enabled with defense against UDP flood attacks directly discards UDP packets with port numbers 7, 13, and 19.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
anti-attack udp-flood enable
```

Defense against UDP flood attacks is enabled.

By default, defense against UDP flood attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including UDP flood attack packets.

----End

7.5.4.3.3 Configuring Defense Against ICMP Flood Attacks

Context

If an attacker sends a large number of ICMP request packets to the target host in a short time, the target host is busy with these ICMP request packets. As a result, the target host is overloaded and cannot process normal services. To prevent ICMP flood attacks, enable defense against ICMP flood attacks.

After defense against ICMP flood attacks is enabled, set the rate limit of ICMP flood attack packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
anti-attack icmp-flood enable
```

Defense against ICMP flood attacks is enabled.

By default, defense against ICMP flood attacks is enabled.

NOTE

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including ICMP flood attack packets.

Step 3 Run:

```
anti-attack icmp-flood car cir cir
```

The rate limit of ICMP flood attack packets is set.

By default, the rate limit of ICMP flood attack packets is 155000000 bit/s.

----End

7.5.4.3.4 Checking the Configuration

Procedure

- Run the **display anti-attack statistics** [**tcp-syn** | **udp-flood** | **icmp-flood**] command to check statistics on defense against flood attacks.

----End

7.5.5 Maintaining Attack Defense

This section describes how to maintain attack defense, including clearing attack defense statistics.

7.5.5.1 Clearing Attack Defense Statistics

Context

NOTICE

Statistics cannot be restored after being cleared. Exercise caution when you run the reset command.

To clear attack defense statistics, run the following command.

Procedure

- Run the **reset anti-attack statistics** [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood**] command to clear attack defense statistics.

----End

7.5.6 References

This section lists references of Attack defense.

None.

7.6 Traffic Suppression Configuration

This chapter describes basic concepts, configuration procedures and examples, and common configuration errors.

7.6.1 Overview

This section describes the definition, and functions of traffic suppression.

Definition

Traffic suppression security technologies to control broadcast packets, multicast packets, and unknown unicast packets and prevent broadcast storms caused by these packets.

Traffic suppression limits the traffic by setting a threshold.

NOTE

Unknown unicast packets refer to unicast packets whose destination MAC addresses are not learned by the device.

Purpose

When receiving broadcast packets, multicast packets, and unknown unicast packets, the device forwards the packets to other Layer 2 Ethernet interfaces in the same VLAN if the device cannot determine the outbound interface based on destination MAC addresses of packets. In this case, broadcast storms may occur on the network and forwarding performance of the device deteriorates.

Traffic suppression can control these packets and prevent broadcast storms.

7.6.2 Principles

This section describes the implementation of traffic suppression.

7.6.2.1 Traffic Suppression

Traffic suppression prevents broadcast storms caused by broadcast packets, multicast packets, and unknown unicast packets in the following modes:

- The device performs traffic suppression for these packets per second on the inbound interface.

  The device detects rates of these packets and compares the rates with the thresholds. When the inbound traffic reaches the threshold, the system discards excess traffic.

7.6.3 Configuration Notes

This section describes the precautions for traffic suppression configuration.

Features Supported by the Device

Table 7-33 lists traffic suppression supported by the device.

Table 7-33 Features supported by the device

View	Traffic Suppression Features Supported by the Device
Interface view	● Traffic suppression for broadcast packets, multicast packets, and unknown unicast packets
Service set view	Traffic suppression for broadcast packets, multicast packets, and unknown unicast packets in a VAP when the WLAN service is configured

7.6.4 Default Configuration

This section describes the default configuration of traffic suppression of the device.

Table 7-34 lists default parameter settings of traffic suppression and storm control.

Table 7-34 Traffic suppression

Parameter	Default Value
Traffic suppression	Disabled
Traffic suppression for Internet Control Message Protocol (ICMP) packets	Disabled **NOTE** The device does not support traffic suppression for ICMP packets from STAs.
Traffic suppression threshold for ICMP Packets	100 pps

7.6.5 Configuring Traffic Suppression

Traffic suppression prevents broadcast storms and ensures device forwarding performance.

7.6.5.1 Configuring Traffic Suppression on an Interface

Context

To limit the rate of incoming and outgoing packets and prevent broadcast storms, configure traffic suppression on an interface.

Pre-configuration Tasks

Before configuring traffic suppression on an interface, complete the following task:

- Configuring link layer protocol parameters for interfaces to ensure that the link layer protocol status on the interfaces is Up

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
{ broadcast-suppression | multicast-suppression | unicast-suppression } packets packets-per-second
```

Traffic suppression is configured.

----End

7.6.5.2 Configuring Traffic Suppression on an VAP

Context

When using the WLAN service, you can configure traffic suppression of packets of certain types in a service set to limit the rates of broadcast packets, multicast packets, and unknown unicast packets in a VAP and to prevent broadcast storms.

Pre-configuration Tasks

Before configuring traffic suppression on an VAP, complete the following task:

- Configuring basic WLAN services so that wireless users can go online

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
service-set { name service-set-name | id service-set-id } *
```

The service set view is displayed.

Step 4 Run:

```
{ broadcast-suppression | multicast-suppression | unicast-suppression } packets packets-per-second
```

Traffic suppression is configured.

----End

7.6.5.3 Limiting the Rate of ICMP Packets

Applicable Environment

The device receives a large number of ICMP packets from the network, and these packets consume a lot of CPU resources. Limiting the rate at which ICMP packets are received can help reduce the burden of the CPU, ensuring nonstop service transmission. After this function is configured, the device discards excess packets.

NOTE

After rate limiting of ICMP packets is configured, the device may fail to respond to ping packets. To make suppression of ICMP packets take effect, disable the fast ICMP reply function.

Procedure

- Configuring the global rate limit for ICMP packets
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     icmp rate-limit enable

     The global ICMP packet rate limiting function is enabled.

     By default, the global ICMP packet rate limiting function is disabled on an device.
  3. (Optional) Run:
     icmp rate-limit threshold *threshold-value*

     The global rate limit for ICMP packets is set.

     By default, the global rate limit for ICMP packets is 100 pps.
- Configuring the rate limit for ICMP packets on a specified interface
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.

     The AP can limit the rate at which ICMP packets are received on GE interfaces and Eth-Trunk interfaces.
  3. Run:
     icmp rate-limit enable

     The ICMP packet rate limiting function is enabled on the interface.

     By default, the ICMP packet rate limiting function is disabled on an device.
  4. (Optional) Run:
     icmp rate-limit threshold *threshold-value*

     The highest rate at which ICMP packets are received on the interface is set.

     By default, the rate limit for ICMP packets on an interface is 100 pps.

----End

7.6.5.4 Checking the Configuration

Procedure

- Run the **display flow-suppression interface** *interface-type interface-number* command to check the traffic suppression configuration.

----End

7.6.6 Example for Configuring Traffic Suppression and Storm Control

This section provides traffic suppression and storm control examples.

7.6.6.1 Example for Configuring WLAN Rate Limit for Traffic Suppression

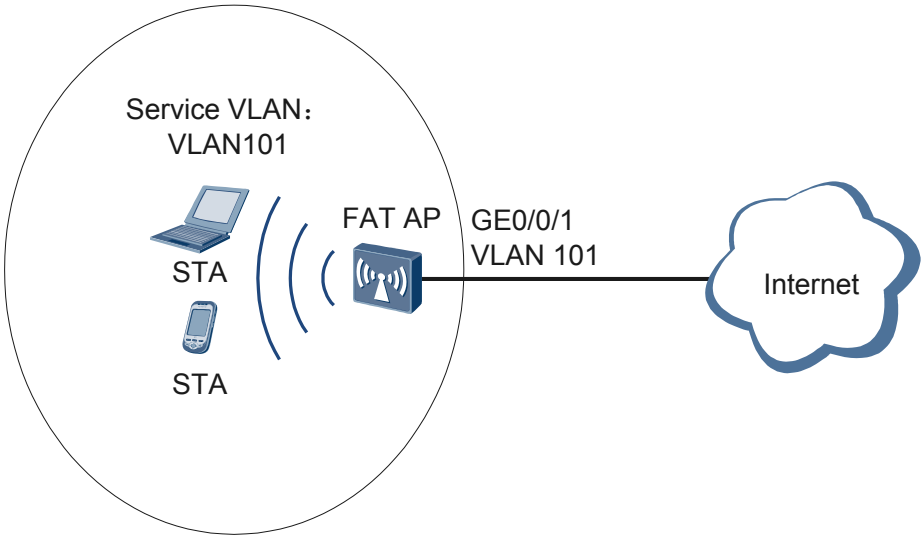
Networking Requirements

As shown in **Figure 7-43**, an enterprise branch deploys WLAN services for mobile office so that branch users can access the enterprise internet network from anywhere at any time. If a user sends a large number of broadcast, multicast, or unknown unicast packets, broadcast storms may occur on the Layer 2 network, which causes network congestion. In such a case, you can configure traffic suppression on VAPs.

Deployed WLAN services include the following:

- A wireless network with SSID **test** is provided. The security policy is set to no authentication and no encryption.
- Branch users are assigned IP addresses on 192.168.11.0/24.

Figure 7-43 Network diagram of Setting the WLAN Rate Limit for Traffic Suppression



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a rate limit for broadcast, multicast, and unknown unicast packets in a service set to prevent network storms.

Procedure

Step 1 Configure traffic suppression.

```
<AP> system-view
[AP] wlan
[AP-wlan-view] service-set name test
[AP-wlan-service-set-test] broadcast-suppression packets 20000
[AP-wlan-service-set-test] multicast-suppression packets 20000
[AP-wlan-service-set-test] unicast-suppression packets 20000
[AP-wlan-service-set-test] quit
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
  broadcast-suppression packets 20000
  multicast-suppression packets 20000
  unicast-suppression packets 20000
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

7.6.7 References

This section lists references of traffic suppression.

Document	Description	Remarks
IEEE 802.1d	Media Access Control (MAC) Bridges Specifies an architecture and protocol for the interconnection of IEEE802 LANs below the MAC service boundary.	-

7.7 ARP Security Configuration

This chapter describes the principle and configuration methods of ARP security and provides configuration examples.

7.7.1 Overview

This section describes the definition and functions of ARP Security.

Definition

Address Resolution Protocol (ARP) security prevents ARP attacks and ARP-based network scanning attacks using a series of methods such as strict ARP learning, dynamic ARP inspection (DAI), ARP anti-spoofing, and rate limit on ARP packets.

Purpose

ARP is easy to use but has no security mechanisms. Attackers often use ARP to attack network devices. The following ARP attack modes are commonly used on networks:

- ARP flood attack: ARP flood attacks, also called denial of service (DoS) attacks, occur in the following scenarios:
  - System resources are consumed when the device processes ARP packets and maintains ARP entries. To ensure that ARP entries can be queried efficiently, a maximum number of ARP entries is set on the device. Attackers send a large number of bogus ARP packets with variable source IP addresses to the device. In this case, APR entries on the device are exhausted and the device cannot generate ARP entries for ARP packets from authorized users. Consequently, communication is interrupted.
  - When attackers scan hosts on the local network segment or other network segments, the attackers send many IP packets with unresolvable destination IP addresses to attack the device. As a result, the device triggers many ARP Miss messages, generates a large number of temporary ARP entries, and broadcasts ARP Request packets to resolve the destination IP addresses, leading to Central Processing Unit (CPU) overload.
- ARP spoofing attack: An attacker sends bogus ARP packets to network devices. The devices then modify ARP entries, causing communication failures.

ARP attacks cause the following problems:

- Network connections are unstable and communication is interrupted, leading to economic loss.
- Attackers initiate ARP spoofing attacks to intercept user packets to obtain accounts and passwords of systems such as the game, online bank, and file server, leading to losses.

To avoid the preceding problems, the device provides multiple techniques to defend against ARP attacks.

Table 7-35 describe various ARP security techniques for defending against different ARP attacks.

Table 7-35 ARP security techniques for defending against ARP flood and spoofing attacks

Attack Type	Attack Defense Function	Description	Deployment
ARP flood attack	Rate limit on ARP packets	This function limits the rate of ARP packets, ensuring that the device has sufficient CPU resources to process other services when processing a large number of ARP packets.	You are advised to enable this function on the gateway.
	Rate limit on ARP Miss messages	This function limits the rate of ARP Miss messages to defend against attacks from a large number of IP packets with unresolvable destination IP addresses.	You are advised to enable this function on the gateway.
	Strict ARP learning	This function allows the device to learn only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself. This prevents ARP entries from being exhausted for invalid ARP packets.	You are advised to enable this function on the gateway.
	ARP entry limiting	This function enables a device interface to dynamically learn a maximum number of ARP entries, preventing ARP entries from being exhausted when a host connected to the interface attacks the device.	You are advised to enable this function on the gateway.
ARP spoofing attack	ARP entry fixing	After the device with this function enabled learns an ARP entry for the first time, it does not change the ARP entry, only updates part of the entry, or sends a unicast ARP Request packet to check validity of the ARP packet for updating the entry. The device supports three ARP entry fixing modes: **fixed-all**, **fixed-mac**, and **send-ack**.	You are advised to enable this function on the gateway.

Attack Type	Attack Defense Function	Description	Deployment
	DAI	Dynamic ARP inspection (DAI) allows the device to compare the source IP address, source MAC address, interface number, and VLAN ID of an ARP packet with a binding entry. If an entry is matched, the device considers the ARP packet valid and allows the packet to pass through. If no entry is matched, the device considers the ARP packet invalid and discards the packet. This function is available only for DHCP snooping scenarios. To configure dynamic ARP detection for the AP to which STAs connect, see **4.6.3.7 Configuring a WLAN Service Set**.	You are advised to enable this function on an access device.
	Gratuitous ARP packet sending	This function allows the device used as the gateway to periodically send ARP Request packets with its IP address as the destination IP address to update the gateway MAC address in ARP entries. This function ensures that packets of authorized users are forwarded to the gateway and prevents hackers from intercepting these packets.	You are advised to enable this function on the gateway.
	MAC address consistency check in an ARP packet	This function defends against attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header.	You are advised to enable this function on the gateway.
	ARP packet validity check	This function allows the device to filter out packets in which the source MAC addresses are different from those in the Ethernet frame header.	You are advised to enable this function on the gateway or an access device.

Attack Type	Attack Defense Function	Description	Deployment
	Strict ARP learning	This function allows the device to learn only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself. This prevents the device from incorrectly updating ARP entries for the received bogus ARP packets.	You are advised to enable this function on the gateway.
	ARP learning triggered by DHCP	This function allows the device to generate ARP entries based on received DHCP ACK messages. When there are a large number of DHCP users, the device needs to learn many ARP entries and age them. This affects device performance. This function prevents this problem. You can also deploy DAI to prevent ARP entries of DHCP users from being modified maliciously.	You are advised to enable this function on the gateway.

Benefits

- Reduces maintenance costs for network operating and security.
- Provides users with stable services on a secure network.

7.7.2 Principles

This section describes the implementation of ARP Security.

7.7.2.1 Rate Limit on ARP Packets

The device has no sufficient CPU resource to process other services when processing a large number of ARP packets. To protect CPU resources of the device, limit the rate of ARP packets.

The device provides the following mechanisms for limiting the rate of ARP packets:

- Limiting the rate of ARP packets based on the source MAC address or source IP address

  When detecting that a host sends a large number of ARP packets in a short period, the device limits the rate of ARP packets sent from this host based on the source MAC address or source IP address. If the number of ARP packets received within 1 second exceeds the threshold, the device discards the excess ARP packets.

  - Limiting the rate of ARP packets based on the source MAC address: If a MAC address is specified, the device applies the rate limit to ARP packets from this source MAC address; otherwise, the device applies the rate limit to all ARP packets.
  - Limiting the rate of ARP packets based on the source IP address: If an IP address is specified, the device applies the rate limit to ARP packets from this source IP address; otherwise, the device applies the rate limit to all ARP packets.
- Limiting the rate on ARP packets globally or on an interface

  The maximum rate and rate limit duration of ARP packets can be set globally or on an interface. The configurations on an interface and globally takes effect in descending order of priority.
  - Limiting the rate of ARP packets globally: limits the number of ARP packets to be processed by the system. When an ARP attack occurs, the device limits the rate of ARP packets globally.
  - Limiting the rate of ARP packets on an interface: limits the number of ARP packets to be processed on an interface. The configuration on an interface does not affect ARP entry learning on other interfaces.

7.7.2.2 Rate Limit on ARP Miss Messages

If a host sends a large number of IP packets with unresolvable destination IP addresses to attack a device, that is, if the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route, the device triggers a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the master control board for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

To avoid the preceding problems, the device provides multiple techniques to limit the rate on ARP Miss messages.

- Limiting the rate of ARP Miss messages based on the source IP address

  If the number of ARP Miss messages triggered by IP packets from a source IP address in 1 second exceeds the limit, the device considers that an attack is initiated from the source IP address.

  If a source IP address is specified, the rate of ARP Miss messages triggered by IP packets from the source IP address is limited. If no source IP address is specified, the rate of ARP Miss messages triggered by IP packets from each source IP address is limited.
- Limiting the rate of ARP Miss messages globally

  The device can limit the number of ARP Miss messages processed by the system.
- Limiting the rate of ARP Miss messages by setting the aging time of temporary ARP entries

  When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.
  - In the aging time of temporary ARP entries:
    - An IP packet that is received before the ARP Reply packet and matches a temporary ARP entry is discarded and triggers no ARP Miss message.
    - After receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.

- When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages are triggered again and temporary ARP entries are regenerated. This process continues.

When ARP Miss attacks occur on the device, you can extend the aging time of temporary ARP entries and reduce the frequency of triggering ARP Miss messages to minimize the impact on the device.

7.7.2.3 Strict ARP Learning

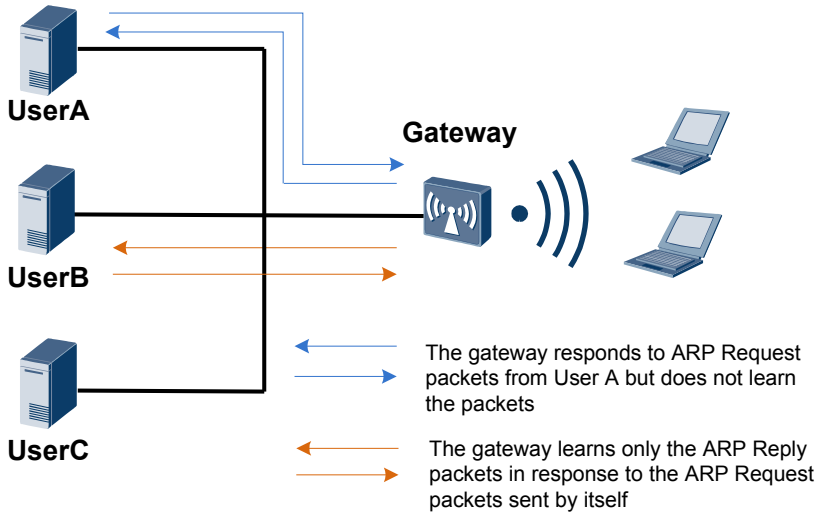
If many users send a large number of ARP packets to a device at the same time, or attackers send bogus ARP packets to the device, the following problems occur:

- Many CPU resources are consumed to process a large number of ARP packets. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- Bogus ARP packets modify ARP entries on the device. As a result, the device cannot communicate with other devices.

To avoid the preceding problems, deploy the strict ARP learning function on the gateway.

After strict ARP learning function is enabled, the device learns only ARP entries for ARP reply packets in response to ARP request packets sent by itself. In this way, the device can defend against most ARP attacks.

Figure 7-44 Strict ARP learning



As shown in **Figure 7-44**, after receiving an ARP Request packet from UserA, the gateway sends an ARP Reply packet to UserA and adds or updates an ARP entry matching UserA. After the strict ARP learning function is enabled on the gateway:

- When receiving an ARP Request packet from UserA, the gateway adds or updates no ARP entry matching UserA. If the ARP Request packet requests the MAC address of the gateway, the gateway sends an ARP Reply packet to UserA.

- If the gateway sends an ARP Request packet to UserB, the gateway adds or updates an ARP entry matching UserB after receiving the ARP Reply packet.

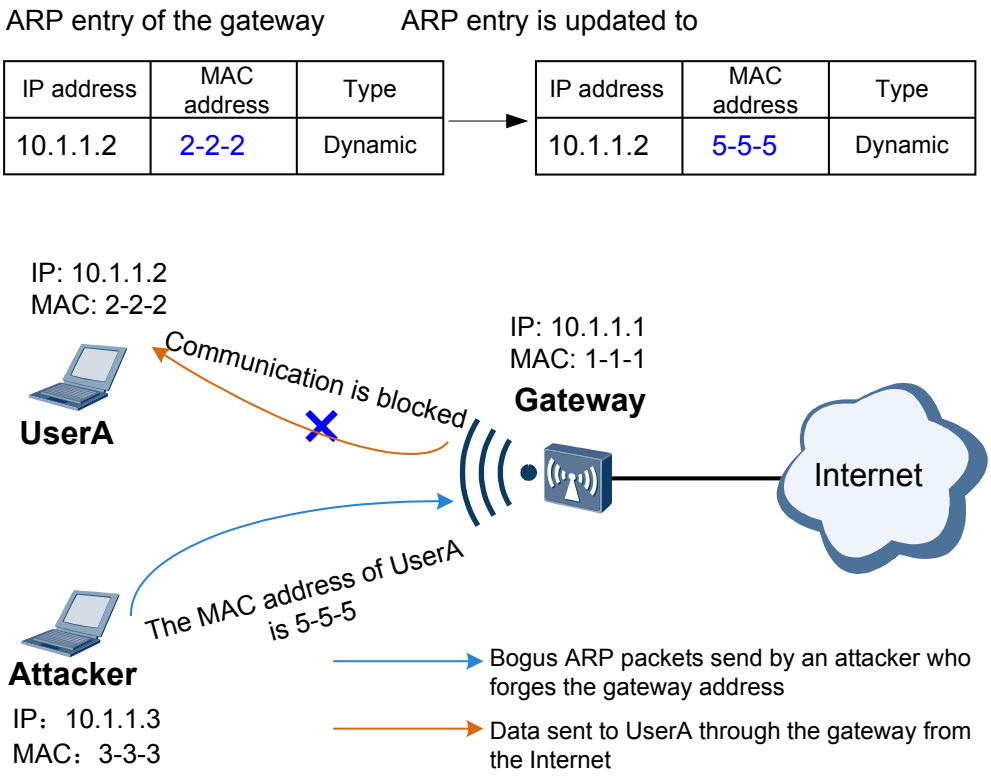
7.7.2.4 ARP Entry Limiting

The ARP entry limiting function controls the number of ARP entries that a gateway interface can learn. By default, the number of ARP entries that an interface can dynamically learn is the same as the default number of ARP entries supported by the device. After the ARP entry limiting function is deployed, if the number of ARP entries that a specified interface dynamically learned reaches the maximum, the interface cannot learn any ARP entry. This prevents ARP entries from being exhausted when a host connecting to this interface initiates ARP attacks.

7.7.2.5 ARP Entry Fixing

As shown in **Figure 7-45**, an attacker simulates UserA to send a bogus ARP packet to the gateway. The gateway then records an incorrect ARP entry for UserA. As a result, UserA cannot communicate with the gateway.

Figure 7-45 ARP gateway spoofing attack



To defend against ARP gateway spoofing attacks, deploy the ARP entry fixing function on the gateway. After the gateway with this function enabled learns an ARP entry for the first time, it does not change the ARP entry, only updates part of the entry, or sends a unicast ARP Request packet to check validity of the ARP packet for updating the entry.

The device supports three ARP entry fixing modes, as described in **Table 7-36**.

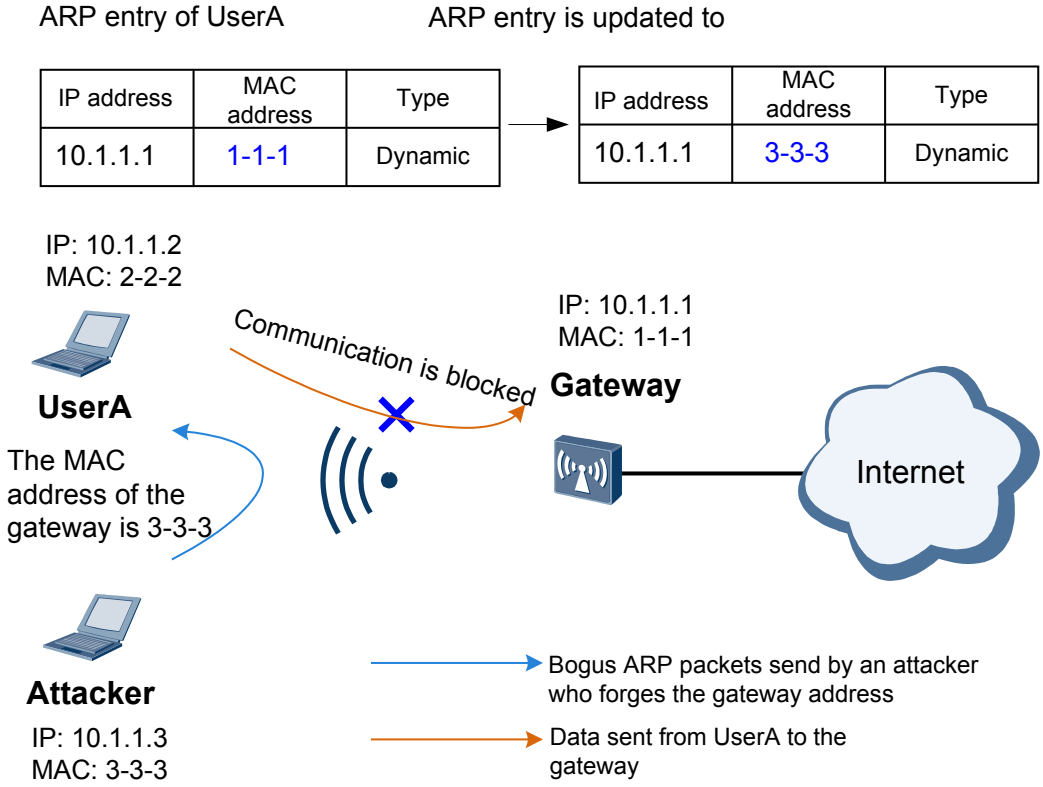
Table 7-36 ARP entry fixing modes

Mode	Description
fixed-all	When receiving an ARP packet, the device discards the packet if the MAC address, interface number, or VLAN ID matches no ARP entry. This mode applies to networks that use static IP addresses and have no redundant link.
fixed-mac	When receiving an ARP packet, the device discards the packet if the MAC address does not match the MAC address in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry. This mode applies to networks where users need to change access interfaces.
send-ack	When the device receives ARP packet A with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user. ● If the device receives ARP Reply packet B within 3 seconds, and the IP address, MAC address, interface number, and VLAN ID of the ARP entry are the same as those in ARP Reply packet B, the device considers ARP packet A as an attack packet and does not update the ARP entry. ● If the device receives no ARP Reply packet within 3 seconds or the IP address, MAC address, interface number, and VLAN ID of the ARP entry are different from those in ARP Reply packet B, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address again. – If the device receives ARP Reply packet C within 3 seconds, and the IP address, MAC address, interface number, and VLAN ID of the ARP packet A are the same as those in ARP Reply packet C, the device considers ARP packet A as a valid packet and update the ARP entry based on ARP packet A. – If the device receives no ARP Reply packet within 3 seconds or the IP address, MAC address, interface number, and VLAN ID of ARP packet A are different from those in ARP Reply packet C, the device considers ARP packet A as an attack packet and does not update the ARP entry. This mode applies to networks that use dynamic IP addresses and have redundant links.

7.7.2.6 Gratuitous ARP Packet Sending

As shown in **Figure 7-46**, an attacker forges the gateway address to send a bogus ARP packet to UserA. UserA then records an incorrect ARP entry for the gateway. As a result, the gateway cannot receive packets from UserA.

Figure 7-46 Bogus gateway attack



To avoid the preceding problem, deploy gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

7.7.2.7 MAC Address Consistency Check in an ARP Packet

This function defends against attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header.

This function enables the gateway to check the MAC address consistency in an ARP packet before ARP learning. If the source and destination MAC addresses in an ARP packet are different from those in the Ethernet frame header, the device discards the packet as an attack. If the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header, the device performs ARP learning.

7.7.2.8 ARP Packet Validity Check

After receiving an ARP packet, the device checks validity of the ARP packet, including:

- Packet length
- Validity of the source and destination MAC addresses in the ARP packet
- ARP Request type and ARP Reply type
- MAC address length
- IP address length
- Whether the ARP packet is an Ethernet frame

The preceding check items are used to determine whether an ARP packet is valid. The packet with different source MAC addresses in the ARP packet and Ethernet frame header is possibly an attack packet although it is allowed by the ARP protocol.

After ARP packet validity check is enabled on the gateway or an access device, the device checks the source MAC addresses in the ARP packet and Ethernet frame header, and discards the packets with inconsistent source MAC addresses.

7.7.3 Default Configuration

This section describes the ARP security default configuration. You can change the configuration based on the site requirements.

Table 7-37 describes the default ARP security configuration.

Table 7-37 Default ARP security configuration

Parameter	Default Setting
Rate limit on ARP packets based on the source MAC address	If the rate of ARP packets from each source MAC address is set to 0, the rate of ARP packets is not limited based on the source MAC address.
Rate limit on ARP packets based on the source IP address	The device allows a maximum of 5 ARP packets from the same source IP address to pass through in 1 second.
Rate limit on ARP packets globally or on an interface	Disabled
Maximum rate and rate limit duration of ARP packets globally or on an interface	The device allows a maximum of 100 ARP packets to pass through in 1 second.
Alarm of ARP packets discarded when the rate limit is exceeded globally or on an interface	Disabled
Alarm threshold of ARP packets discarded when the rate limit is exceeded globally or on an interface	100
Maximum rate of broadcasting ARP Request packets on the VLANIF interface of the super-VLAN	1000 pps

Parameter	Default Setting
Rate limit on ARP Miss messages based on the source IP address	The device can process a maximum of 5 ARP Miss messages triggered by IP packets from the same source IP address.
Rate limit on ARP Miss messages globally	Disabled
Maximum rate and rate limit duration of ARP Miss messages globally	The device can process a maximum of 100 ARP Miss messages in 1 second.
Alarm of ARP Miss messages discarded when the rate limit is exceeded globally	Disabled
Alarm threshold of ARP Miss messages discarded when the rate limit is exceeded globally	100
Aging time of temporary ARP entries	1 second
Strict ARP learning	Disabled
Interface-based ARP entry limit	The maximum number of ARP entries that an interface can dynamically learn is the same as the number of ARP entries supported by the device.
ARP entry fixing	Disabled
Gratuitous ARP packet sending	Disabled
Interval for sending gratuitous ARP packets	90 seconds
MAC address consistency check in an ARP packet	Disabled
ARP packet validity check	Disabled

7.7.4 Configuring ARP Security

This section describes the procedures for configuring ARP security.

7.7.4.1 Configuring Defense Against ARP Flood Attacks

Configuring defense against ARP flood attacks prevents ARP entries from being exhausted and CPU overload, ensures user communication.

Pre-configuration Tasks

Before configuring defense against ARP flood attacks, complete the following task:

- Connecting interfaces and setting physical parameters for the interfaces to ensure that the physical status of the interfaces is Up

Configuration Process

Operations in the configuration process can be performed in any sequence as required.

NOTE

When rate limit on ARP packets is configured globally or on an interface and rate limit on ARP packets based on the source MAC address or source IP address is also configured, the smallest rate is used.

When rate limit on ARP Miss messages is configured globally or on an interface and rate limit on ARP Miss messages based on the source MAC address or source IP address is also configured, the smallest rate is used.

7.7.4.1.1 Configuring Rate Limit on ARP Packets based on the Source MAC Address

Context

When processing a large number of ARP packets with fixed source MAC addresses but variable IP addresses, the CPU is overloaded and ARP entries are exhausted.

To prevent this problem, limit the rate of ARP packets based on the source MAC address. The device collects statistics on ARP packets from a specified source MAC address. If the number of ARP packets from the specified source IP address in 1 second exceeds the threshold, the device discards the excess ARP packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configuring rate limit on ARP packets based on the source MAC address

- Run:

  ```
  arp speed-limit source-mac maximum maximum
  ```

  The maximum rate of ARP packets from a source MAC address is set

- Run:

  ```
  arp speed-limit source-mac mac-addrress maximum maximum
  ```

  The maximum rate of ARP packets from a specified source MAC address is set.

When the preceding configurations are both performed, the maximum rate set using the **arp speed-limit source-mac** *mac-address* **maximum** *maximum* command takes effect on ARP packets from the specified source MAC address, and the maximum rate set using the **arp speed-limit source-mac maximum** *maximum* command takes effect on ARP packets from other source MAC addresses.

By default, the maximum rate of ARP packets from each source MAC address is set to 0, that is, the rate of ARP packets is not limited based on the source MAC address.

----End

7.7.4.1.2 Configuring Rate Limit on ARP Packets based on the Source IP Address

Context

When processing a large number of ARP packets with fixed IP addresses, the CPU is overloaded and cannot process other services.

To prevent this problem, limit the rate of ARP packets based on the source IP address. The device collects statistics on ARP packets from a specified source IP address. If the number of ARP packets from the specified source IP address in 1 second exceeds the threshold, the device discards the excess ARP packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configuring rate limit on ARP packets based on the source IP address

- Run:

  ```
  arp speed-limit source-ip maximum maximum
  ```

  The maximum rate of ARP packets from a source IP address is set.

- Run:

  ```
  arp speed-limit source-ip ip-address maximum maximum
  ```

  The maximum rate of ARP packets from a specified source IP address is set.

When the preceding configurations are both performed, the maximum rate set using the **arp speed-limit source-ip** *ip-address* **maximum** *maximum* command takes effect on ARP packets from the specified source IP address, and the maximum rate set using the **arp speed-limit source-ip maximum** *maximum* command takes effect on ARP packets from other source IP addresses.

By default, the device allows a maximum of 5 ARP packets from the same source IP address to pass through in 1 second.

----End

7.7.4.1.3 Configuring Rate Limit on ARP Packets (Globally or on an Interface)

Context

The device has no sufficient CPU resource to process other services when processing a large number of ARP packets. To protect CPU resources of the device, limit the rate of ARP packets.

After rate limit on ARP packets is enabled, set the maximum rate and rate limit duration of ARP packets globally or on an interface. In the rate limit duration, if the number of received ARP packets exceeds the limit, the device discards the excess ARP packets.

- Limiting the rate of ARP packets globally: limits the number of ARP packets to be processed by the system. When an ARP attack occurs, the device limits the rate of ARP packets globally.
- Limiting the rate of ARP packets on an interface: limits the number of ARP packets to be processed on an interface. The configuration on an interface does not affect ARP entry learning on other interfaces.

If the maximum rate and rate limit duration are set globally or on an interface at the same time, the configurations on an interface and globally take effect in descending order of priority.

If you want that the device can generate alarms to notify the network administrator of a large number of discarded excess ARP packets, enable the alarm function. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

NOTE

If the alarm function is enabled, you need to run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending alarms.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 (Optional) Run:

```
interface interface-type interface-number
```

The interface view is displayed.

NOTE

If you configure rate limit on ARP packets in the system view, skip this step.

Step 3 Run:

```
arp anti-attack rate-limit enable
```

Rate limit on ARP packets is enabled.

By default, rate limit on ARP packet is disabled.

Step 4 Run:

```
arp anti-attack rate-limit packet-number [ interval-value ]
```

The maximum rate and rate limit duration of ARP packets are set.

By default, a maximum of 100 ARP packets are allowed to pass in 1 second.

Step 5 (Optional) Run:

```
arp anti-attack rate-limit alarm enable
```

The alarm function for discarded ARP packets when the rate of ARP Miss packets exceeds the limit is enabled.

By default, the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit is disabled.

Step 6 (Optional) Run:

arp anti-attack rate-limit alarm threshold *threshold*

The alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit is set.

By default, the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit is 100.

----End

7.7.4.1.4 Configuring Rate Limit on ARP Miss Messages based on the Source IP Address

Context

If the number of ARP Miss messages triggered by IP packets from a source IP address in 1 second exceeds the limit, the device considers that an attack is initiated from the source IP address.

The administrator can set the maximum number of ARP Miss messages that the device can process within a specified duration based on the actual network environment, protecting the system resources and ensuring proper running of other services.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Configuring rate limit on ARP Miss messages based on the source IP address

- Run:
  arp-miss speed-limit source-ip maximum *maximum*

  The maximum rate of ARP Miss messages from a specified source IP address is set.
- Run:
  arp-miss speed-limit source-ip *ip-address* **maximum** *maximum*

  The maximum rate of ARP Miss messages triggered by IP packets from a specified source IP address is set.

When the preceding configurations are both performed, the maximum rate set using the **arp-miss speed-limit source-ip** *ip-address* **maximum** *maximum* command takes effect on ARP Miss messages triggered IP packets from the specified source IP address, and the maximum rate set using the **arp-miss speed-limit source-ip maximum** *maximum* command takes effect on ARP Miss messages triggered by IP packets from other source IP addresses.

If the maximum rate of ARP Miss messages is set to 0, the rate of ARP Miss messages is not limited based on the source IP address. By default, the device processes a maximum of 5 ARP Miss messages triggered by IP packets from the same source IP address in 1 second.

----End

7.7.4.1.5 Configuring Rate Limit on ARP Miss Messages Globally

Context

If a host sends a large number of IP packets with unresolvable destination IP addresses to attack a device, that is, if the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route, the device triggers a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the master control board for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

To avoid the preceding problems, configure rate limit on ARP Miss messages.

If you want that the device can generate alarms to notify the network administrator of a large number of discarded excess ARP Miss messages, enable the alarm function. When the number of discarded ARP Miss messages exceeds the alarm threshold, the device generates an alarm.

NOTE

If the alarm function is enabled, you need to run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending alarms.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
arp-miss anti-attack rate-limit enable
```

Rate limit on ARP Miss messages is enabled.

By default, rate limit on ARP Miss messages is disabled.

Step 3 Run:

```
arp-miss anti-attack rate-limit packet-number [ interval-value ]
```

The maximum rate and rate limit duration of ARP Miss messages are set.

By default, the device can process a maximum of 100 ARP Miss messages in 1 second.

Step 4 (Optional) Run:

```
arp-miss anti-attack rate-limit alarm enable
```

The alarm function for discarded ARP Miss messages when the rate of ARP Miss packets exceeds the limit is enabled.

By default, the alarm function is disabled.

Step 5 (Optional) Run:

```
arp-miss anti-attack rate-limit alarm threshold threshold
```

The alarm threshold for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit is set.

By default, the alarm threshold is 100.

----End

7.7.4.1.6 Setting the Aging Time of Temporary ARP Entries

Context

When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.

- In the aging time of temporary ARP entries:
  - An IP packet that is received before the ARP Reply packet and matches a temporary ARP entry is discarded and triggers no ARP Miss message.
  - After receiving the ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.
- When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages are triggered again and temporary ARP entries are regenerated. This process continues.

You can limit the rate of ARP Miss messages by setting the aging time of temporary ARP entries. When ARP Miss attacks occur on the device, you can extend the aging time of temporary ARP entries to reduce the frequency of triggering ARP Miss messages so that the impact on the device is minimized.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

The interface type can be GE,or VLANIF.

Step 3 Run:

```
arp-fake expire-time expire-time
```

The aging time of temporary ARP entries is set.

By default, the aging time of temporary ARP entries is 1 second.

----End

7.7.4.1.7 Configuring Strict ARP Learning

Context

If many users send a large number of ARP packets to a device at the same time, or attackers send bogus ARP packets to the device, the following problems occur:

- Many CPU resources are consumed to process a large number of ARP packets. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device

from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.

- Bogus ARP packets modify ARP entries on the device. As a result, authorized users cannot communicate.

To avoid the preceding problems, configure the strict ARP learning function on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself. In this way, the device can defend against most ARP attacks.

Strict ARP learning can be configured in globally or in the interface view.

- If strict ARP learning is enabled globally, all interfaces on the device learn ARP entries strictly.
- If strict ARP learning is enabled in the interface view, only the interface learns ARP entries strictly.

When strict ARP learning is enabled globally and in the interface view simultaneously, the configuration on the interface takes precedence over the global configuration.

NOTE

When strict ARP learning is enabled globally:

- If you run the **arp learning strict force-disable** command on a specified interface, strict ARP learning is forced to be disabled on the interface.
- If you run the **arp learning strict trust** command on a specified interface, strict ARP learning configured globally takes effect on the interface.

Procedure

- Configuring strict ARP learning globally
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     arp learning strict

     Strict ARP learning is enabled globally.

     By default, strict ARP learning is disabled.
- Configuring strict ARP learning on the interface
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     arp learning strict { **force-enable** | **force-disable** | **trust** }

     Strict ARP learning on the interface is enabled.

By default, strict ARP learning is disabled on the interface.

----End

7.7.4.1.8 Configuring Interface-based ARP Entry Limit

Context

To prevent ARP entries from being exhausted by ARP attacks from a host connecting to an interface on the device, set the maximum number of ARP entries that the interface can dynamically learn. When the number of the ARP entries learned by a specified interface reaches the maximum number, no dynamic ARP entry can be added.

Procedure

- Configuring ARP entry limiting on the Ethernet interface
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*

     The interface view is displayed.
  3. Run:
     arp-limit vlan *vlan-id1* [**to** *vlan-id2*] **maximum** *maximum*

     ARP entry limit on the Ethernet interface is configured.
- Configuring ARP entry limit on the VLANIF interface
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface vlanif *vlan-id*

     The VLANIF interface view is displayed.
  3. Run:
     arp-limit maximum *maximum*

     ARP entry limit on the VLANIF interface is configured.

----End

7.7.4.1.9 Checking the Configuration

Procedure

- Run the **display arp anti-attack configuration** { **arp-rate-limit** | **arpmiss-rate-limit** | **arp-speed-limit** | **arpmiss-speed-limit** | **entry-check** | **packet-check** | **all** } command to check the ARP anti-attack configuration.

- Run the **display arp-limit** [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] command to check the maximum number of ARP entries that an interface can learn.
- Run the **display arp learning strict** command to check strict ARP learning globally and on all VLANIF interfaces.

----End

7.7.4.2 Configuring Defense Against ARP Spoofing Attacks

An attacker sends bogus ARP packets to the device or host on a network. The device or hosts modify their ARP entries, leading to packet forwarding failures.

Pre-configuration Tasks

Before configuring defense against ARP spoofing attacks, complete the following task:

- Connecting interfaces and setting physical parameters for the interfaces to ensure that the physical status of the interfaces is Up

Configuration Process

Operations in the configuration process can be performed in any sequence as required.

7.7.4.2.1 Configuring ARP Entry Fixing

Context

To defend against ARP address spoofing attacks, configure ARP entry fixing. The **fixed-mac**, **fixed-all**, and **send-ack** modes are applicable to different scenarios and are mutually exclusive:

- **fixed-mac** mode: When receiving an ARP packet, the device discards the packet if the MAC address does not match that in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry. This mode applies to networks that use static IP addresses and have redundant links. When services are switched on the link, the ARP interface can change rapidly.
- **fixed-all** mode: When the MAC address, interface number, and VLAN ID of an ARP packet match those in the corresponding ARP entry, the device updates other information about the ARP entry. This mode applies to networks that use static IP addresses and have no redundant link, and the scenario where users with the same IP address access the device using the same interface.
- **send-ack** mode: When the device receives an ARP packet with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user. This mode applies to networks that use dynamic IP addresses and have redundant links.

Procedure

Step 1 Configure ARP entry fixing globally

1. Run:
   system-view

   The system view is displayed.
2. Run:
   arp anti-attack entry-check { **fixed-mac** | **fixed-all** | **send-ack** } **enable**

   ARP entry fixing is enabled.

   By default, ARP entry fixing is disabled.

----End

7.7.4.2.2 Configuring Gratuitous ARP Packet Sending

Context

If an attacker forges the gateway address to send ARP packets to other hosts, ARP entries on the hosts record the incorrect gateway address. As a result, the gateway cannot receive data sent from the hosts. You can enable gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

You can configure gratuitous ARP packet sending globally or on a VLANIF interface.

- If gratuitous ARP packet sending is enabled globally, all interfaces have this function enabled by default.
- If gratuitous ARP packet sending is enabled globally and on a VLANIF interface simultaneously, the configuration on the VLANIF interface takes precedence over the global configuration.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 (Optional) Run:
interface vlanif *vlan-id*

The VLANIF interface view is displayed.

NOTE

If you configure gratuitous ARP packet sending in the system view, skip this step.

Step 3 Run:
arp gratuitous-arp send enable

Gratuitous ARP packet sending is enabled.

By default, gratuitous ARP packet sending is disabled.

Step 4 (Optional) Run:

```
arp gratuitous-arp send interval interval-time
```

The interval for sending gratuitous ARP packets is set.

By default, the interval for sending gratuitous ARP packets is 90 seconds.

----End

7.7.4.2.3 Configuring MAC address Consistency Check in an ARP Packet

Context

This function defends against attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header.

This function enables the gateway to check the MAC address consistency in an ARP packet before ARP learning. If the source and destination MAC addresses in an ARP packet are different from those in the Ethernet frame header, the device discards the packet as an attack. If the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header, the device performs ARP learning.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
arp validate { source-mac | destination-mac }*
```

MAC address consistency check in an ARP packet is enabled. This function compares the source and destination MAC addresses in ARP packets with those in the Ethernet frame header.

By default, MAC address consistency check in an ARP packet is disabled.

NOTE

VLANIF interfaces do not support the **arp validate** { **source-mac** | **destination-mac** }* command. When receiving ARP packets, a VLANIF interface checks MAC address consistency based on the rule configured on the member interface.

----End

7.7.4.2.4 Configuring ARP Packet Validity Check

Context

After receiving an ARP packet, the device checks validity of the ARP packet, including:

- Packet length

- Validity of the source and destination MAC addresses in the ARP packet
- ARP Request type and ARP Reply type
- MAC address length
- IP address length
- Whether the ARP packet is an Ethernet frame

The preceding check items are used to determine whether an ARP packet is valid. The packet with different source MAC addresses in the ARP packet and Ethernet frame header is possibly an attack packet although it is allowed by the ARP protocol.

After ARP packet validity check is enabled, the device checks the source MAC addresses in the ARP packet and Ethernet frame header, and discards the packets with inconsistent source MAC addresses.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
arp anti-attack packet-check sender-mac
```

ARP packet validity check is enabled.

By default, ARP packet validity check is disabled.

----End

7.7.4.2.5 Configuring Strict ARP Learning

Context

If many users send a large number of ARP packets to a device at the same time, or attackers send bogus ARP packets to the device, the following problems occur:

- Many CPU resources are consumed to process a large number of ARP packets. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- Bogus ARP packets modify ARP entries on the device. As a result, authorized users cannot communicate.

To avoid the preceding problems, configure the strict ARP learning function on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself. In this way, the device can defend against most ARP attacks.

Strict ARP learning can be configured in globally or in the interface view.

- If strict ARP learning is enabled globally, all interfaces on the device learn ARP entries strictly.

- If strict ARP learning is enabled in the interface view, only the interface learns ARP entries strictly.

When strict ARP learning is enabled globally and in the interface view simultaneously, the configuration on the interface takes precedence over the global configuration.

NOTE

When strict ARP learning is enabled globally:

- If you run the **arp learning strict force-disable** command on a specified interface, strict ARP learning is forced to be disabled on the interface.
- If you run the **arp learning strict trust** command on a specified interface, strict ARP learning configured globally takes effect on the interface.

Procedure

- Configuring strict ARP learning globally
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     arp learning strict
     ```
     Strict ARP learning is enabled globally.

     By default, strict ARP learning is disabled.
- Configuring strict ARP learning on the interface
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     interface interface-type interface-number
     ```
     The interface view is displayed.
  3. Run:
     ```
     arp learning strict { force-enable | force-disable | trust }
     ```
     Strict ARP learning on the interface is enabled.

     By default, strict ARP learning is disabled on the interface.

----End

7.7.4.2.6 Checking the Configuration

Procedure

- Run the **display arp anti-attack configuration** { **arp-rate-limit** | **arpmiss-rate-limit** | **arp-speed-limit** | **arpmiss-speed-limit** | **entry-check** | **packet-check** | **all** } command to check the ARP anti-attack configuration.

- Run the **display arp learning strict** command to check strict ARP learning globally and on all VLANIF interfaces.

----End

7.7.5 ARP Security Maintenance

The section describes the ARP security maintenance, including monitoring ARP running status, clearing statistics on ARP packets, clearing statistics on discarded ARP packets, and configuring the alarm and log functions for potential ARP attacks.

7.7.5.1 Monitoring ARP Running Status

Procedure

- Run:
  display arp packet statistics

  Statistics on ARP-based packets is displayed.

----End

7.7.5.2 Clearing ARP Security Statistics

Context

NOTICE

ARP security statistics cannot be restored after being cleared. Confirm the action before you use the command.

To clear ARP security statistics, run the following commands in the user view:

Procedure

- Run:
  reset arp packet statistics

  Statistics on ARP packets is cleared.
- Run:
  reset arp anti-attack statistics rate-limit { **global** | **interface** *interface-type interface-number* }

  Statistics about ARP packets discarded when the number of ARP packets exceeds the limit is cleared.

----End

7.7.5.3 Configuring the Alarm Function for Potential ARP Attacks

Context

To allow the administrator to learn the ARP running status in real time, define potential attacks, and take measures, the device provides the alarm function for potential ARP attacks. This function records exceptions of ARP running in real time. To avoid excessive alarms when ARP attacks occur, reduce the alarm quantity by setting a proper interval for sending alarms.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
arp anti-attack log-trap-timer time
```

The interval for sending ARP alarms is set.

The default interval for sending alarms is 0, indicating that the device does not send ARP alarms.

----End

7.7.6 References

This section lists references of ARP Security.

The following table lists the references of this document.

Document	Description	Remarks
RFC826	Ethernet Address Resolution Protocol	-
RFC903	Reverse Address Resolution Protocol	-
RFC1027	Using ARP to Implement Transparent Subnet Gateways	-
RFC1042	Standard for the Transmission of IP Datagrams over IEEE 802 Networks	-

7.8 PKI Configuration

Using the PKI function, the device can obtain a digital certificate, which is used to verify the identifies of the two communication parties.

7.8.1 Overview

This section describes the definition, background, and functions of PKI.

Definition

The public key infrastructure (PKI) is a key management platform. It provides key services including encryption and digit certificates and required key and certificate management system

for all network applications. That is, PKI provides information security services using public key theories and technologies. PKI is the core of information security technologies and e-commerce.

Usage Scenarios

The PKI provides network communication and trade (especially e-government and e-commerce) with a set of transparent security services, including identity authentication, confidentiality, and data consistency and non-repudiation.

The PKI technology develops fast and is widely used. The following are common application scenarios of PKI:

1. Virtual private network

   A virtual private network (VPN) is built on a public communications infrastructure. On a VPN, PKI's encryption and digital signature functions can work with network layer security protocols such as Internet Security (IPSec) to help protect data confidentiality.

2. Email security

   PKI also helps ensure confidentiality, integrity, non-repudiation, and authentication of emails. It is the basis of secure email protocols, such as Secure/Multipurpose Internet Mail Extensions (S/MIME) that allows users to send encrypted emails with signatures.

3. Web security

   Before two entities start to exchange data in a server/browser model, they establish a Secure Sockets Layer (SSL) connection. The SSL protocol uses the PKI technology to encrypt data exchanged between the browser and server. The server and browser use digital certificates to authenticate each other. This process is transparent to application layer protocols.

Benefits

- Benefits to users
  - The certificate authentication technology allows users to authenticate network devices to which they connect, ensuring that users connect to secure and legal networks.
  - The encryption technology protects data against tampering and eavesdropping so that data is transmitted securely on networks.
  - The digital signature technology ensures that data is accessible to only authorized devices and users, protecting data privacy.
- Benefits to enterprises
  - PKI prevents unauthorized users from connecting to enterprise networks.
  - PKI establishes secure connections between enterprise branches to ensure data security.

7.8.2 Principles

This section describes the implementation of PKI.

7.8.2.1 PKI Basics

Public Key Encryption Algorithm

Public key encryption algorithm is also called asymmetric encryption algorithm or double-key encryption algorithm. It uses two keys to encrypt and decrypt data respectively.

Public key encryption algorithm uses a pair of keys, namely, a public key and a private key. The public key can be distributed to any user, and the private key is kept secret by the intended data receiver. Data encrypted using one key can be decrypted only by the other key in the key pair.

RSA Key Pair

The digital certificate system depends on the public key system. The RSA encryption system is most widely used in the PKI.

The RSA uses a pair of asymmetric RSA keys, namely, an RSA public key and an RSA private key. When an entity applies for a digital certificate, the request must contain the RSA public key.

The RSA key length (in bits) equals the modulus of the RSA key. A larger modulus provides stronger key security but it takes a longer time to generate keys, and encrypt or decrypt data using the key pair.

Digital Fingerprint

A digital fingerprint is a digit sequence of a fixed length computed by an algorithm. This digit sequence is also called an information digest and is usually obtained from the original data using a one-way hash algorithm.

Digital Signature

Digital signature is the data that the data sender generates by encrypting the digital fingerprint of the original data using the private key.

The data receiver decrypts the digital signature attached in the original data using the sender's public key to obtain the digital fingerprint. Then the receiver matches the obtained digital fingerprint with that obtained in an outband method and determines whether the original data is tampered according to the match result.

Digital Certificate

A digital certificate is a file that is signed by a CA and contains the public key and identity of an entity.A digital certificate associates the identity of an entity with the public key of the entity, providing the basis for implementing secure communication.A certificate is signed by a CA to ensure its legality and authority.

A certificate contains multiple fields, including the name of a certificate issuer, public key of an entity, digital signature of a CA, and certificate validity period.

NOTE

This document involves two types of digital certificates: local certificates and CA certificates. A local certificate is issued by a CA to an entity. A CA certificate is issued to a CA itself. If multiple CAs exist in the PKI system, a CA hierarchy is formed. At the top of the hierarchy is a root CA, which has a self-signed certificate.

Certificate Revocation List

When an entity name is changed, a private key is revealed, or a service is ceased, there must be a method to revoke the certificate of the entity, namely, unbind the public key from the identity of the entity. In the PKI, a certificate revocation list (CRL) is used to revoke certificates.

After a certificate is revoked, the CA must issue a CRL to declare that the certificate is invalid. The CRL lists the serial numbers of all revoked certificates. The CRL provides a method to verify certificate validity.

If a CRL lists many revoked certificates, the CRL size is large, which deteriorates the performance of network resources. To avoid this, a CA issues multiple CRLs and uses CRL distribution points (CDPs) to indicate the location of these CRLs.

CRL Distribution Point

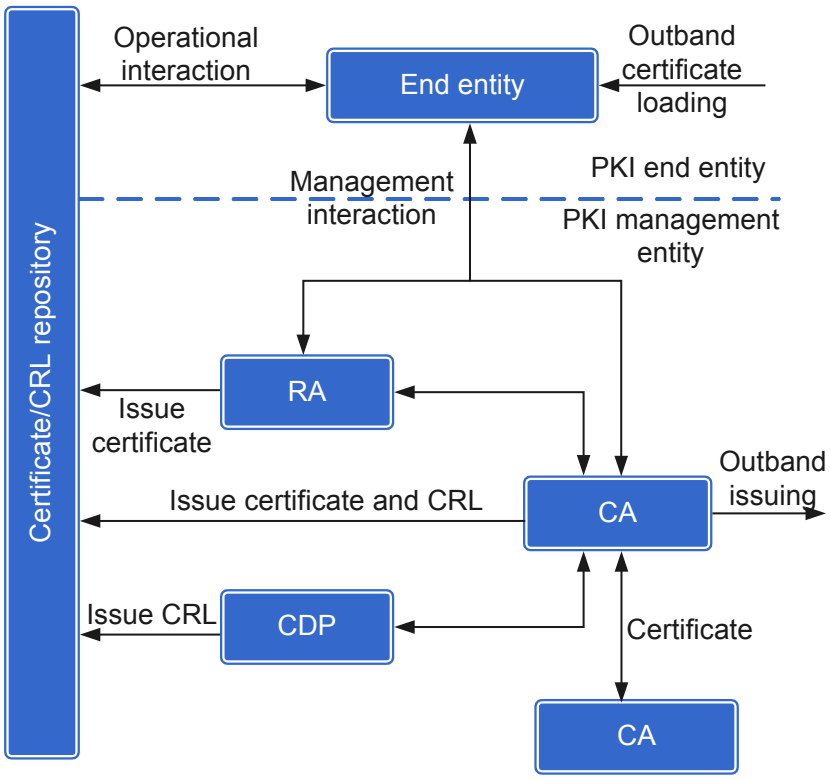
A CRL distribution point (CDP) is a location from which a CRL is obtained. It is specified in a digital certificate. A CDP is a uniform resource locator (URL) in the Hypertext Transfer Protocol (HTTP) or Lightweight Directory Access Protocol (LDAP) format, an LDAP directory, or a URL of another type.

7.8.2.2 PKI System

PKI System Architecture

The PKI system consists of the entity, CA, RA, and Certificate/CRL repository, as shown in **Figure 7-47**.

Figure 7-47 PKI system architecture



- End entity

  An entity is an end user of PKI products or services. An entity can be an individual, an organization, a device (for example, a router or a switch), or a computer process.

- CA

  The CA is the trust basis of the PKI and the trusted entity used to issue and manage digital certificates. A CA is used to issue certificates, specify certificate validity periods, and release CRLs.

- RA

  The registration authority (RA) is the extension of the CA. The RA can be an independent agent or a part of the CA. The RA authenticates individual identities, manages CRLs, and generates and backs up key pairs. The international standard of PKI recommends to use an independent RA to manage registrations, which can improve the security o application systems.

- Certificate/CRL repository

  The certificate or CRL repository stores certificates and CRLs for PKI entities to query and manage.

CA

- CA hierarchy

  The PKI system uses a multi-layer CA hierarchy, in which the CA on the top is the root CA and the other CAs are subordinate CAs. Upper-layer CAs issue and manage certificates for lower-layer CAs, and the CAs at the lowest layer issue certificates to end entities. Certificates issued by CAs at different layers form a certificate chain, in which each certificate is signed by the subsequent certificate. The end of a certificate chain is the root CA, which has a self-signed certificate.

  - The root CA is the first CA (trustpoint) in the PKI system. It issues certificates to subordinate CAs, PCs, users, and servers. In most certificate-based applications, users can find the root CA in certificate chains.
  - A subordinate CA must obtain a certificate from the root CA or another subordinate CA that has been authorized by the root CA to issue CA certificates.

  In a CA hierarchy, a subordinate CA obtains its CA certificate from the upper-layer CA, and the root CA creates a self-signed certificate.

- CA types

  CAs are classified into the following types:

  - Self-signed CA: uses a self-signed certificate. The public key in the certificate is the same as the public key used to certify the digital signature.
  - Subordinate CA: uses a certificate issued by an upper-layer CA. The public key in the certificate is different from the public key used to certify the digital signature.
  - Root CA: is on the top of the CA hierarchy and trusted unconditionally by users. The root CA is the end of all certificate chains and signs its own certificate.

- CA functions

  The main function of CAs is to issue and manage certificates. A CA is responsible for the following:

- Receiving and verifying certificate applications from users
- Determining whether to accept certificate applications from users
- Issuing certificates to users or rejecting certificate applications
- Receiving and processing certificate renewal requests
- Responding to user requests to query or revoke certificates
- Creating and issuing CRLs
- Archiving certificates
- Backing up and recovering keys
- Archiving historical data

RA

An RA helps CAs issue and manage certificates. It verifies user identities when receiving certificate enrollment and revocation requests, and determines whether to submit the requests to the corresponding CA.

An RA is usually integrated with a CA. Independent RAs can also be used to reduce CA workloads and enhance CA system security.

7.8.2.3 PKI Implementation

Working Process

On a PKI network, PKI is configured to apply to a CA for a local certificate for a specified entity and verify certificate validity. The PKI working process is as follows:

1. An entity applies to an RA for a certificate.
2. The RA authenticates the entity's identity and sends the entity's identity information and public key as a digital signature to a CA.
3. The CA authenticates the digital signature and issues a certificate to the RA.
4. The RA receives the certificate and notifies the entity that the certificate is issued.
5. The entity obtains the certificate and uses it to securely communicate with other entities in encryption and digital signature modes.
6. The entity sends a revocation request to the CA to revoke a certificate. The CA approves the entity's revocation request and updates the CRL.

Working Principle

PKI uses public key theories and technologies to provide secure services for various network applications.

Because public keys are transmitted on a network, the public key encryption system must solve public key management problems. The digital certificate mechanism in the PKI better solves the problem. PKI core technologies involve digitical certificate application, issuing, usage, and revocation.

Certificate Enrollment

Certificate enrollment is a process in which an entity registers with a CA and obtains a certificate from the CA. During this process, the subject provides the identity information and public key, which will be added to the certificate issued to the subject.

A subject can apply to a CA for a certificate online or offline. In offline enrollment mode, the subject provides the identity information and public key in outband mode(for example, through phone call, disk, or email). In online enrollment mode, an enrollment request can be initiated manually or automatically. The following enrollment modes are often used:

- PKCS#10 mode (offline certificate enrollment)

  If a PKI entity use cannot SCEP to request a certificate online, it can save the certificate request information in PKCS#10 format to a file, and then send the file to the CA in outband mode.
- Simple Certificate Enrollment Protocol (SCEP) mode (online certificate enrollment and downloading)

  A PKI entity uses the Hypertext Transfer Protocol (HTTP) to communicate with a CA or a registration authority (RA). It sends an SCEP certificate enrollment request to apply for a local certificate or sends a certificate download request to download the CA/RA certificate or local certificate. This mode is most commonly used.
- Self-signed certificate

  A PKI entity issues a self-signed certificate, in which the certificate issuer and subject are the same.

Certificate Renewal

The device supports the certificate renewal function. It applies for a shadow certificate before the current certificate expires. When the current certificate expires, the shadow certificate takes effect.

The device completes a certificate enrollment process to obtain the shadow certificate.

The certificate renewal function can be used only when the CA server supports this function.

Certificate Downloading

An end entity can use the SCEP protocol to query and download issued certificates from a CA server. It can also use the CDP mechanism to download certificates from the specified CDP URL. Entities can download their own certificates, CA certificates, or certificates of other entities.

Certificate Revocation

Certificate revocation unbinds the public key of a subject from the subject's identity. A certificate subject needs to revoke its certificate when the subject's identity, information, or public key changes or the service for the subject ceases. A CA issues a CRL to revoke certificates, and an end entity submits a certificate revocation request to the CA server administrator in outband mode.

The administrator requires the end entity to provide the challenge password. The challenge password has been sent to the CA with a PKCS10# certificate enrollment request during certificate enrollment. If the challenge password provided by the end entity is the same as that saved on the CA server, the CA issues a CRL to revoke the certificate of the end entity.

CRL Downloading

CAs and RAs send CRLs to end entities only when they receive CRL query requests from end entities. Entities download CRLs from CAs or RAs in CDP or SCEP mode.

If a CA supports CDPs, it encodes a CDP URL and encapsulates the URL in the certificate issued to an end entity. The end entity then downloads the CRL from the URL.

If the certificate of an end entity does not contain the CDP information and no CDP URL is configured on the end entity, the end entity sends an SCEP message to request the CRL from the CA server. The SCEP message contains the certificate issuer name and certificate serial number.

Certificate Status Checking

When an end entity verifies a peer certificate, it checks the status of the peer certificate. For example, the end entity checks whether the peer certificate expires and whether the certificate is in a CRL. An end entity uses any of the following methods to check the peer certificate status:

- CRL

  If a CA supports CRL distribution points (CDPs), a certificate that the CA issues to an end entity contains the CDP information, specifying how and where to obtain the CRL for the certificate. The end entity then uses the specified method to find the CRL from the specified location and download the CRL.

  If a CDP URL is configured in a PKI domain, the end entity bound to the PKI domain obtains the CRL from the CDP URL.
- OCSP

  If a certificate does not specify any CDP and no CDP URL is configured in the PKI domain, an end entity can use the Online Certificate Status Protocol (OCSP) to check the certificate status.
- None

  This mode is used when no CRL or OCSP server is available to an end entity or the end entity does not need to check the peer certificate status. In this mode, an end entity does not check whether a certificate has been revoked.

Certificate Legality Verification

When an end entity needs to authenticate a peer, it checks the validity of the peer certificate. For example, when an end entity needs to set up a secure tunnel or connection with a peer, it verifies the peer certificate and issuer's certificate. If the certificate of a CA is invalid or has expired, all certificates issued by this CA are invalid. This invalidation seldom occurs because a device usually renews the CA/RA certificate before the certificate expires.

During certificate authentication, the local device must obtain the peer certificate and the following information: trusted CA certificate, CRL, local certificate and private key in the local certificate, and certificate authentication configuration.

The local device authenticates a certificate as follows:

1. Uses the public key of the CA to verify the digital signature of the CA.
2. Checks whether the certificate has expired.
3. Checks whether the certificate has been revoked in CRL, OCSP, or None mode.

Certificate Chain Authentication

A user must obtain the public key of a certificate issuer before verifying the private key signature in the certificate. Each CA certificate is certified by an upper-layer CA, and the certificate

authentication process is performed along a certificate chain. A certificate chain ends at a trustpoint, which is the root CA holding a self-signed certificate or a trusted intermediate CA.

A certificate chain is a series of trusted certificates, which starts at an end entity's certificate and ends at a root certificate. Entities that have the same root CA or subordinate CA and have obtained CA certificates can authenticate each other's certificates (peer certificates). Authentication of a peer certificate chain ends at the first trusted certificate or CA.

In brief, certificate chain authentication starts at an entity certificate and ends at a trustpoint certificate.

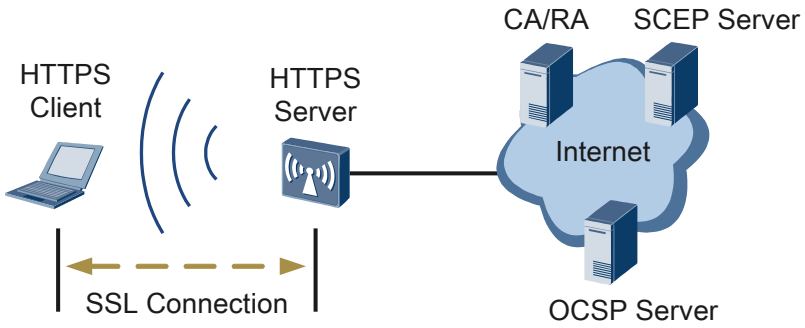
7.8.3 Applications

This section describes the applicable scenario of PKI.

7.8.3.1 PKI in SSL Networking

Figure 7-48 shows an example of Secure Sockets Layer (SSL) networking.

Figure 7-48 Networking of an SSL application



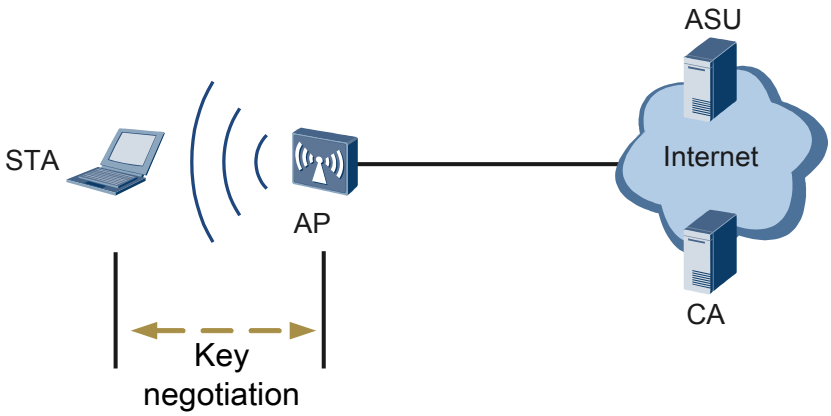
The SSL protocol provides secure connections for application layer protocols based on the Transmission Control Protocol (TCP). For example, SSL is combined with the Hypertext Transfer Protocol (HTTP) in the Hypertext Transfer Protocol Secure (HTTPS) application. SSL provides secure communication for ecommerce and online banking services.

To establish a secure connection, an HTTPS client authenticates an HTTPS server. The HTTPS server can also authenticate the HTTPS client. When authenticating each other, the HTTPS client and server exchange and verify each other's certificate. PKI implements certificate application, certificate renewal, and certificate authentication.

7.8.3.2 PKI in WAPI Networking

Figure 7-49 shows an example of networking of WLAN authentication and privacy infrastructure (WAPI) networking.

Figure 7-49 Networking of a WAPI application



WLAN stations (STAs) use the WAPI certificate authentication mode (WAPI-CERT) to connect to the Internet. The authentication service unit (ASU) authenticates STAs and access points (APs). The CA server issues certificates. Generally, the ASU and CA server are deployed on the same device.

During WAPI-CERT authentication, both STAs and APs must be authenticated. Before authentication, STAs and APs must obtain their certificates. The ASU checks their certificates to authenticate them.

An AP does not check an STA's certificate. Instead, it sends its own certificate and the STA's certificate to the ASU for authentication.

In WAPI applications, the PKI module reads a certificate file from a device's storage device and loads the certificate to the memory.

7.8.4 Default Configuration

This topic describes the default configuration for the PKI. The configuration can be modified based on the site requirements.

Table 7-38 lists the PKI default configuration.

Table 7-38 PKI default configuration

Parameter	Default Value
PKI Entity	Unspecified
PKI Domain	default
Length of the RSA key	1024
Certificate status check mode	CRL mode

7.8.5 Configuration Task Summary

After the PKI configurations are complete, the device can obtain the digital certificates for identity verification, data encryption, and data signing.

Table 7-39 lists the PKI configuration tasks. The device obtains certificates in one of the following ways. The certificates include CA certificates and device certificate. The device uses the device certificate to show its own identity, and uses the CA certificates to verify the validity of the device certificate.

Table 7-39 Configuration task summary

Scenario	Description	Task
Applying for certificates	An entity submits the identity information to the CA server and obtains the certificates. In this process, the entity submits the identity information and public key to the CA server. The CA server adds the identity information and public key into the certificate issued to the entity. Depending on whether there is a reachable route between the device and CA server, two ways to apply for certificates are available: ● Online: When a reachable route exists between the device and CA server, the device communicates with the CA server through SCEP to obtain certificates. ● Offline: When no reachable route exists between the device and CA server, the user needs to manually generate a certificate request file on the device, and sends the file to the CA server through disk or email.	1. **7.8.6.1 Configuring a PKI Entity** 2. **7.8.6.2 Configuring a PKI Domain** 3. **7.8.6.3 Configuring Certificate Registration and Obtaining** 4. **7.8.6.4 Configuring Certificate Authentication**
Importing certificates	The user uploads the certificate files to the storage device on the device through FTP or TFTP, and imports the files to the memory. This mode is applicable when the user has bought certificates from the IAOPC or has obtained certificates from the CA server.	**7.8.6.5.2 Importing a Certificate**

Scenario	Description	Task
Self-signed certificate	A self-signed certificate is issued by the device. That is, the certificate requester and issuer are the same. This mode is applicable when the user requires a temporary certificate or has low requirement on data security.	**7.8.6.3.3 Creating a Self-signed Certificate or Local Certificate**

7.8.6 Configuring PKI

This section describes the AAA configuration procedure.

7.8.6.1 Configuring a PKI Entity

A certificate binds a public key to a set of information that uniquely identifies a PKI entity. A PKI entity identifies a certificate applicant.

7.8.6.1.1 Configuring a PKI Entity Identifier

Context

You can configure a common name to uniquely identify a PKI entity.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki entity entity-name
```

A PKI entity is created and the PKI entity view is displayed.

By default, no PKI entity is configured on the device.

Step 3 Run:

```
common-name common-name
```

A common name is configured on the device.

By default, no common name is configured on the device.

----End

7.8.6.1.2 (Optional) Configuring PKI Entity Attributes

Context

In addition to configuring a common name or an FQDN for a PKI entity, you can configure the fully qualified domain name (FQDN), country code, state name or province name, and department name for the PKI entity to identify this PKI entity.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

pki entity *entity-name*

The PKI entity view is displayed.

Step 3 Run:

fqdn *fqdn-name*

A FQDN is configured for the PKI entity.

By default, no FQDN is configured on the device.

Step 4 Run:

country *country-code*

A country code is configured for the PKI entity.

By default, no country code is configured for a PKI entity.

Step 5 Run:

locality *locality-name*

A geographic area is configured for the PKI entity.

By default, no geographic area is configured for a PKI entity on the device.

Step 6 Run:

state *state-name*

A state name or province name is configured for the PKI entity.

By default, no state name or province name is configured for a PKI entity.

Step 7 Run:

organization *organization-name*

An organization name is configured for the PKI entity.

By default, no organization name is configured for a PKI entity.

Step 8 Run:

organization-unit *organization-unit-name*

A department name is configured for the PKI entity.

By default, no department name is configured for a PKI entity.

Step 9 Run:

```
ip-address ip-address
```

An IP address is configured for the PKI entity.

By default, no IP address is configured for a PKI entity.

----End

7.8.6.1.3 Checking the Configuration

Context

After a PKI entity is configured, you can view the PKI entity configuration.

Procedure

- Run the **display pki entity** [*entity-name*] command to check the PKI entity configuration.

----End

7.8.6.2 Configuring a PKI Domain

Before an entity applies for a PKI certificate, registration information needs to be configured for the entity. A set of the registration information is the PKI domain of the entity.

7.8.6.2.1 Creating a PKI Domain

Context

A PKI domain is a set of identity information required when a PKI entity enrolls a certificate. A PKI domain allows other applications, such as Internet Key Exchange (IKE) and Secure Sockets Layer (SSL), to reference the PKI configuration easily.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

A PKI domain is created.

----End

7.8.6.2.2 Configuring a PKI Entity Name

Context

In a PKI domain, configure a name for the PKI entity applying for a certificate. A PKI entity name binds to only one PKI entity.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

The PKI domain view is displayed.

Step 3 Run:

```
entity entity-name
```

A PKI entity is specified.

By default, no PKI entity is specified on the device.

----End

7.8.6.2.3 Configuring the Trusted CA Name and Enrollment URL

Context

A trusted authentication authority enrolls and issues certificates to entities. Therefore, a trusted CA name and enrollment URL must be configured.

A registration authority (RA) receives registration requests from users, checks users' certificate credentials, and decides whether a CA can issue digital certificates to the users. An RA does not issue certificates to users and it only checks users' certificate credentials. Sometimes, a CA implements the registration management function and therefore no independent RA is required.

Before an entity requests a certificate, an enrollment URL must be specified. The entity requests a certificate using the Simple Certificate Enrollment Protocol (SCEP) with the server specified by the enrollment URL. SCEP is used by entities to communicate with CAs.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

The PKI domain view is displayed.

Step 3 Run:

```
ca id ca-name
```

A trusted CA name is configured.

By default, no trusted CA is configured on the device.

Step 4 Run:

```
enrollment-url url [ interval minutes ] [ times count ] [ ra ]
```

An enrollment URL is configured.

By default, no enrollment URL is configured on the device.

----End

7.8.6.2.4 Configuring CA Certificate Fingerprint

Context

Before the device obtains a CA certificate, the device needs to check the CA certificate fingerprint to ensure that the content of the certificate is not tampered by unauthorized users. The CA certificate fingerprint is unique to each certificate. If the CA certificate fingerprint is different from the fingerprint configured in a specified PKI domain, the device refuses the issued certificate.

NOTE

A CA certificate fingerprint is usually sent to the device in outband mode (for example, through phone call, disk, or email).

If a certificate is applied for in automatic mode, the CA certificate fingerprint must be configured. If a certificate is applied for in manual mode, the configuration of the CA certificate fingerprint is optional. If the CA certificate fingerprint is not configured, users must authenticate the CA certificate fingerprint by themselves.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

The PKI domain view is displayed.

Step 3 Run:

```
fingerprint { md5 | sha1 } fingerprint
```

The CA certificate fingerprint used in CA certificate authentication is configured.

By default, no CA certificate fingerprint is configured on the device.

----End

7.8.6.2.5 (Optional) Configuring the RSA Key Length of Certificates

Context

The digital certificate system depends on the public key system. The device supports the RSA public key system. The RSA uses a pair of asymmetric RSA keys, namely, an RSA public key and an RSA private key. When an entity applies for a digital certificate, the request must contain the RSA public key.

The length of the RSA key equals the modulus of the RSA key. A larger modulus provides stronger key security but it takes a longer time to generate keys, and encrypt or decrypt data using the key pair.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

The PKI domain view is displayed.

Step 3 Run:

```
rsa-key-size size
```

The RSA key length of certificates is set.

By default, the RSK key length of certificates is 1024 on the device.

----End

7.8.6.2.6 (Optional) Configuring a Certificate Revocation Password

Context

Configuring a certificate revocation password prevents users from incorrectly revoking certificates. This improves operation security.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

The PKI domain view is displayed.

Step 3 Run:

```
password cipher password
```

A certificate revocation password is configured.

By default, no certificate revocation password is configured on the device.

----End

7.8.6.2.7 (Optional) Configuring a Source Interface for TCP Connection Setup

Context

The device uses the IP address of a specified source interface to establish a TCP connection with the Simple Certificate Enrollment Protocol (SCEP) server or Online Certificate Status Protocol (OCSP) server.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

The PKI domain view is displayed.

Step 3 Run:

```
source interface interface-type interface-number
```

The source interface is specified.

By default, the device uses the outbound interface as the source interface for TCP connection setup.

----End

7.8.6.2.8 Checking the Configuration

Context

After a PKI domain is configured, you can check the PKI domain configuration.

Procedure

- Run the **display pki realm** [*pki-realm-name*] command to check the PKI domain configuration.

----End

7.8.6.3 Configuring Certificate Registration and Obtaining

The device supports manual and automatic certificate enrollment and manual certificate obtaining.

7.8.6.3.1 Configuring Manual Certificate Enrollment

Prerequisites

A PKI domain has been created and configured. For details, see **7.8.6.2 Configuring a PKI Domain**.

Context

An entity can apply to a CA for a certificate online or offline. In offline enrollment mode, the entity provides the identity information and public key in outband mode.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki enroll-certificate pki-realm-name [ pkcs10 [ filename filename ] ]
```

Manual certificate enrollment is configured.

- If **pkcs10** is specified, an entity applies to a CA for a certificate in offline mode. The entity saves the certificate request information in a file in PKCS#10 format and sends the file to the CA in outband mode.
- If **pkcs10** is not specified, an entity applies to a CA for a certificate in online mode.

NOTE

When a certificate is enrolled manually, the CA certificate and local certificate are downloaded and saved in the default path automatically. Refer to **7.8.6.5.4 Configuring the Default Path Where Certificates Are Stored** to configure the default path.

----End

7.8.6.3.2 Configuring Automatic Certificate Enrollment

Prerequisites

A PKI domain has been created and configured. For details, see **7.8.6.2 Configuring a PKI Domain**.

Context

Automatic certificate enrollment: A PKI device uses the Simple Certification Enrollment Protocol (SCEP) to request a certificate from a CA when the configuration required for certificate enrollment is complete but no local certificate is available. When the certificates are unavailable, will expire, or have expired, an entity automatically requests a new certificate or renews the certificate using the Simple Certification Enrollment Protocol (SCEP).

After the automatic certificate enrollment and update function is enabled, users do not need to manually download certificates. When an external application requires a CA or local certificate, it instructs the system to download a CA or local certificate.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

The PKI domain view is displayed.

Step 3 Run:

```
auto-enroll [ percent ] [ regenerate ]
```

The automatic certificate enrollment and update function is enabled.

By default, the automatic certificate enrollment and update function is disabled on the device.

----End

7.8.6.3.3 Creating a Self-signed Certificate or Local Certificate

Context

A PKI device can generate a self-signed certificate or local certificate and issue the certificate to a user.

NOTICE

The device does not provide lifecycle management for self-signed certificates. For example, self-signed certificates cannot be updated, or revoked on the device. To ensure security of the device and certificates, it is recommended the user's certificate be used.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki create-certificate [ self-signed ] filename file-name
```

A self-signed certificate or local certificate is created.

----End

7.8.6.3.4 Configuring Certificate Obtaining

Context

Certificate obtaining is configured so that an entity can query and download an issued certificate from a CA server. Entities can download their own certificates, CA certificates, or certificates of other entities.

The purposes of obtaining a certificate are as follows:

- Stores certificates on a local computer to improve certificate query efficiency and reduce the times of querying the PKI certificate repository.
- Prepares for certificate authentication.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki get-certificate { ca | local } pki-realm-name
```

A CA or local certificate is obtained.

----End

7.8.6.3.5 Checking the Configuration

Context

After a certificate is obtained from a CA, or a self-signed certificate or local certificate is created, you can view certificate information.

Procedure

- Run the **display pki certificate** { **ca** | **local** | **ocsp** } *pki-realm-name* [**verbose**] command to view information about the CA certificate, local certificate or OCSP certificate.
- Run the **display pki certificate enroll-status** *pki-realm-name* command to view the certificate enrollment status.

----End

7.8.6.4 Configuring Certificate Authentication

Before a certificate is used, it must be authenticated.

7.8.6.4.1 Configuring the Certificate Check Mode

Context

When an end entity verifies a peer certificate, it checks the status of the peer certificate. For example, the end entity checks whether the peer certificate expires and whether the certificate is in a CRL. An end entity uses any of the following methods to check the peer certificate status:

- CRL

  If a CA supports CRL distribution points (CDPs), a certificate that the CA issues to an end entity contains the CDP information, specifying how and where to obtain the CRL for the certificate. The end entity then uses the specified method to find the CRL from the specified location and download the CRL.

  If a CDP URL is configured in a PKI domain, the end entity bound to the PKI domain obtains the CRL from the CDP URL.

- OCSP

  If a certificate does not specify any CDP and no CDP URL is configured in the PKI domain, an end entity can use the Online Certificate Status Protocol (OCSP) to check the certificate status.

- None

  This mode is used when no CRL or OCSP server is available to an end entity or the end entity does not need to check the peer certificate status. In this mode, an end entity does not check whether a certificate has been revoked.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki realm realm-name
```

The PKI domain view is displayed.

Step 3 Run:

```
certificate-check { crl | none | ocsp }
```

The certificate check mode is configured.

By default, the device checks certificates using CRLs.

- When the CRL mode is used:

1. Run the **cdp-url** *cdp-url* command to configure the CDP URL.

   By default, the CDR URL is not configured.

2. Run the **crl update-period** *hours* command to configure the interval for an PKI entity to download CRLs from a CRL server.

   By default, the CRLs are updated at the next update time that is specified in the certificate.

3. (Optional) Run the **crl cache** command to permit PKI domains to use cached CRLs.

   By default, the PKI domain is permitted to use the cached CRLs.

4. Run the **quit** command to go back to the system view.
5. (Optional) Run the **pki get-crl** *pki-realm-name* command to configure the device to download CRLs form CA servers.

NOTE

When suspecting that the local CRLs are outdated, users can run the command to download the latest CRLs from CA servers.

- When the OCSP mode is used:

1. Run the **ocsp-url** *ocsp-url* command to configure the URL of the OCSP server.

   This URL overrides the OCSP server's address in the certificate.

----End

7.8.6.4.2 Checking Certificate Validity

Context

When an end entity needs to authenticate a peer, it checks the validity of the peer certificate. For example, when an end entity needs to set up a secure tunnel or connection with a peer, it verifies the peer certificate and issuer's certificate. If the certificate of a CA is invalid or has expired, all certificates issued by this CA are invalid. This invalidation seldom occurs because a device usually renews the CA/RA certificate before the certificate expires.

During certificate authentication, the local device must obtain the peer certificate and the following information: trusted CA certificate, CRL, local certificate and private key in the local certificate, and certificate authentication configuration.

The local device authenticates a certificate as follows:

1. Uses the public key of the CA to verify the digital signature of the CA.
2. Checks whether the certificate has expired.
3. Checks whether the certificate has been revoked in CRL, OCSP, or None mode.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki validate-certificate { ca | local } pki-realm-name
```

The CA certificate validity or local certificate validity is checked.

----End

7.8.6.4.3 Checking the Configuration

Context

After the certificate authentication mode is configured, you can view certificate information.

Procedure

- Run the **display pki certificate enroll-status** *pki-realm-name* command to check the certificate enrollment status.
- Run the **display pki crl** *pki-realm-name* command to check CRL information.

----End

7.8.6.5 Managing Certificates

Managing certificates include deleting, importing, and exporting certificates, and configuring the default path where certificates are stored.

7.8.6.5.1 Deleting a Certificate

Context

When a certificate expires or a user wants to request a new certificate, you can delete the existing certificate.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki delete-certificate { ca | local  | ocsp } pki-realm-name
```

The certificate is deleted.

----End

7.8.6.5.2 Importing a Certificate

Context

To use an external certificate, copy it to a storage device in outband mode and import it to the device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki import-certificate { ca | local | ocsp } pki-realm-name { der | pkcs12 | pem }
```

The external certificate is imported to the device.

----End

7.8.6.5.3 Exporting a Certificate

Context

To provide a certificate for another device, export the certificate.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki export-certificate { ca | local | ocsp } pki-realm-name { der | pkcs12 | pem }
```

The certificate is exported and saved in a file.

----End

7.8.6.5.4 Configuring the Default Path Where Certificates Are Stored

Context

You can configure the default path where certificate files are stored.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
pki credential-storage local-dir
```

The default path and directory where the CA certificate, local certificate, and private key are stored are configured.

----End

7.8.7 Configuration Examples

This section provides PKI configuration examples.

7.8.7.1 Example for Configuring Manual Certificate Enrollment

Networking Requirements

Configure the PKI entity AP to apply for a certificate from a CA, as shown in **Figure 7-50**.

Figure 7-50 Configuring a PKI entity to request a certificate from a CA

Configuration Roadmap

1. Configure a PKI entity to identify a certificate applicant.
2. Configure a PKI domain and specify identity information required for certificate enrollment, including the trusted CA name, bound entity name, enrollment URL, and CA certificate fingerprint.
3. Enroll the certificate manually.

Procedure

Step 1 Configure a PKI entity to identify a certificate applicant.

Configure a PKI entity user01.

```
<Huawei> system-view
[Huawei] pki entity user01
[Huawei-pki-entity-user01] common-name hello
[Huawei-pki-entity-user01] country cn
[Huawei-pki-entity-user01] state jiangsu
[Huawei-pki-entity-user01] organization huawei
[Huawei-pki-entity-user01] organization-unit info
[Huawei-pki-entity-user01] quit
```

Step 2 Configure a PKI domain and specify the identity information required for certificate enrollment in the PKI domain.

Configure the trusted CA, bound entity, enrollment URL, and CA certificate fingerprint.

```
[Huawei] pki realm abc
[Huawei-pki-realm-abc] ca id ca_root
[Huawei-pki-realm-abc] entity user01
[Huawei-pki-realm-abc] enrollment-url http://10.137.145.158:8080/certsrv/mscep/
mscep.dll ra
[Huawei-pki-realm-abc] fingerprint sha1 7A34D94624B1C1BCBF6D763C4A67035D5B578EAF
[Huawei-pki-realm-abc] quit
```

Step 3 Enroll the certificate manually.

```
[Huawei] pki enroll-certificate abc
 Create a challenge password. You will need to verbally provide this password to
 the CA Administrator in order to revoke your certificate.
 For security reasons your password will not be saved in the configuration. Plea
se make a note of it.
 Choice no password ,please enter the enter-key.
 Please enter Password:
 Start certificate enrollment ...
 Certificate is enrolling now,It will take a few minutes or more.
 Please waiting...
 The certificate enroll successful.
```

You will be prompted to enter the password during certificate enrollment. If you do not have a password, press **Enter**.

Step 4 Verify the configuration.

After the preceding configurations are complete, the CA issues a certificate to the PKI entity. In the certificate information, the **issued to** field value is the entity common name *hello*.

Run the **display pki certificate local** command on the PKI entity to view the certificate.

```
[Huawei] display pki certificate local abc
Certificate
  Status : Available
  Version: 3
  Serial Number:
    19 36 41 af 00 00 00 00 02 ba
  Subject:
    C=CN
    ST=jiangsu
    O=huawei
    OU=info
    CN=hello

  Associated Pki Realm : abc

Total Number: 1
```

----End

Configuration Files

```
#
pki entity user01
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
#
pki realm abc
 ca id ca_root
 enrollment-url http://10.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity user01
 fingerprint sha1 7a34d94624b1c1bcbf6d763c4a67035d5b578eaf
#
return
```

7.8.7.2 Example for Importing Certificates Manually

Networking Requirements

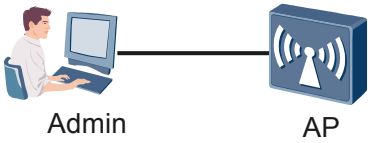
An enterprise has bought the following certificates from a branch of the International Association of Professional Certification (IAOPC):

- localcert.pem: local certificate, which can be used as the identity information of a device to ensure device security.
- privatekey.pem: private key file of the local certificate, using abcd@huawei20091201 as the password.
- middlecert.pem: CA certificate (level-3 CA certificate) issued by the subordinate CA server, which verifies the validity of the device certificate.

- crosscert.pem: CA certificate (level-2 CA certificate) issued by the root CA server, through which the CA server verifies the validity of the level-3 CA certificate.

As shown in **Figure 7-51**, the administrator needs to import the certificates to the device so that the applications such as SSL can reference the certificates.

Figure 7-51 Importing certificates manually



Configuration Roadmap

1. Create a PKI domain so that the applications such as SSL can reference the PKI configurations.
2. Import the local certificate to the device so that the device can encrypt and sign on the data and securely communicate with other devices.
3. Import the CA certificates to the device to verify the validity of the local certificate.

NOTE

Ensure that the **crosscert.pem**, **localcert.pem**, **middlecert.pem**, and **privatekey.pem** files have been loaded to the device through FTP or SFTP.

Procedure

Step 1 Create a PKI domain.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
```

Step 2 Import the local certificate.

Import the local certificate **localcert.pem** and private key **privatekey.pem**.

```
[Huawei] pki import-certificate local abc pem
 Please enter the name of certificate file <length 1-127>: localcert.pem
 You are importing a local certificate,
 You can directly enter "Enter" only the local certificate getting by pkcs10
message in security realm
 Please enter the name of private key file <length 1-127>: privatekey.pem
 Please enter the type of private key file(pem , p12 , der): pem
 The current password is required, please enter your password <length 1-31>:
******************
 Successfully imported the certificate.
```

Step 3 Import the CA certificates.

Import the CA certificate **middlecert.pem** issued by the subordinate CA server.

```
[Huawei] pki import-certificate ca abc pem
 Please enter the name of certificate file <length 1-127>:
middlecert.pem
  The CA's Subject is C=US,O=GeoTrust Inc.,OU=Domain Validated SSL,CN=GeoTrust DV
SSL CA
```

```
  The CA's fingerprint is:
    MD5  fingerprint: f4858289  ead55c53  b36d4b55  3f267837
    SHA1 fingerprint: bae30b15  dbb1544c  f194d076  b75b7bb9  e3d6b760
  Is the fingerprint correct? [Y/N]: y
 Successfully imported the certificate.
```

Import the CA certificate **crosscert.pem** issued by the root CA server.

```
[Huawei] pki import-certificate ca abc pem
 Please enter the name of certificate file <length 1-127>: crosscert.pem
  The CA's Subject is C=US,O=GeoTrust Inc.,CN=GeoTrust Global CA
  The CA's fingerprint is:
    MD5  fingerprint: 2e7db2a3  1d0e3da4  b25f49b9  542a2e1a
    SHA1 fingerprint: 7359755c  6df9a0ab  c3060bce  369564c8  ec4542a3
  Is the fingerprint correct? [Y/N]: y
 Successfully imported the certificate.
```

Step 4 Verify the configuration.

After the configurations are complete, run the **display pki certificate local** and **display pki certificate ca** command on the device to view the imported local certificate and CA certificates.

```
[Huawei] display pki certificate local abc
Certificate
  Status : Available
  Version: 3
  Serial Number:
    07 1e 39
  Subject:
    OU=GT51268791
    CN=securelogin.huawei.com

  Associated Pki Realm : abc

Total Number: 1
[Huawei] display pki certificate ca abc
CA certificate
  Status : Available
  Version: 3
  Serial Number:
    12 bb e6
  Subject:
    C=US
    O=GeoTrust Inc.
    CN=GeoTrust Global CA

  Associated Pki Realm : abc

CA certificate
  Status : Available
  Version: 3
  Serial Number:
    02 36 d2
  Subject:
    C=US
    O=GeoTrust Inc.
    OU=Domain Validated SSL
    CN=GeoTrust DV SSL CA

  Associated Pki Realm : abc

Total Number: 2
```

----End

Configuration Files

Configuration file of the AP

```
#
pki realm abc
#
return
```

7.9 SSL Configuration

The Secure Sockets Layer (SSL) protocol protects information privacy on the Internet.

7.9.1 SSL Overview

The Secure Sockets Layer (SSL) protocol uses data encryption, identity authentication, and message integrity check to ensure security of TCP-based application layer protocols.

Introduction to SSL

SSL is a cryptographic protocol that provides communication security over the Internet. It allows a client and a server to communicate in a way designed to prevent eavesdropping. The server must be authenticated by the client before they start to communicate, and the client can also be authenticated by the server. SSL is widely used in ecommerce and online banking. It has the following advantages:

- High security: SSL ensures secure data transmission by using data encryption, identity authentication, and message integrity check.
- Support for various application layer protocols: SSL was originally designed to secure World Wide Web traffic. SSL functions between the application layer and the transport layer, so it can provide security for any TCP-based application.
- Easy to deploy: SSL has become a world-wide communications standard used to authenticate websites and web users, and to encrypt data transmitted between browser users and web servers.

SSL improves device security using the following functions:

- Allows only authorized users to connect to servers.
- Encrypts data transmitted between a client and a server to secure data transmission and computes a digest to ensure data integrity.
- Defines an access control policy on a device based on certificate attributes to control access rights of clients. This access control policy prevents unauthorized users from attacking the device.

Terms

- Certificate Authority (CA)

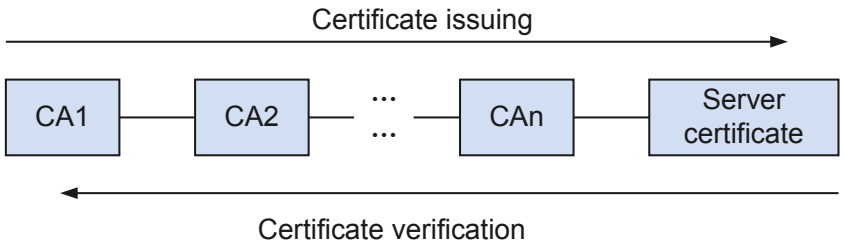
  A CA is an entity that issues, manages, and abolishes digital certificates. A CA checks validity of digital certificate owners, signs digital certificates to prevent eavesdropping and tampering, and manages certificates and keys. A world-wide trusted CA is called a root CA. The root CA can authorize other CAs as subordinate CAs. The CA identities are described in a trusted-CA file.

In the certificate issuing process, CA1 functions as the root CA and issues a certificate for CA2, and CA2 issues a certificate for CA3. The process repeats until CAn issues the final server certificate.

In the certificate authentication process, the client first authenticates the server's certificate. If CA3 issues the server certificate, the client uses CA3 certificate to authenticate the server certificate. If the server certificate is authenticated, the client uses CA2 certificate to authenticate the CA3 certificate. After CA2 certificate is authenticated, the client uses CA1 certificate to authenticate CA2 certificate. The client considers the server certificate valid only when CA2 certificate has been authenticated.

Figure 7-52 shows the certificate issuing and authentication processes.

Figure 7-52 Certificate issuing and authentication



- Digital certificate

  A digital certificate is an electronic document issued by a CA to bind a public key with a certificate subject (an applicant that has obtained a certificate). Information in a digital certificate includes the applicant name, public key, digital signature of the CA that issues the digital certificate, and validity period of the digital certificate. A digital certificate verifies the identities of two communicating parties, improving communication reliability.

  A user must obtain the public key certificate of the information sender to decrypt and authenticate information in the certificate. The user also needs the CA certificate of the information sender to verify the identity of the information sender.

- Certificate Revocation List (CRL)

  A CRL is issued by a CA to specify certificates that have been revoked.

  Each certificate has a validity period. A CA can issue a CRL to revoke certificates before their validity periods expire. The validity period of a certificate specified in the CRL is shorter than the original validity period of the certificate. If a CA revokes a digital certificate, the key pair defined in the certificate cannot be used. After a certificate in a CRL expires, the certificate is deleted from the CRL to shorten the CRL.

  Information in a CRL includes the issuer and serial number of each certificate, the issuing date of the CRL, certificate revocation date, and time when the next CRL will be issued.

  Clients use CRLs to check validity of certificates. When verifying a server's digital certificate, a client checks the CRL. If the certificate is in the CRL, the client considers the certificate invalid.

Security Mechanisms

SSL provides the following security mechanisms:

- Connection privacy

SSL uses symmetric cryptography to encrypt data. It uses the Rivest-Shamir-Adleman (RSA) algorithm (an asymmetric algorithm) to encrypt the key used by the symmetric cryptography.

- Identity authentication

  Digital certificates are used to authenticate a server and a client that need to communicate with each other. The SSL server and client use the mechanism provided by the public key infrastructure (PKI) to apply to a CA for a certificate.

- Message integrity

  A keyed message authentication code (MAC) is used to verify message integrity during transmission.

  A MAC algorithm computes a key and data of an arbitrary length to generate a MAC of a fixed length.

  - A message sender uses a MAC algorithm and a key to compute a MAC, appends it to a message, and send the message to a receiver.
  - The receiver uses the same key and MAC algorithm to compute a MAC and compares it with the MAC in the received message.

  If the two MACs are the same, the message has not been tampered during transmission. If the two MACs are different, the message has been tampered, and the receiver discards this message.

7.9.2 Default Configuration

This section provides the default SSL configuration. You can change the configuration as needed.

Table 7-40 describes the default SSL configuration.

Table 7-40 Default SSL configuration

Parameter	Default Setting
SSL protocol version in a client SSL policy	TLS1.0
Cipher suite in a client SSL policy	rsa_aes_128_cbc_sha, rsa_des_cbc_sha, rsa_rc4_128_md5, and rsa_rc4_128_sha
Cipher suite in a server SSL policy	rsa_aes_128_cbc_sha, rsa_des_cbc_sha, rsa_rc4_128_md5, and rsa_rc4_128_sha
Maximum number of sessions that can be saved and timeout period of a saved session	By default, a maximum of 3600 sessions can be saved, and the timeout period of a saved session is 128.

7.9.3 Configuring a Server SSL Policy

A server SSL policy defines parameters that an SSL server uses in SSL handshakes, including the PKI domain name, maximum number of sessions that can be saved, timeout period of a saved session, and cipher suite. Among these parameters, the PKI domain name is mandatory, and the others are optional.

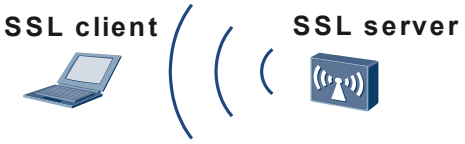
Prerequisites

The **PKI domain** has been configured.

Context

The SSL protocol uses data encryption, identity authentication, and message integrity check to ensure security of TCP-based application layer protocols. To use an AP as an SSL server, configure a server SSL policy on the AP. A server SSL policy can be applied to application layer protocols such as HTTP to provide secure connections.

Figure 7-53 AP functions as an SSL server



As shown in **Figure 7-53**, the AP functions as an SSL server and has a server SSL policy configured. During an SSL handshake, the AP uses the SSL parameters in the server SSL policy to negotiate session parameters with an SSL client. After the handshake is complete, the AP establishes a session with the client.

The AP is authenticated by the SSL client, but it cannot authenticate the client.

NOTE

When functioning as an SSL server, the AP can communicate with SSL clients running SSL3.0, TLS1.0, or TLS1.1. The AP determines the SSL protocol version used for this communication and sends a Server Hello message to notify the client.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ssl policy policy-name type server
```

A server SSL policy is created, and the server SSL policy view is displayed.

Step 3 Run:

```
pki-realm realm-name
```

A PKI domain is specified for the server SSL policy.

By default, no PKI domain is specified for a server SSL policy on the AP.

NOTE

The AP obtains a digital certificate from a CA in the specified PKI domain. SSL clients can then authenticate the AP by checking the digital certificate.

Step 4 (Optional) Run:

```
session { cachesize size | timeout time } *
```

The maximum number of sessions that can be saved and the timeout period of a saved session are set.

By default, a maximum of 3600 sessions can be saved, and the timeout period of a saved session is 128.

Step 5 (Optional) Run:

```
ciphersuite { rsa_aes_128_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 |
rsa_rc4_128_sha } *
```

A cipher suite is specified.

By default, a server SSL policy supports all the cipher suites: **rsa_aes_128_cbc_sha**, **rsa_des_cbc_sha**, **rsa_rc4_128_md5**, and **rsa_rc4_128_sha**.

----End

Checking the Configuration

Run the **display ssl policy** *policy-name* command to view the configuration of the SSL policy.

7.9.4 Configuring a Client SSL Policy

A client SSL policy defines the parameters that an SSL client uses in SSL handshakes, including the PKI domain name, SSL protocol version, and cipher suite.

Prerequisites

The **PKI domain** has been configured.

Context

The SSL protocol uses data encryption, identity authentication, and message integrity check to ensure security of TCP-based application layer protocols. To use an AP as an SSL client, configure a client SSL policy on the AP. A client SSL policy can be applied to application layer protocols to provide secure connections.

Figure 7-54 AP functions as an SSL client

As shown in **Figure 7-54**, the **Figure 7-54** functions as an SSL client and has a client SSL policy configured. During an SSL handshake, the AP uses the SSL parameters in the client SSL policy to negotiate session parameters with the SSL server. After the handshake is complete, the AP establishes a session with the server.

When functioning as an SSL client, the AP does not allow SSL servers to authenticate it, but it can authenticate SSL servers. When the AP functions as an SSL client, enable it to authenticate servers to ensure secure communication.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ssl policy policy-name type client
```

A server SSL policy is created, and the client SSL policy view is displayed.

Step 3 Run:

```
server-verify enable
```

SSL server authentication is enabled.

By default, SSL server authentication is disabled in a client SSL policy.

Step 4 Run:

```
pki-realm realm-name
```

A PKI domain is specified for the client SSL policy.

By default, no PKI domain is specified for a client SSL policy on the AP.

NOTE

The AP obtains a CA certificate chain from CAs in the specified PKI domain. The AP authenticates an SSL server by checking the server certificate and CA certificates against the CA certificate chain.

Step 5 (Optional) Run:

```
version { ssl3.0 | tls1.0 | tls1.1 }
```

The SSL protocol version is specified.

By default, a client SSL policy uses Transport Layer Security (TLS) version 1.0.

NOTE

Ensure that the specified SSL protocol version is supported by the SSL server. Before performing this step, check the SSL protocol versions that the SSL server supports.

Step 6 (Optional) Run:

```
prefer-ciphersuite { rsa_aes_128_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 |
rsa_rc4_128_sha }
```

A cipher suite is specified.

By default, a client SSL policy uses all the cipher suites: **rsa_aes_128_cbc_sha**, **rsa_des_cbc_sha**, **rsa_rc4_128_md5**, and **rsa_rc4_128_sha**.

NOTE

Ensure that the specified cipher suite is supported by the SSL server. Before performing this step, check the cipher suites that the SSL server supports.

----End

Checking the Configuration

Run the **display ssl policy** *policy-name* command to view the configuration of the SSL policy.

7.9.5 Configuration Examples

This section provides several SSL configuration examples.

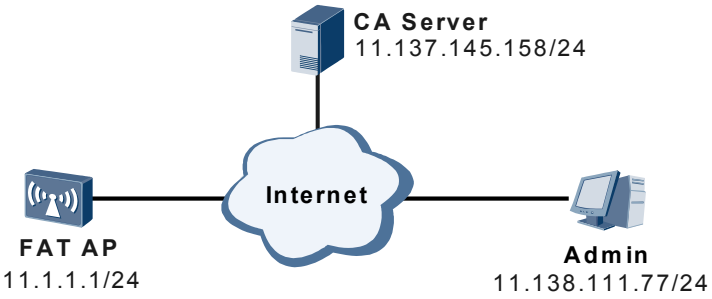
7.9.5.1 Example for Configuring a Server SSL Policy

Networking Environment

As shown in **Figure 7-55**, enterprise users use a web browser to connect to the AP. To prevent eavesdropping and tampering during data transmission, a network administrator requires users to use HTTPS to access the AP securely.

To meet this requirement, configure the AP as an HTTPS server and associate the HTTPS server with a server SSL policy so that users can securely access and manage the device through web pages.

Figure 7-55 Networking diagram of the server SSL policy configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a PKI entity and a PKI domain.
2. Configure a server SSL policy.
3. Configure the AP as an HTTPS server.

NOTE

Ensure that there are reachable routes between the AP, PC, and CA server.

Procedure

Step 1 Configure a PKI entity and a PKI domain.

Configure a PKI entity.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] pki entity users
[AP-pki-entity-users] common-name hello
[AP-pki-entity-users] country cn
[AP-pki-entity-users] state jiangsu
[AP-pki-entity-users] organization huawei
[AP-pki-entity-users] organization-unit info
[AP-pki-entity-users] quit
```

NOTE

If the entity name and entity common name are not set to the AP's IP address 11.1.1.1, the system will display a message indicating that the certificate is invalid when the client opens a website. This does not affect HTTPS application.

Configure a PKI domain, and enable the automatic certificate enrollment and update function.

```
[AP] pki realm users
[AP-pki-realm-users] entity users
[AP-pki-realm-users] ca id ca_root
[AP-pki-realm-users] enrollment-url http://11.137.145.158:8080/certsrv/mscep/
mscep.dll ra
[AP-pki-realm-users] fingerprint sha1 7bb05ada0482273388ed4ec228d79f77309ea3f4
[AP-pki-realm-users] auto-enroll regenerate
[AP-pki-realm-users] quit
```

Step 2 Configure a server SSL policy **sslserver**.

Create a server SSL policy and specify PKI domain **users** in the policy. This allows the AP to obtain a digital certificate from the CA specified in the PKI domain.

```
[AP] ssl policy sslserver type server
[AP-ssl-policy-sslserver] pki-realm users
```

Set the maximum number of sessions that can be saved and the timeout period of a session.

```
[AP-ssl-policy-sslserver] session cachesize 40 timeout 7200
[AP-ssl-policy-sslserver] quit
```

Step 3 Configure the AP as an HTTPS server.

Apply the SSL policy **sslserver** to the HTTPS service.

```
[AP] http secure-server ssl-policy sslserver
```

Enable the HTTPS server function on the AP.

```
[AP] http secure-server enable
```

Configure the port number of the HTTPS service.

```
[AP] http secure-server port 1278
```

Step 4 Verify the configuration.

Run the **display ssl policy** command to view the configuration of the SSL policy **sslserver**.

```
[AP] display ssl policy sslserver
 ------------------------------------------------------------------------------
  Policy name                        :
sslserver
  Policy ID                          :
1
  Policy type                        :
Server
  Cache number                       :   40
  Time out(second)                   :
7200
  Server certificate load status     :
loaded
  CA certificate chain load status   :   loaded
  Bind number                        :
1
  SSL connection number              :
1
  ------------------------------------------------------------------------------
```

Start the web browser on a PC, and enter **https://11.1.1.1:1278** in the address box. The web management system of the AP is displayed, and you can manage the AP on the web pages.

----End

Example

Configuration file of the AP

```
#
 sysname AP
#
pki entity users
 country CN
 state jiangsu
 organization huawei
 organization-unit info
 common-name hello
#
pki realm users
 ca id ca_root
 enrollment-url http://11.137.145.158:8080/certsrv/mscep/mscep.dll ra
 entity users
 auto-enroll regenerate
 fingerprint sha1 7bb05ada0482273388ed4ec228d79f77309ea3f4
#
ssl policy sslserver type server
 pki-realm users
 session cachesize 40 timeout 7200
#
 http secure-server port 1278
 http secure-server ssl-policy sslserver
 http secure-server enable
#
return
```

7.10 HTTPS Configuration

The Hypertext Transfer Protocol Secure (HTTPS) protocol provides secure web access using security mechanisms provided by the Secure Sockets Layer (SSL) protocol, including data encryption, identity authentication, and message integrity check.

7.10.1 Overview

This section describes the definition, background, and functions of HTTPS.

Definition

HTTPS supports the secure sockets Layer (SSL).

Purpose

HTTPS improves device security using SSL:

- Allows authorized clients access the device securely and rejects unauthorized clients
- Encrypts data exchanged between clients and the device to ensure data transmission security and integrity and implement secure management.

- Defines access control policies based on certificate attributes and controls access rights of clients to defend against attacks from unauthorized clients.

As shown in **Figure 7-56**, an SSL policy is configured on the device (an HTTP server). After the HTTPS server function is enabled on the device, users can use a web browser to log in to the device (an HTTPS server) and manage the device on web pages.

Figure 7-56 Logging in to an HTTPS server through the web browser

7.10.2 Configuring the Device as an HTTPS Server

The HTTPS server function allows users to securely access the device on web pages.

Prerequisites

A server SSL policy has been configured. For details on how to configure a server SSL policy, see **7.9.3 Configuring a Server SSL Policy**.

Context

When users access a remote device functioning as an HTTP server, the following problems exist:

- Users cannot authenticate the device.
- Privacy and integrity of data transmitted between users and the device cannot be ensured.

To solve the preceding problems, configure the device as an HTTPS server. The device uses the SSL protocol's data encryption, identity authentication, and message integrity check mechanisms to protect security of data transmitted between users and the device. These mechanisms ensure that users securely access a remote device on web pages.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
http secure-server ssl-policy ssl-policy
```

An SSL policy is applied to the HTTPS service.

By default, no SSL policy is applied to the HTTPS service on the device.

Step 3 (Optional) Run:

```
http secure-server port port-number
```

The port number is set for the HTTPS service.

By default, the port number of the HTTPS service is 443.

Step 4 Run:

```
http secure-server enable
```

The HTTPS server function is enabled on the device.

By default, the HTTPS server function is disabled on the device.

----End

Checking the Configuration

Run the **display current-configuration** command to check the configuration of the HTTPS server.

```
<Huawei> display current-configuration | include http secure-server
 http secure-server port
1026
 http secure-server ssl-policy
user
 http secure-server enable
```

7.10.3 Configuration Examples

This section provides an HTTPS configuration example.

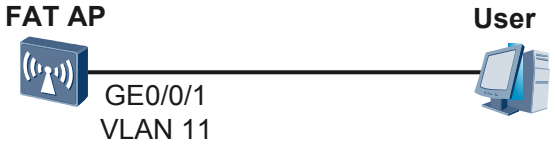
7.10.3.1 Example for Configuring the Device as an HTTPS Server

Networking Environment

As shown in **Figure 7-57**, users access the gateway AP through web.

To prevent data intercepting and tampering during data transmission, a network administrator requires that users use HTTPS to access the AP securely.

Figure 7-57 Networking diagram of HTTPS server configuration



Configuration Roadmap

The configuration roadmap is as follows:

1. Create a VLAN and a VLANIF interface, and configure the interface to allow enterprise users to access the router.
2. Configure a server SSL policy and apply the default PKI domain to the server SSL policy. The CA server is not required.

3. Configure an HTTPS server to ensure confidentiality and integrity of data transmission between users and the AP.

Procedure

Step 1 Create a VLAN and configure the interface.

Create VLAN 11 on the AP.

```
<Huawei> system-view
[Huawei] vlan batch 11
```

Add GE0/0/1 connecting to users to VLAN 11.

```
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] port link-type access
[Huawei-GigabitEthernet0/0/1] port default vlan 11
[Huawei-GigabitEthernet0/0/1] quit
```

Create VLANIF 11 and assign IP address 12.1.1.1/24 to VLANIF 11.

```
[Huawei] interface vlanif11
[Huawei-Vlanif11] ip address 12.1.1.1 24
[Huawei-Vlanif11] quit
```

Step 2 Configure a server SSL policy.

Apply the default PKI domain **default** to the server SSL policy.

```
[Huawei] ssl policy userserver type server
[Huawei-ssl-policy-userserver] pki-realm default
```

Set the maximum number of sessions that can be saved and the timeout period of a saved session are set.

```
[Huawei-ssl-policy-userserver] session cachesize 20 timeout 7200
[Huawei-ssl-policy-userserver] quit
```

Step 3 Configure the HTTPS server.

Bind the SSL policy **userserver** to the HTTPS server.

```
[Huawei] http secure-server ssl-policy userserver
```

Configure the port number of the HTTPS service.

```
[Huawei] http secure-server port 1278
```

Enable the HTTPS server function on the AP.

```
[Huawei] http secure-server enable
  This operation will take several minutes, please wait...
Info:HTTPS server has been started
[Huawei] quit
```

Step 4 Verify the configuration.

Run the **display ssl policy** *policy-name* command to view the configuration of the SSL policy **userserver**.

```
<Huawei> display ssl policy userserver
 --------------------------------------------------------------------------------
  Policy name                    :   userserver
  Policy ID                      :   0
```

```
  Policy type                     :   Server
  Cache number                    :   20
  Time out(second)                :   7200
  Server certificate load status  :   loaded
  CA certificate chain load status:   loaded
  Bind number                     :   1
  SSL connection number           :   0
  --------------------------------------------------------------------------------
```

Start the web browser on a computer, and enter https://12.1.1.1:1278 in the address box. The web management system is displayed, and you can manage the AP on the web pages.

----End

Configuration File

Configuration file of the AP

```
#
 http server enable
 http secure-server port 1278
 http secure-server ssl-policy userserver
 http secure-server enable
#
vlan batch 11
#
pki realm default
 enrollment self-signed
#
ssl policy userserver type server
 pki-realm default
 session cachesize 20 timeout 7200
#
interface Vlanif11
 ip address 12.1.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 11
#
return
```

8 Configuration Guide - QoS

About This Chapter

Quality of service (QoS) defines a service provider's ability to meet the level of service required by a customers' traffic. The QoS-enabled device controls enterprise network traffic, implements congestion congestion and congestion avoidance, reduces the packet loss ratio, and provides dedicated bandwidth for enterprise users or differentiated services.

8.1 Traffic Policing Configurations

This document describes basic concepts of traffic policing, and configuration methods of traffic policing based on an interface or a traffic classifier, and provides configuration examples.

8.1.1 Overviews of Traffic Policing

Traffic policing monitor traffic entering a network to control traffic and resource usage and better serve users.

If the transmit rate of packets is greater than the receive rate of packets or the rate of an interface on a downstream device is smaller than that of the connected interface on the upstream device, network congestion occurs. If traffic sent by users is not limited, continuous burst data from numerous users may aggravate network congestion. To efficiently use limited network resources and better serve more users, traffic sent by users must be limited.

Traffic policing limit traffic and resource usage by monitoring the traffic rate.

8.1.2 Traffic Policing and Traffic Shaping

If traffic sent by users is not limited, continuous burst data from numerous users may aggravate network congestion. To efficiently use limited network resources and better serve more users, traffic sent by users must be limited.

Traffic policing and traffic shaping limit traffic and resource usage by monitoring the traffic rate. Before implementing traffic policing and traffic shaping, assess whether the traffic exceeds the rate limit. Then traffic policies are implemented based on the assessment result. Generally, token buckets are used to assess traffic.

Differences Between Traffic Policing and Traffic Shaping

The differences between traffic policing and traffic shaping are as follows:

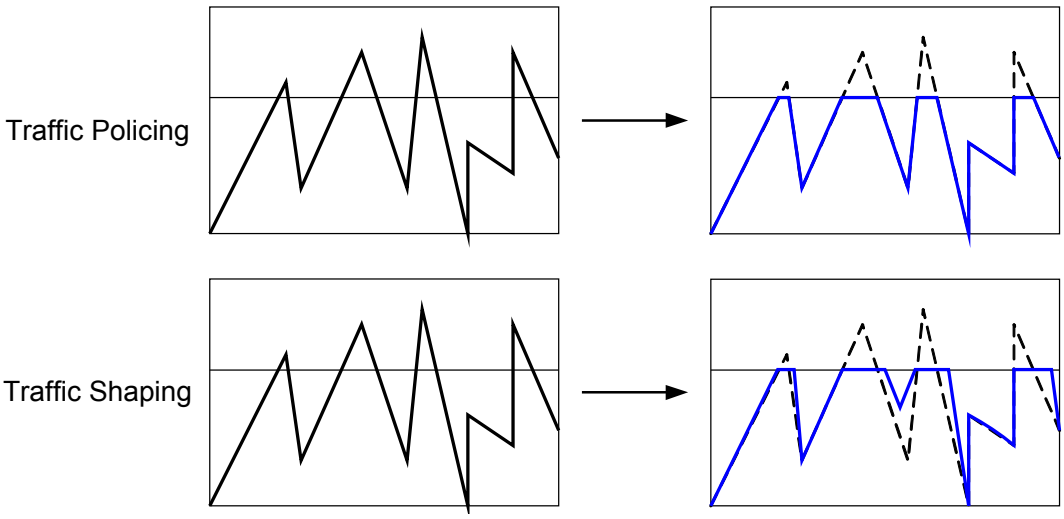
- Traffic policing directly discards the packets whose rate exceeds the rate limit. Traffic shaping, however, buffers the packets whose rate is greater than the traffic shaping rate. When there are sufficient tokens in the token bucket, the device forwards buffered packets at an even rate.
- Traffic shaping increases the delay, whereas traffic policing does not.

Table 8-1 Differences between traffic policing and traffic shaping

Type	Advantage	Disadvantage
Traffic shaping	Discards less packets.	Increases the delay and jitter. More buffer resources are required to buffer packets.
Traffic policing	Supports the re-marking action. No extra buffer is needed.	Discards more packets. Packets may be retransmitted.

Figure 8-1 shows the differences between traffic shaping and traffic policing.

Figure 8-1 Differences between traffic policing and traffic shaping



8.1.2.1 Token Bucket

Overview

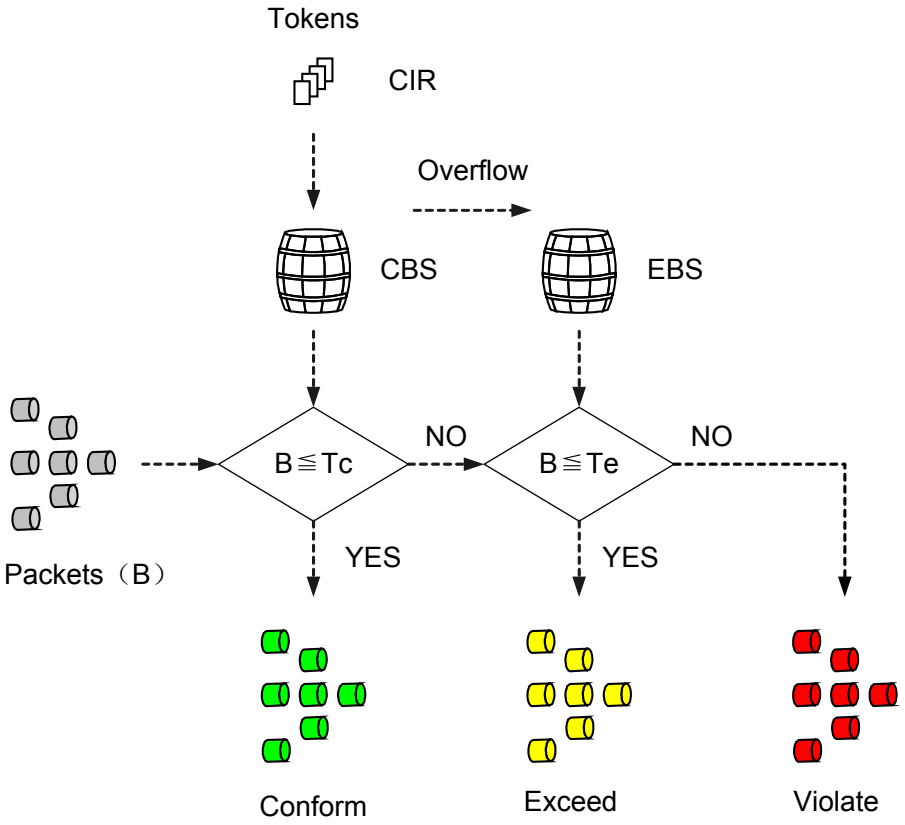
A token bucket has specified capacity to store tokens. The system places tokens into a token bucket at the configured rate. If the token bucket is full, excess tokens overflow and no token is added.

When assessing traffic, a token bucket forwards packets based on the number of tokens in the token bucket. If there are enough tokens in the token bucket for forwarding packets, the traffic rate is within the rate limit. Otherwise, the traffic rate is not within the rate limit.

Dual Buckets at a Single Rate

Dual buckets at a single rate use A Single Rate Three Color Marker (srTCM) defined in RFC 2697 to assess traffic and mark packets in green, yellow, and red based on the assessment result.

Figure 8-2 Dual buckets at a single rate



As shown in **Figure 8-2**, the two buckets are called bucket C and bucket E. Tc indicates the number of tokens in bucket C, and Te indicates the number of tokens in bucket E. Dual buckets at a single rate use the following parameters:

- CIR: indicates the rate at which tokens are put into bucket C, that is, average traffic rate permitted by bucket C.
- CBS: indicates the capacity of bucket C, that is, maximum volume of burst traffic allowed by bucket C each time.
- Excess burst size (EBS): indicates the capacity of bucket E, that is, maximum volume of excess burst traffic allowed by bucket E each time.

The system places tokens into the bucket at the CIR:

- If Tc is smaller than the CBS, Tc increases.
- If Tc is equal to the CBS and Te is smaller than the EBS, Te increases.
- If Tc is equal to the CBS and Te is equal to the EBS, Tc and Te do not increase.

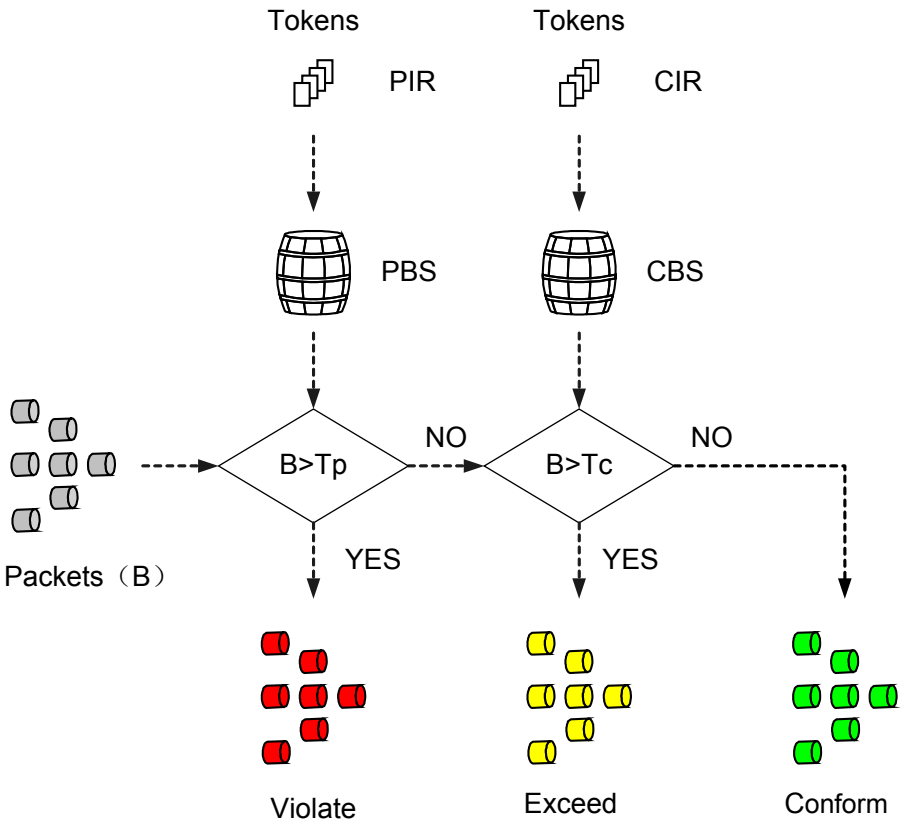
B indicates the size of an arriving packet:

- If B is smaller than or equal to Tc, the packet is colored green, and Tc decreases by B.
- If B is larger than Tc and smaller than or equal to Te, the packet is colored yellow and Te decreases by B.
- If B is larger than Te, the packet is colored red, and Tc and Te remain unchanged.

Dual Buckets at Dual Rates

Dual buckets at dual rates use A Two Rate Three Color Marker (trTCM) defined in RFC 2698 to assess traffic and mark packets in green, yellow, and red based on the assessment result.

Figure 8-3 Dual buckets at dual rates



As shown in **Figure 8-3**, the two buckets are called bucket P and bucket C. Tp indicates the number of tokens in bucket P, and Tc indicates the number of tokens in bucket C. Dual buckets at dual rates use the following parameters:

- Peak information rate (PIR): indicates the rate at which tokens are put into bucket P, that is, maximum traffic rate permitted by bucket P. The PIR must be greater than the CIR.
- CIR: indicates the rate at which tokens are put into bucket C, that is, average traffic rate permitted by bucket C.
- Peak burst size (PBS): indicates the capacity of bucket P, that is, maximum volume of burst traffic allowed by bucket P each time.
- CBS: indicates the capacity of bucket C, that is, maximum volume of burst traffic allowed by bucket C each time.

The system places tokens into bucket P at the PIR and places tokens into bucket C at the CIR:

- If Tp is smaller than the PBS, Tp increases. If Tp is larger than or equal to the PBS, Tp remains unchanged.

- If Tc is smaller than the CBS, Tc increases. If Tc is larger than or equal to the CBS, Tp remains unchanged.

B indicates the size of an arriving packet:

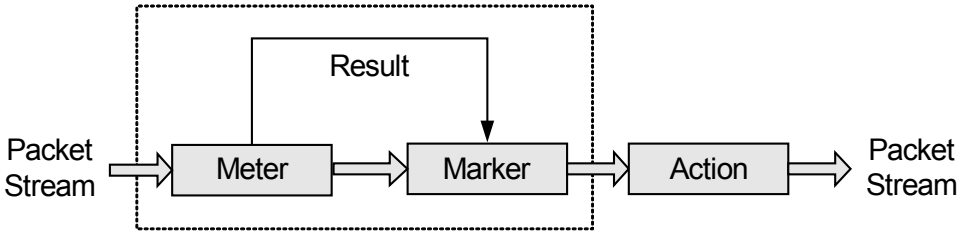
- If B is larger than Tp, the packet is colored red.
- If B is larger than Tc and smaller than or equal to Tp, the packet is colored yellow and Tp decreases by B.
- If B is smaller than or equal to Tc, the packet is colored green, and Tp and Tc decrease by B.

8.1.2.2 Traffic Policing

Traffic policing discards excess traffic to limit the traffic within a specified range and to protect network resources as well as the enterprise benefits.

Implementation of Traffic Policing

Figure 8-4 Traffic policing components



As shown in **Figure 8-4**, traffic policing involves the following components:

- Meter: measures the network traffic using the token bucket mechanism and sends the measurement result to the marker.
- Marker: colors packets in green, yellow, or red based on the measurement result received from the meter.
- Action: performs actions based on packet coloring results received from the marker. The following actions are defined:
  - Pass: forwards the packets that meet network requirements.
  - Remark + pass: changes the local priorities of packets and forwards them.
  - Discard: drops the packets that do not meet network requirements.

  By default, green and yellow packets are forwarded, and red packets are discarded.

If the rate of a type of traffic exceeds the threshold, the device reduces the packet priority and then forwards the packets or directly discards the packets based on traffic policing configuration. By default, the packets are discarded.

8.1.3 Default Configuration

This section provides the default traffic policing configurations.

Table 8-2 lists the default traffic policing configuration.

Table 8-2 Default traffic policing configuration

Parameter	Default Setting
Interface-based traffic policing	Disabled

8.1.4 Configuring Traffic Policing

Interface-based traffic policing allows the device to limit the rate of all service traffic on an interface. Flow-based traffic policing allows the device to limit the rate of packets matching traffic classification rules.

Pre-configuration Tasks

Before configuring traffic policing, complete the following tasks:

- Configuring link layer attributes of interfaces to ensure that the interfaces work properly
- Configuring IP addresses and routing protocols for interfaces to ensure connectivity

8.1.4.1 Configuring Interface-based Traffic Policing

Context

To limit the rate of traffic on an interface, configure traffic policing on the interface. If the rate of received or sent packets exceeds the rate limit, the device discards packets.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
qos car inbound cir cir-value [ cbs cbs-value [ pbs pbs-value ] | pir pir-value
[ cbs cbs-value pbs pbs-value ] ]
```

Traffic policing is configured in the inbound direction on an interface.

----End

8.1.4.2 Checking the Configuration

Procedure

- Run the **display qos car statistics interface** *interface-type interface-number* { **inbound** | **outbound** } command to check statistics about forwarded and discarded packets on the interface.

----End

8.1.5 Configuration Examples

This section provides several configuration examples of traffic policing and traffic shaping.

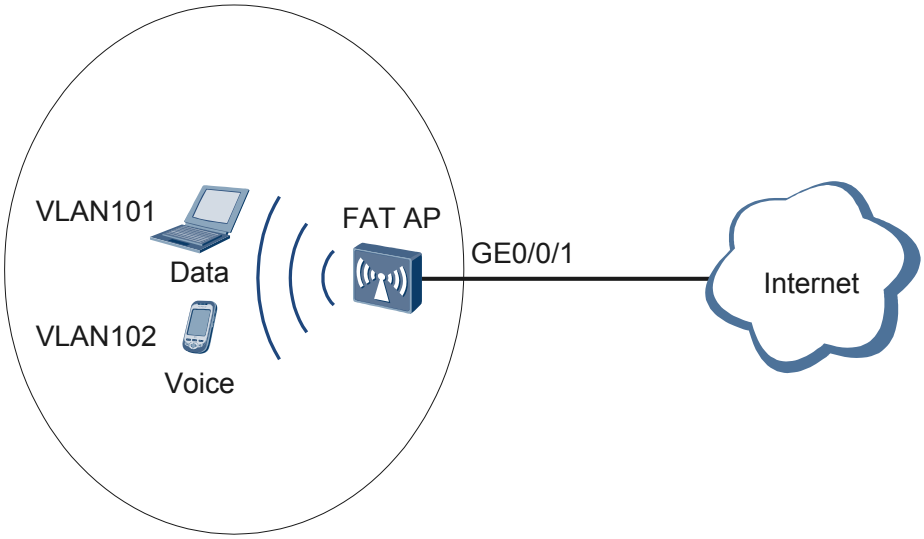
8.1.5.1 Example for Configuring Interface-based Traffic Policing

Networking Requirements

As shown in **Figure 8-5**, a Fat AP accesses the Internet through wired connections and connects to STAs wirelessly.

It is required that the bandwidth for voice services be 8 Mbit/s and for data services be 5 Mbit/s.

Figure 8-5 Networking diagram of interface-based traffic policing



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic WLAN services to ensure interworking.
2. Configure traffic policing in the inbound direction of WLAN-BSS interfaces.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101 and VLAN 102.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101 102
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
[AP] interface vlanif 102
[AP-Vlanif101] ip address 192.168.12.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm**.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind the WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Configure traffic policing in the inbound direction of WLAN-BSS interfaces

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] qos car inbound cir 8192
[AP-Wlan-Bss1] quit
[AP] interface wlan-bss 2
[AP-Wlan-Bss2] port hybrid pvid vlan 102
[AP-Wlan-Bss2] port hybrid untagged vlan 102
[AP-Wlan-Bss2] qos car inbound cir 5120
[AP-Wlan-Bss2] quit
```

Create a security profile named **security**.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic**.
```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Configure service sets and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test1 id 1
[AP-wlan-service-set-test] ssid test1
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] service-set name test2 id 2
[AP-wlan-service-set-test] ssid test2
[AP-wlan-service-set-test] wlan-bss 2
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test1
[AP-Wlan-Radio0/0/0] service-set name test2
[AP-Wlan-Radio0/0/0] quit
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.12.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 qos car inbound cir 8192 cbs 1540096 pbs 2564096
#
interface Wlan-Bss2
 port hybrid pvid vlan 102
 port hybrid untagged vlan 102
 qos car inbound cir 5120 cbs 962560 pbs 1602560
#
wlan
```

```
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test1 id 1
  Wlan-Bss 1
  ssid test1
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
 service-set name test2 id 2
  Wlan-Bss 2
  ssid test2
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
 service-set id 2 wlan 2
#
return
```

8.2 ACL-based Simplified Traffic Policy Configuration

The device to which an ACL-based simplified traffic policy is applied filters packets matching ACL rules.

8.2.1 ACL-based Simplified Traffic Policy Overview

The device to which an ACL-based simplified traffic policy is applied matches packet characteristics with ACLs and provides the same QoS for packets matching ACL rules, implementing differentiated services.

To control traffic entering a network, configure an ACL to match information such as the source IP address, fragment flag, destination IP address, source port number, and source MAC address and then configure an ACL-based simplified traffic policy so that the device can filter packets matching ACL rules.

Compared with a traffic policy based on traffic classifiers, an ACL-based simplified traffic policy is easy to configure because you do not need to configure a traffic classifier, traffic behavior, or traffic policy independently. However, an ACL-based simplified traffic policy defines less matching rules than a traffic policy based on traffic classifiers.

8.2.2 Configuring ACL-based Packet Filtering

By configuring ACL-based packet filtering, the device permits or rejects packets matching ACL rules to control network traffic.

Pre-configuration Tasks

Before configuring ACL-based packet filtering, complete the following tasks:

- Configuring link layer attributes of interfaces to ensure that the interfaces work properly
- Configuring IP addresses and routing protocols for interfaces to ensure connectivity

- Configuring an ACL

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
traffic-filter { inbound | outbound } acl { acl-number | name acl-name }
```

ACL-based packet filtering is configured.

----End

Checking the Configuration

- Run the **display traffic-filter applied-record** command to check ACL-based packet filtering information.
- Run the **display traffic-filter statistics interface** *interface-type interface-number* { **inbound** | **outbound** } command to view traffic statistics about ACL-based packet filtering on an interface.

8.2.3 Maintaining an ACL-based Simplified Traffic Policy

This section describes how to maintain an ACL-based simplified traffic policy.

8.2.3.1 Displaying Statistics on ACL-based Packet Filtering

Context

After ACL-based packet filtering is configured on an interface, you can run the following command to view statistics on forwarded and discarded packets.

Procedure

- Run the **display traffic-filter statistics interface** *interface-type interface-number* { **inbound** | **outbound** } command to view traffic statistics about ACL-based packet filtering on an interface.

----End

8.2.3.2 Clearing Statistics on ACL-based Packet Filtering

Context

To recollect statistics on ACL-based packet filtering, run the following command to clear existing statistics.

NOTICE

The cleared statistics on ACL-based packet filtering cannot be restored. Exercise caution when you run the command.

Procedure

- Run the **reset traffic-filter statistics interface** *interface-type interface-number* { **inbound** | **outbound** } command to view clear statistics about ACL-based packet filtering on an interface.

----End

8.3 WLAN QoS Configuration

WLAN QoS enables network administrators to plan and allocate network resources based on service characteristics, meeting user requirements and improving network usage.

8.3.1 Introduction to WLAN QoS

This section describes the definition, background, and functions of WLAN QoS.

Definition

WLAN Quality of Service (QoS) provides differentiated service for wireless users to satisfy their traffic requirements. WLAN QoS has the following functions:

1. High-efficiency use of wireless channels: The Wi-Fi multimedia (WMM) standard enables the high-priority users to preempt wireless channels.
2. Efficient bandwidth use: Priority mapping preferentially transmits the data of high-priority users.
3. Network congestion prevention: Traffic policing limits users' transmission rate, preventing network congestion.
4. Differentiated services for different types of packets: The same QoS services are provided for packets that match a specified ACL. In this way, differentiated services are implemented for different types of packets.

Purpose

Applications have differentiated network requirements. The traditional WLAN is mainly used to transmit data due to its low transmission rate. With development of new WLAN technologies, WLANs have been applied to media, financial, education, and enterprise networks. In addition to data traffic, WLANs can also transmit delay-sensitive multimedia data, such as voice and

video. By enforcing QoS policies on a WLAN, the network administrator can properly plan and assign network resources based on service characteristics. The WLAN then provides differentiated access services for applications, meeting customer requirements and improving network use efficiency.

8.3.2 Principles

This section describes the implementation of WLAN QoS.

8.3.2.1 WMM

Background

Before learning WMM, you must understand 802.11 link layer transport mechanism.

802.11 MAC layer uses the coordination function to determine the data transmitting and receiving methods used between STAs in a BSS. 802.11 MAC layer consists of two sub-layers:

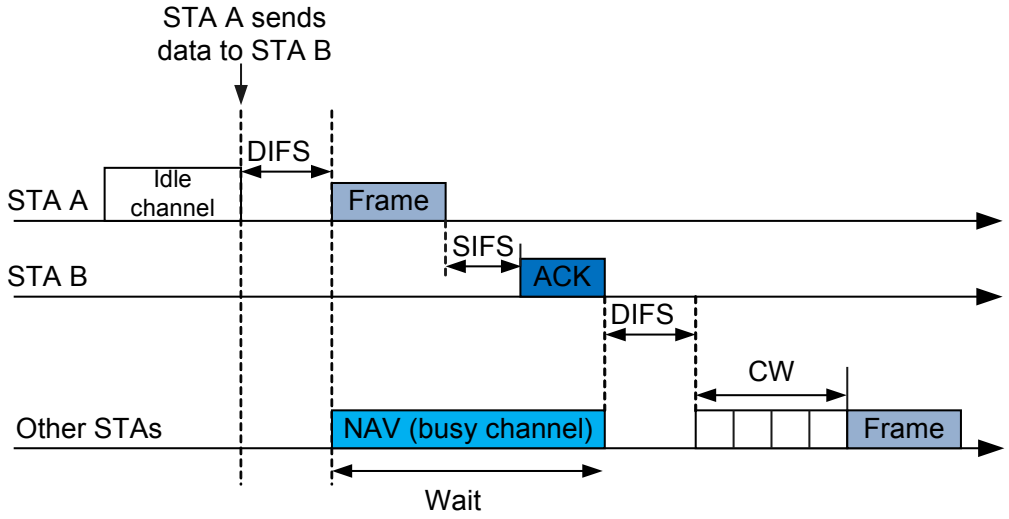
- Distributed Coordination Function (DCF): uses the CSMA/CA mechanism. STAs compete channels to obtain the authority to transmit data frames.
- Point Coordination Function (PCF): uses centralized control to authorize STAs to transmit data frames in turn. This method prevents conflict.

NOTE

In 802.11 protocol, DCF is mandatory, and PCF is optional.

Figure 8-6 shows how CSMA/CA is implemented.

Figure 8-6 CSMA/CA working mechanism



1. Before sending data to STA B, STA A detects channel status. When detecting an idle channel, STA A sends a data frame after Distributed Inter-Frame Space (DIFS) times out and waits for a response from STA B. The data frame contains NAV information. After

receiving the data frame, STA B updates the NAV information, indicating that the channel is busy and data transmission will be delayed.

NOTE

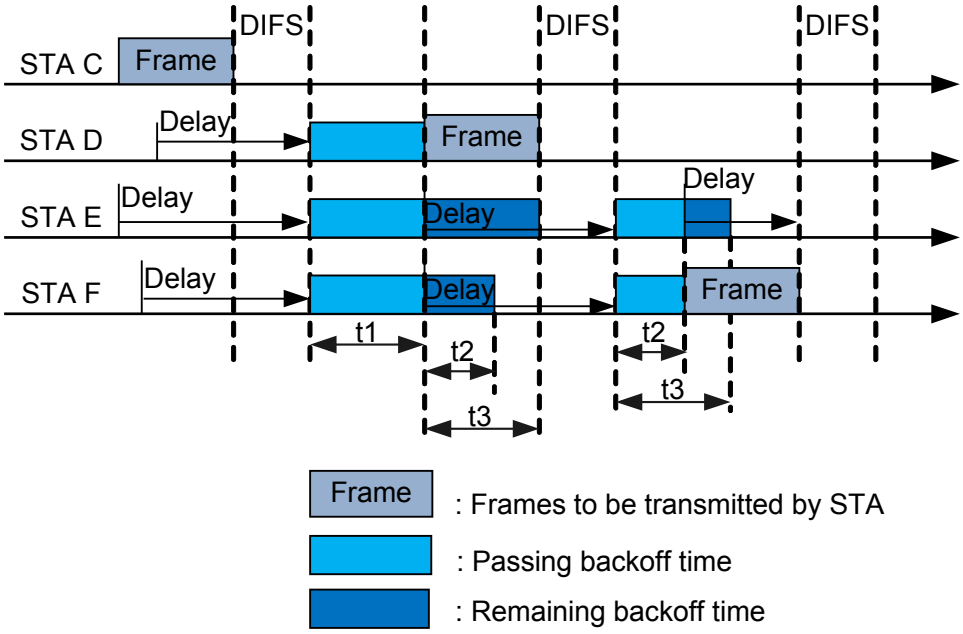
According to 802.11 protocol, the receiver must return an ACK frame each time it receives a data frame.

2. STA B receives the data frame, waits until Short Interframe Space (SIFS) times out, and sends an ACK frame to STA A. After the ACK frame is transmitted, the channel becomes idle. After the DIFS times out, the STAs use the exponential backoff algorithm to compete channels. The STA of which the backoff counter is first reduced to 0 starts to send data frame.

Concepts

- InterFrame Space (IFS): According to 802.11 protocol, after sending a data frame, the STA must wait until the IFS times out, and then sends the next data frame. The IFS length depends on the data frame type. The high-priority data frames are sent earlier than the low-priority data frames. There are three IFS types:
  - Short IFS (SIFS): It is the time interval between a data frame and its ACK frame. SIFS is used for high priority transmissions, for example, transmissions of ACK and CTS frames.
  - PCF IFS (PIFS): PCF-enabled access points wait for PIFS duration rather than DIFS to occupy the wireless medium. PIFS length is SIFS plus slot time. If an STA accesses a channel when the slot time starts, the other STAs in the BSS detect that the channel is busy when the next slot time starts.
  - DCF IFS (DIFS): Data frames and management frames are transmitted at the DIFS interval. DIFS length is PIFS plus slot time.
- Contention window: backoff time. When multiple STAs need to transmit data and detect that all channels are busy, the STAs use the backoff algorithm. That is, the STAs wait for a random number of slot times, and then transmit data. Backoff time is a multiple of slot time, and its length depends on the physical layer technology. An STA detect channel status at the interval of slot time. When detecting an idle channel, the STA starts the backoff timer. If all channels become busy, the STA freezes the remaining time in the backoff timer. When a channel becomes idle, the STA waits until DIFS times out, and continues the backoff timer. When the backoff timer is reduced to 0, the STA starts to send data frames. **Figure 8-7** shows the data frame transmission process.

Figure 8-7 Backoff algorithm diagram



1. STA C is occupying a channel to send data frames. STA D, STA E, and STA F also need to send data frames. They detect that the channel is busy, so they wait.
2. After STA C finishes data frame transmission, the other STAs wait until DIFS times out. When DIFS times out, the STAs generate random backoff time and start their backoff timers. For example, the backoff time of STA D is t1, the backoff time of STA E is t1+t3, and the backoff time of STA F is t1+t2.
3. When t1 times out, the backoff timer of STA D is reduced to 0. STA D starts to send data frames.
4. STA E and STA F detect that the channel is busy, so they freeze their backoff timers and wait. After STA D completes data transmission, STA E and STA F wait until DIFS times out, and continue their backoff timers.
5. When t2 times out, the backoff timer of STA F is reduced to 0. STA F starts to send data frames.

Principles

Channel competition is based on DCF. To all STAs, the DIFS is fixed and backoff time is random; therefore, all the STAs fairly compete channels. WMM is an enhancement to 802.11 protocol. It makes channel competition unfair.

- **EDCA parameters**

  WMM defines a set of Enhanced Distributed Channel Access (EDCA) parameters, which distinguish high priority packets and enables the high priority packets to preempt channels.

  WMM classifies data packets into four access categories (ACs). **Table 8-3** shows the mappings between ACs and 802.11 user preferences (UPs). A large UP value indicates a high priority.

Table 8-3 Mappings between ACs and UPs

UP	AC
7	AC_VO (Voice)
6	
5	AC_VI (Video)
4	
3	AC_BE (Best Effort)
0	
2	AC_BK (Background)
1	

Each AC queue defines a set of EDCA parameters, which determine the capability of occupying channels. These parameters ensure that the high priority ACs have higher probability to preempt channels than low priority ACs.

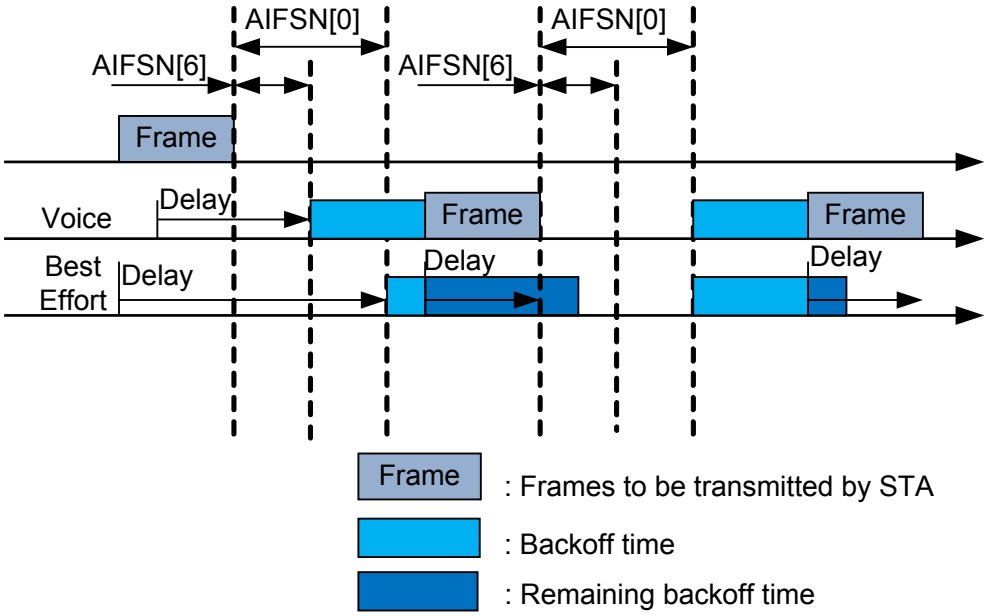
Table 8-4 describes the EDCA parameters.

Table 8-4 EDCA parameter description

Parameter	Meaning
Arbitration Inter Frame Spacing Number (AIFSN)	The DIFS has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value means that the STA must wait for a long time and has a low priority.
Exponent form of CWmin (ECWmin) and Exponent form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. They determine the average backoff time. Large ECWmin and ECWmax values mean that the average backoff time for the STA is long and the STA priority is low.
Transmission Opportunity Limit (TXOPLimit)	After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can send only one data frame every time it preempts a channel.

As shown in **Figure 8-8**, the AIFSN (AIFSN[6]) and backoff time of voice packets are shorter than those of Best Effort packets. When both voice packets and Best Effort packets need to be sent, voice packets can preempt the channel.

Figure 8-8 WMM working mechanism



- **ACK policy**

  WMM defines two ACK policies: normal ACK and no ACK.

  - Normal ACK: The receiver must return an ACK frame each time it receives a unicast packet.
  - No ACK: The receiver does not need to return ACK frames after receiving packets. This mode is applicable to the environment that has high communication quality and little interference.

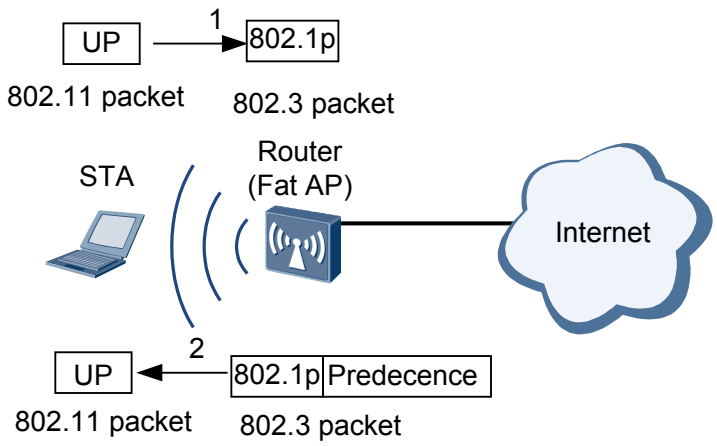
    NOTE

    - The ACK policy is only valid to APs.
    - If communication quality is poor, the no ACK policy may cause more packets to be lose.

8.3.2.2 Priority Mapping

Packets of different types have different priorities. For example, the 802.11 packets sent by STAs carry user priorities, VLAN packets on the wired networks carry 802.1p priorities, and IP packets carry precedence values or DSCP priorities. Priority mapping must be configured on network devices to retain priorities of packets when the packets traverse different networks.

Figure 8-9 Priority mapping diagram



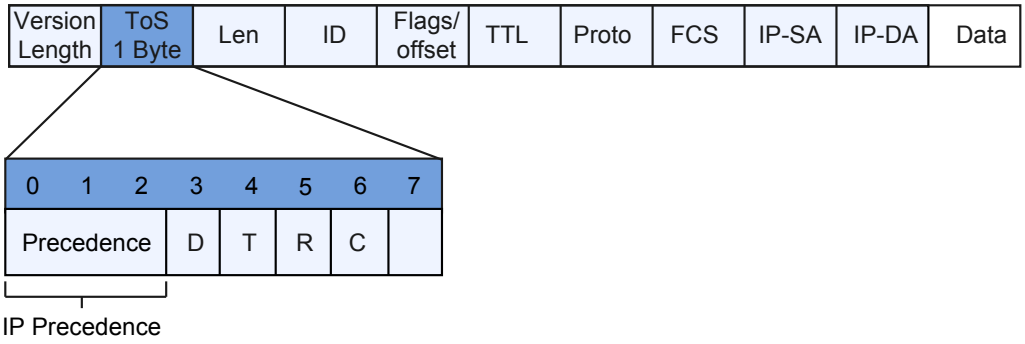
As shown in **Figure 8-9**:

1. After receiving the upstream 802.11 frames from the STA, the AP maps the user priorities to the 802.1p priorities.
2. After receiving the downstream 802.3 frames, the AP maps the 802.1p priorities or precedence values to the user priority.

Precedence field

As defined in RFC 791, the 8-bit ToS field in an IP packet header contains a 3-bit IP precedence field. **Figure 8-10** shows the Precedence field in an IP packet. Bits 0 to 2 constitute the Precedence field, representing precedence values 7, 6, 5, 4, 3, 2, 1 and 0 in descending order of priority.

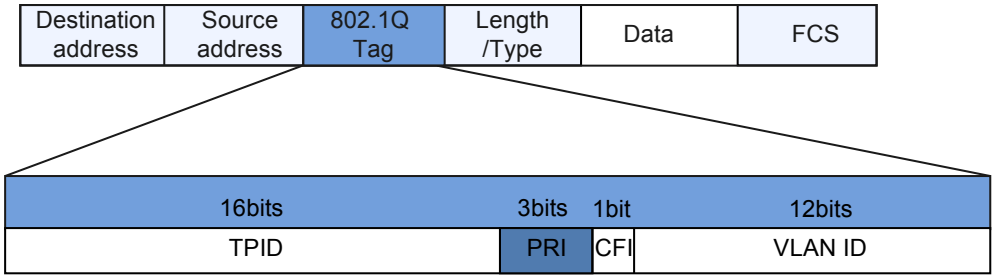
Figure 8-10 IP Precedence field



802.1p Field

Layer 2 devices exchange ethernet frames. As defined in IEEE 802.1Q, the PRI field (802.1p field) in the ethernet frame header identifies the Class of Service (CoS) requirement. **Figure 8-11** shows the PRI field in ethernet frames.

Figure 8-11 802.1p field in the Ethernet frame with VLAN tags



The 802.1Q header contains a 3-bit PRI field, representing eight service priorities 7, 6, 5, 4, 3, 2, 1 and 0 in descending order of priority.

8.3.2.3 Traffic Policing

Traffic policing discards excess traffic to limit the traffic within a specified range and to protect network resources as well as the enterprise benefits.

Traffic policing is implemented using the token bucket.

A token bucket has specified capacity to store tokens. The system places tokens into a token bucket at the configured rate. If the token bucket is full, excess tokens overflow and no token is added.

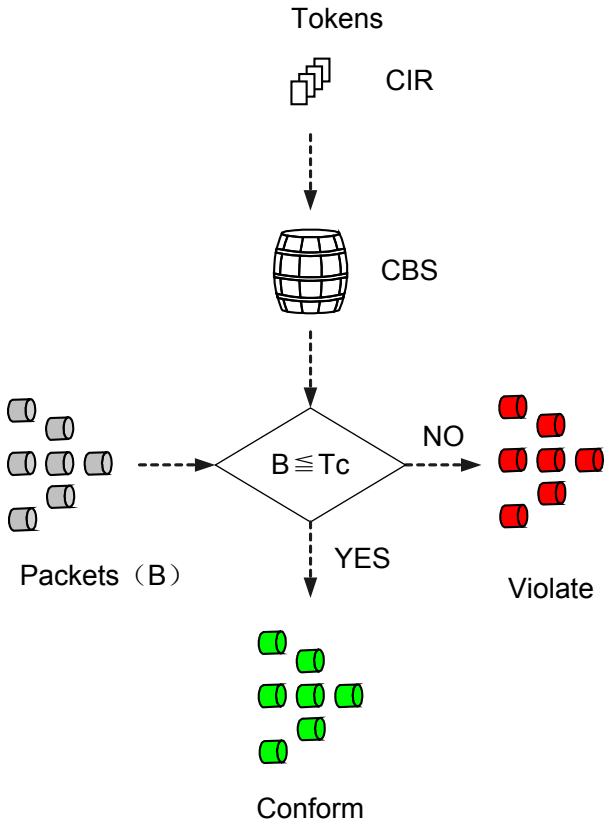
When assessing traffic, a token bucket forwards packets based on the number of tokens in the token bucket. If there are enough tokens in the token bucket for forwarding packets, the traffic rate is within the rate limit. Otherwise, the traffic rate is not within the rate limit.

The working mechanisms of token buckets include single rate single bucket, single rate dual bucket, and dual rate dual bucket.

Single Bucket at a Single Rate

If burst traffic is not allowed, the EBS is set to 0 in dual buckets at a single rate. The number of tokens in bucket E is always 0, that is, one token bucket is used.

Figure 8-12 Single bucket at a single rate



As shown in **Figure 8-12**, the bucket is called bucket C. Tc indicates the number of tokens in bucket C. A single bucket at a single rate uses the following parameters:

- Committed Information Rate (CIR): indicates the rate at which tokens are put into bucket C, that is, the average traffic rate permitted by bucket C.
- Committed burst size (CBS): indicates the capacity of bucket C, that is, maximum volume of burst traffic allowed by bucket C each time.

The system places tokens into the bucket at the CIR. If Tc is smaller than the CBS, Tc increases. If Tc is smaller than or equal to the CBS, Tc remains unchanged.

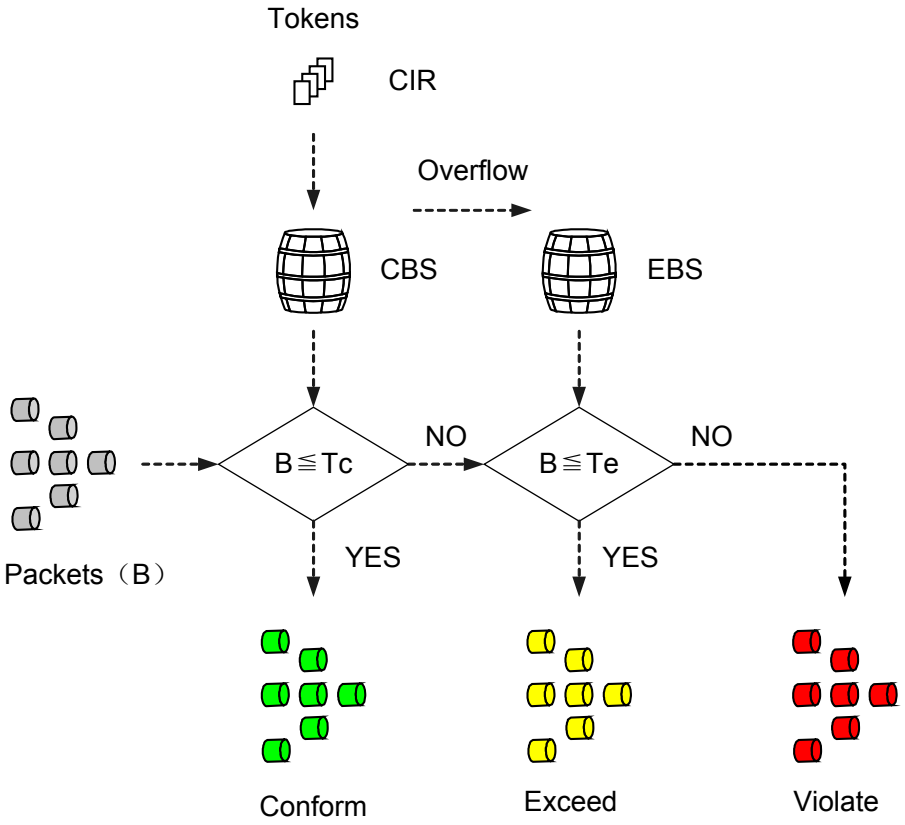
B indicates the size of an arriving packet:

- If B is smaller than or equal to Tc, the packet is colored green, and Tc decreases by B.
- If B is greater than Tc, the packet is colored red, and Tc remains unchanged.

Dual Buckets at a Single Rate

Dual buckets at a single rate use A Single Rate Three Color Marker (srTCM) defined in RFC 2697 to assess traffic and mark packets in green, yellow, and red based on the assessment result.

Figure 8-13 Dual buckets at a single rate



As shown in **Figure 8-13**, the two buckets are called bucket C and bucket E. Tc indicates the number of tokens in bucket C, and Te indicates the number of tokens in bucket E. Dual buckets at a single rate use the following parameters:

- CIR: indicates the rate at which tokens are put into bucket C, that is, average traffic rate permitted by bucket C.
- CBS: indicates the capacity of bucket C, that is, maximum volume of burst traffic allowed by bucket C each time.
- Excess burst size (EBS): indicates the capacity of bucket E, that is, maximum volume of excess burst traffic allowed by bucket E each time.

The system places tokens into the bucket at the CIR:

- If Tc is smaller than the CBS, Tc increases.
- If Tc is equal to the CBS and Te is smaller than the EBS, Te increases.
- If Tc is equal to the CBS and Te is equal to the EBS, Tc and Te do not increase.

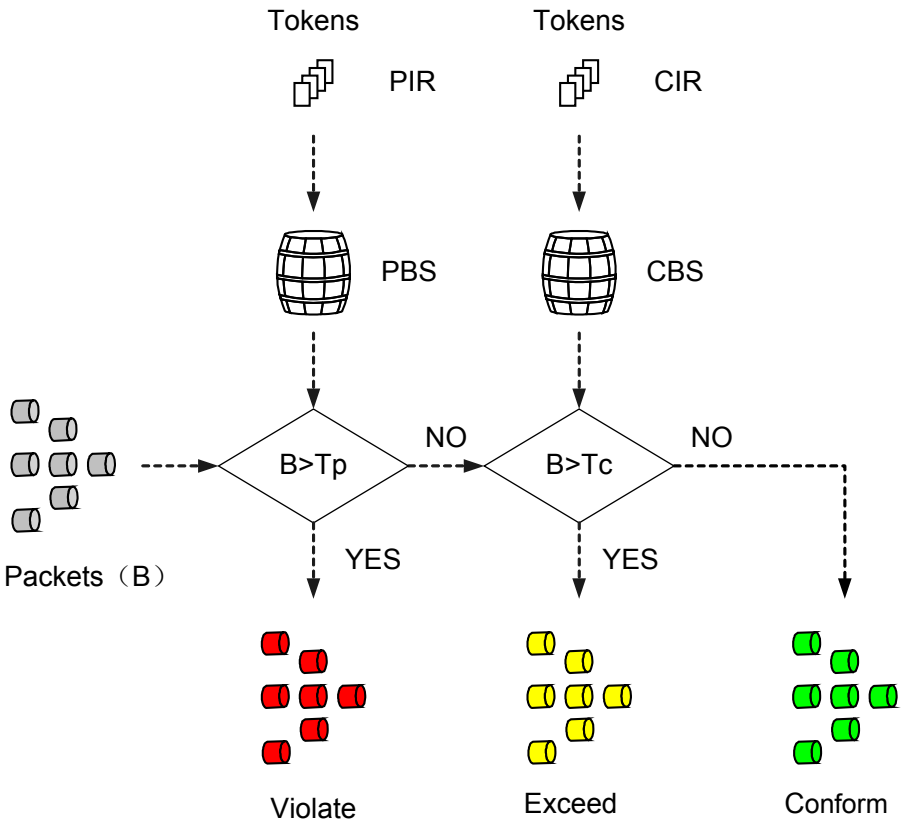
B indicates the size of an arriving packet:

- If B is smaller than or equal to Tc, the packet is colored green, and Tc decreases by B.
- If B is larger than Tc and smaller than or equal to Te, the packet is colored yellow and Te decreases by B.
- If B is larger than Te, the packet is colored red, and Tc and Te remain unchanged.

Dual Buckets at Dual Rates

Dual buckets at dual rates use A Two Rate Three Color Marker (trTCM) defined in RFC 2698 to assess traffic and mark packets in green, yellow, and red based on the assessment result.

Figure 8-14 Dual buckets at dual rates



As shown in **Figure 8-14**, the two buckets are called bucket P and bucket C. Tp indicates the number of tokens in bucket P, and Tc indicates the number of tokens in bucket C. Dual buckets at dual rates use the following parameters:

- Peak information rate (PIR): indicates the rate at which tokens are put into bucket P, that is, maximum traffic rate permitted by bucket P. The PIR must be greater than the CIR.
- CIR: indicates the rate at which tokens are put into bucket C, that is, average traffic rate permitted by bucket C.
- Peak burst size (PBS): indicates the capacity of bucket P, that is, maximum volume of burst traffic allowed by bucket P each time.
- CBS: indicates the capacity of bucket C, that is, maximum volume of burst traffic allowed by bucket C each time.

The system places tokens into bucket P at the PIR and places tokens into bucket C at the CIR:

- If Tp is smaller than the PBS, Tp increases. If Tp is larger than or equal to the PBS, Tp remains unchanged.

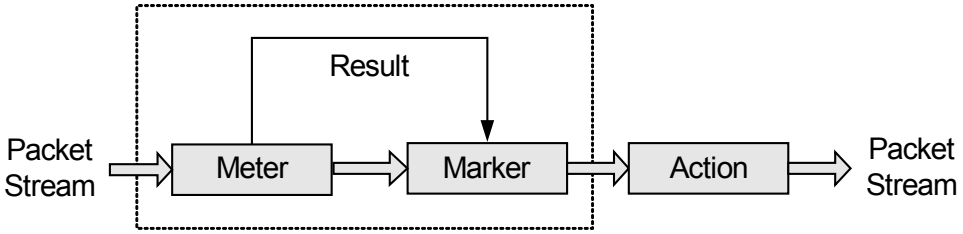
- If Tc is smaller than the CBS, Tc increases. If Tc is larger than or equal to the CBS, Tp remains unchanged.

B indicates the size of an arriving packet:

- If B is larger than Tp, the packet is colored red.
- If B is larger than Tc and smaller than or equal to Tp, the packet is colored yellow and Tp decreases by B.
- If B is smaller than or equal to Tc, the packet is colored green, and Tp and Tc decrease by B.

Implementation of Traffic Policing

Figure 8-15 Traffic policing components



As shown in **Figure 8-15**, traffic policing involves the following components:

- Meter: measures the network traffic using the token bucket mechanism and sends the measurement result to the marker.
- Marker: colors packets in green, yellow, or red based on the measurement result received from the meter.
- Action: performs actions based on packet coloring results received from the marker. The following actions are defined:
  - Pass: forwards the packets that meet network requirements.
  - Remark + pass: changes the local priorities of packets and forwards them.
  - Discard: drops the packets that do not meet network requirements.

  By default, green and yellow packets are forwarded, and red packets are discarded.

If the rate of a type of traffic exceeds the threshold, the device reduces the packet priority and then forwards the packets or directly discards the packets based on traffic policing configuration. By default, the packets are discarded.

8.3.2.4 ACL-based Packet Filtering

The device to which an ACL-based simplified traffic policy is applied matches packet characteristics with ACLs and provides the same QoS for packets matching ACL rules, implementing differentiated services.

To control traffic entering a network, configure an ACL to match information such as the source IP address, fragment flag, destination IP address, source port number, and source MAC address

and then configure an ACL-based simplified traffic policy so that the device can filter packets matching ACL rules.

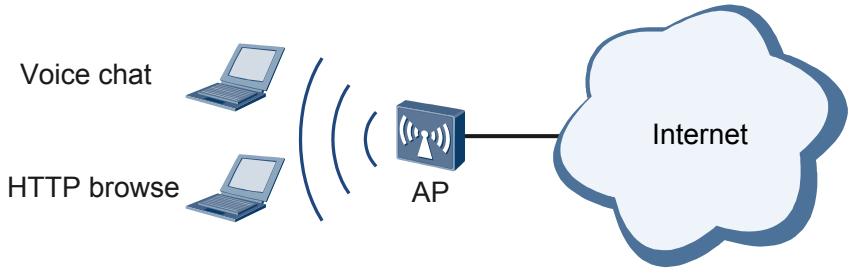
Compared with a traffic policy based on traffic classifiers, an ACL-based simplified traffic policy is easy to configure because you do not need to configure a traffic classifier, traffic behavior, or traffic policy independently. However, an ACL-based simplified traffic policy defines less matching rules than a traffic policy based on traffic classifiers.

8.3.3 Applicable Scenario

This section describes application scenarios of WLAN QoS

As shown in **Figure 8-16**, network bandwidth is limited. The device needs to provide differentiated services for services, for example, reducing jitter and latency of voice packets and guaranteeing bandwidth for key services.

Figure 8-16 WLAN QoS networking diagram



- By using WMM, voice or video data can preempt wireless channels.
- By using priority mapping, high priority data is transmitted first.
- By using traffic policing, user data rate is limited and network congestion is prevented.
- By using ACL-based packet filtering, packets that match the same ACL are provided with the same QoS services. In this way, differentiated services are implemented for different types of packets.

8.3.4 Configuration Task Summary

After basic WLAN service configurations are complete, STAs can access the wireless network. In addition to basic WLAN QoS policies, you can also configure other WLAN QoS policies according to the reference sections provided in the following table.

Table 8-5 WLAN QoS configuration tasks

Task	Configuration	Description
Configure WMM	**8.3.6 Configuring WMM**	Mandatory
Configure Priority Mapping	**8.3.7 Configuring Priority Mapping**	Mandatory
Configure Traffic Policing	**8.3.8 Configuring Traffic Policing**	Optional

Task	Configuration	Description
Configure ACL-based Packet Filtering	8.3.9 Configuring ACL-based Packet Filtering	Optional

8.3.5 Default Configuration

This section provides the default WLAN QoS configuration.

Table 8-6 Default WLAN QoS configuration

Parameter	Default Setting
WMM	Enabled
Whether STAs that do not support WMM are allowed to connect to a WMM-enabled AP	Yes
Priorities of AC queues	AC_VO (Voice) > AC_VI (Video) > AC_BE (Best Effort) > AC_BK (Background)
Traffic policing	Disabled
Mappings from user priorities of 802.11 packets to 802.1p priorities of 802.3 packets when data packets are sent from STAs to an AP.	User priority 0 maps 802.1p priority 0, user priority 1 maps 802.1p priority 1, and so on.
Mappings from Precedence priorities of 802.3 packets to user priorities of 802.11 packets when data packets are sent from the Internet to an AP.	IP precedence 0 maps user priority 0, IP precedence 1 maps user priority 1, and so on.
ACL-based packet filtering	Disabled

8.3.6 Configuring WMM

You can configure WMM profiles to provide different capabilities for different services on STAs or APs to compete for channels to determine the quality of services.

Pre-configuration Tasks

Before configuring WMM, complete the following task:

- Configuring Basic WLAN Services

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
wmm-profile { id profile-id | name profile-name } *
```

The WMM profile view is displayed.

Step 4 (Optional) Run:

```
display wmm-profile { all | id profile-id | name profile-name }
```

The WMM profile configuration is displayed.

If the WMM configuration has not been modified, you can run the **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to view the default configuration of a WMM profile and determine whether to modify the WMM configuration.

Step 5 Run:

```
wmm enable
```

WMM is enabled.

By default, WMM is enabled.

NOTE

By default, WMM is disabled on a terminal. To implement the WMM function, you must enable WMM on terminals and devices concurrently.

Step 6 (Optional) Run:

```
wmm mandatory enable
```

STAs that do not support WMM are not allowed to connect to a WMM-enabled AP.

By default, STAs that do not support WMM are allowed to connect to a WMM-enabled AP.

On a WLAN, wireless channels are open and all STAs have the same chance to occupy a channel. You can configure WMM to distinguish high-priority packets and enable the high-priority packets to preempt channels. You can also disable STAs that do not support WMM from connecting to a WMM-enabled AP, which prevents those STAs from preempting channels of WMM-capable STAs.

Step 7 Run:

```
wmm edca client { ac-vo | ac-vi | ac-be | ac-bk } { aifsn aifsn-value | ecw ecwmin ecwmin-value ecwmax ecwmax-value | txoplimit txoplimit-value } *
```

EDCA parameters are set for STAs.

Table 8-7 lists the default EDCA parameter settings for STAs.

Table 8-7 Default EDCA parameter settings for STAs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit
AC_VO	3	2	2	47
AC_VI	4	3	2	94
AC_BE	10	4	3	0
AC_BK	10	4	7	0

As shown in the table, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority.

Step 8 Run:

wmm edca ap { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *

EDCA parameters are set for APs.

Table 8-8 lists the default EDCA parameter settings and ACK policy for APs.

Table 8-8 Default EDCA parameter settings and ACK policy for APs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	3	2	1	47	normal
AC_VI	4	3	1	94	normal
AC_BE	6	4	3	0	normal
AC_BK	10	4	7	0	normal

As shown in the table, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority.

NOTE

After high-density AP deployment is enabled, APs optimize EDCA parameters of AC_BE packets and adjust the size of the contention window to reduce chances of collisions so that better experience can be provided for users in high-density access scenarios. If EDCA parameters have been configured in WMM profiles, EDCA parameters in AC_BE packets do not take effect.

----End

Checking the Configuration

- Run the **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check the WMM profile configuration.

8.3.7 Configuring Priority Mapping

You can configure priority mapping to distinguish data priority and ensure that data of high-priority users is transmitted first.

Pre-configuration Tasks

Before configuring priority mapping, complete the following task:

- **Configuring Basic WLAN Services**

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
wlan
```

The WLAN view is displayed.

Step 3 Run:

```
traffic-profile { name profile-name | id profile-id } *
```

The traffic profile view is displayed.

Step 4 Run the following commands as required to configure priority mapping.

- Use either of the following methods to set mappings from user priorities of 802.11 packets to 802.1p priorities of 802.3 packets when data packets are sent from STAs to an AP.
  - If you do not want to distinguish service priorities of 802.3 packets, map user priorities of all 802.11 packets to a specified 802.1p priority of 802.3 packets.

    Run:

    ```
    8021p designate value
    ```

    User priorities of all 802.11 packets are mapped to a specified 802.1p priority of 802.3 packets.
  - If you want to distinguish service priorities of 802.3 packets, map user priorities of 802.11 packets to different 802.1p priorities of 802.3 packets.

    Run:

    ```
    8021p up-mapping value0 value1 value2 value3 value4 value5 value6 value7
    ```

    User priorities of 802.11 packets are mapped to different 802.1p priorities of 802.3 packets.

    By default, mappings from user priorities of 802.11 packets to 802.1p priorities of 802.3 packets are shown in **Table 8-9**.

Table 8-9 Default mappings from user priorities of 802.11 packets to 802.1p priorities of 802.3 packets

User-Priority	802.1p
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

- Use either of the following methods to set mappings from 802.1p priorities of 802.3 packets to user priorities of 802.3 packets when data packets are sent from the Internet to an AP.
  - Run:

    8021p-map-up *value0 value1 value2 value3 value4 value5 value6 value7*

    802.1p priorities of 802.3 packets are mapped to user priorities of 802.11 packets.

    By default, mappings from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets are shown in **Table 8-10**.

    Table 8-10 Mappings from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets

802.1p	User-Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

  - Run:

    tos-map-up *value0 value1 value2 value3 value4 value5 value6 value7*

    IP precedences of 802.3 packets are mapped to user priorities of 802.11 packets.

By default, mappings from IP precedences of 802.3 packets to user priorities of 802.11 packets are shown in **Table 8-11**.

Table 8-11 Mappings from IP precedences to user priorities

Precedence	User-Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

----End

Checking the Configuration

- Run the **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check the priority mapping configuration in a traffic profile.

8.3.8 Configuring Traffic Policing

You can configure traffic policing to limit the STA transmission rate or AP forwarding rate, which prevents network congestion.

Context

To protect network resources and prevent network congestion, you can configure traffic policing to limit the rate of traffic entering the WLAN.

Traffic policing on a WLAN network:

- Traffic policing can be configured in a traffic profile to limit the rate of upstream and downstream traffic of a single user or all users on the VAP bound to the traffic profile.
- Traffic policing can be configured on a WLAN-BSS interface to limit the rate of upstream and downstream traffic of all users on the VAP bound to the WLAN-BSS interface.

Pre-configuration Tasks

Before configuring traffic policing, complete the following task:

Procedure

- Configuring traffic policing in a traffic profile

1. Run:
   system-view

   The system view is displayed.
2. Run:
   wlan

   The WLAN view is displayed.
3. Run:
   traffic-profile { **name** *profile-name* | **id** *profile-id* } *

   The traffic profile view is displayed.
4. Run:
   rate-limit vap { **up** | **down** } *rate-limit-value*

   The rate limit is configured for upstream and downstream traffic on all STAs associated with a VAP.

   By default, the rate limit for upstream and downstream traffic on all STAs associated with a VAP is 4294967295, in kbit/s.
5. Run:
   rate-limit client { **up** | **down** } *rate-limit-value*

   The rate limit is configured for upstream and downstream traffic on each STA associated with a VAP.

   By default, the rate limit for upstream and downstream traffic on each STA associated with a VAP is 4294967295, in kbit/s.

- Configure traffic policing on a WLAN-BSS interface

  In this method, the rate of all traffic is monitored and limited within a proper range so that network resources are protected.

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface wlan-bss *wlan-bss-number*

     The WLAN-BSS interface view is displayed.
  3. Run:
     qos car { **inbound** | **outbound** } **cir** *cir-value* [**cbs** *cbs-value* [**pbs** *pbs-value*] | **pir** *pir-value* [**cbs** *cbs-value* **pbs** *pbs-value*]]

     QoS CAR parameters are configured on the WLAN-BSS interface.
  4. Run:
     quit

     Return to the system view.

----End

Checking the Configuration

- Run the **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check the configuration of the rate limit for upstream and downstream traffic of all STAs in the VAP in the traffic profile.
- Run the **display user-profile** { **all** | **id** *profile-id* | **name** *profile-name* } command to check the user profile configuration.
- Run the **display qos car** { **all** | **name** *car-name* } command to check the configuration of the QoS CAR profile.

8.3.9 Configuring ACL-based Packet Filtering

By configuring ACL-based packet filtering, the device permits or rejects packets matching ACL rules to control network traffic.

Context

After ACL-based packet filtering is configured in a service set, the device filters packets of users that connect to VAPs bound to the service set based on the configured ACL rules.

Pre-configuration Tasks

Before configuring ACL-based Packet Filtering, complete the following task:

- **Configuring Basic WLAN Services**
- Configuring an ACL

Procedure

- Configure ACL-based packet filtering in a service set.
  1. Run:
     ```
     system-view
     ```
     The system view is displayed.
  2. Run:
     ```
     wlan
     ```
     The WLAN view is displayed.
  3. Run:
     ```
     service-set { name service-set-name | id service-set-id } *
     ```
     The service set view is displayed.
  4. Run:
     ```
     traffic-filter { inbound | outbound } acl { acl-number | name acl-name }
     ```
     ACL-based packet filtering is configured.

----End

Checking the Configuration

- After ACL-based packet filtering is configured in the service set, run the **display traffic-filter applied-record** command to check applications of ACL-based packet filtering.

8.3.10 Configuration Examples

This section provides WLAN QoS configuration examples, including networking requirements, configuration roadmap, and configuration procedure.

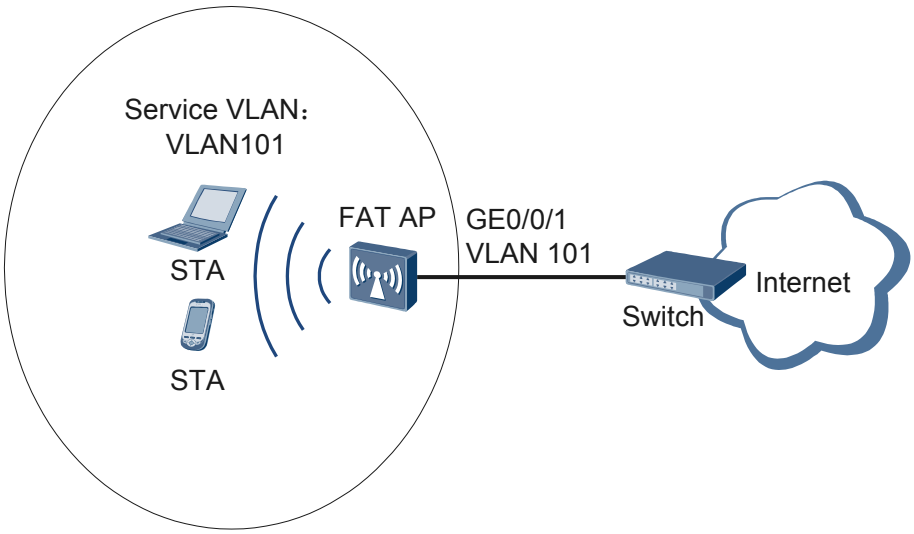
8.3.10.1 Example for Configuring WMM

Networking Requirements

As shown in **Figure 8-17**, a Fat AP accesses the Internet through wired connections and connects to STAs wirelessly. An enterprise branch needs to deploy basic WLAN services for mobile office so that branch users can access internal network resources anywhere at any time.

Voice, video, and data services are transmitted within the coverage of the AP. Users expect that video services preferentially preempt channels and have the highest priority to use wireless network resources.

Figure 8-17 Networking diagram for configuring WMM



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic WLAN services so that users can connect to the wireless network.
2. Configure parameters in the WMM profile used by the AP so that video services have higher priorities over voice and data services and preferentially use the bandwidth.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm** and set WMM parameters.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] wmm edca ap ac-vo ecw ecwmin 3 ecwmax 4 txoplimit 94
[AP-wlan-wmm-prof-wmm] wmm edca ap ac-vi ecw ecwmin 2 ecwmax 3 txoplimit 47
[AP-wlan-wmm-prof-wmm] wmm edca client ac-vo ecw ecwmin 3 ecwmax 4 txoplimit 94
[AP-wlan-wmm-prof-wmm] wmm edca client ac-vi ecw ecwmin 2 ecwmax 3 txoplimit 47
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security** and retain the default configurations. The authentication mode is open system authentication and the encryption mode is no encryption.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic** and retain the default configurations in the profile.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 6 Verify the configuration.

After the configuration is complete, run the **display vap service-set name test** command. The command output shows that the VAP has been created.

```
[AP] display vap service-set name test
  All VAP Information(Total-1):
  SS: Service-set     BP: Bridge-profile
  ------------------------------------------------------------------------
  Radio ID  SS ID  BP ID  WLAN ID  BSSID           Type
  0         1      -      1        DCD2-FC21-5D40  service
  ------------------------------------------------------------------------
  Total: 1
```

STAs discover the WLAN with SSID **test** and attempt to associate with the WLAN. You can run the **display station assoc-info interface wlan-radio0/0/0 service-set 1** command on the AP. The command output shows that the STAs associate with the WLAN **test**.

```
[AP] display station assoc-info interface wlan-radio0/0/0 service-set 1
  ------------------------------------------------------------------------------
  STA MAC          AP-ID   RADIO-ID  SS-ID   SSID
  ------------------------------------------------------------------------------
  14cf-9208-9abf   0       0         1        test
  ------------------------------------------------------------------------------
  Total stations: 1
```

Run the **display wmm-profile name wmm** command on the AP to view the WMM profile configuration. You can see that the priority of AC_VI packets is higher than that of AC_VO packets, so video services occupy channels.

```
[AP-wlan-view] display wmm-profile name wmm
  Profile ID      : 1
  Profile name    : wmm
  WMM switch      : enable
  Mandatory switch: disable
  Client EDCA parameters:
  ---------------------------------------------------
         ECWmax  ECWmin  AIFSN  TXOPLimit
  AC_VO  4       3       2      94
```

```
AC_VI  3       2       2      47
AC_BE  10      4       3      0
AC_BK  10      4       7      0
-------------------------------------------------
AP EDCA parameters:
-------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
AC_VO  4       3       1      94         normal
AC_VI  3       2       1      47         normal
AC_BE  6       4       3      0          normal
AC_BK  10      4       7      0          normal
-------------------------------------------------
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
  wmm edca ap ac-vi aifsn 1 ecw ecwmin 2 ecwmax 3 txoplimit
47
  wmm edca ap ac-vo aifsn 1 ecw ecwmin 3 ecwmax 4 txoplimit
94
  wmm edca client ac-vi aifsn 2 ecw ecwmin 2 ecwmax 3 txoplimit
47
  wmm edca client ac-vo aifsn 2 ecw ecwmin 3 ecwmax 4 txoplimit
94
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  wlan-bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

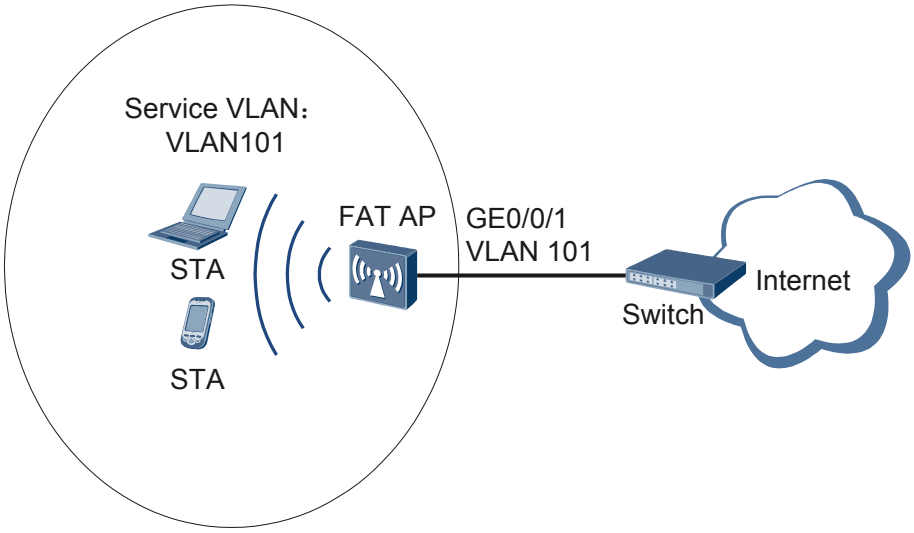
8.3.10.2 Example for Configuring Priority Mapping

Networking Requirements

As shown in **Figure 8-18**, a Fat AP accesses the Internet through wired connections and connects to STAs wirelessly. An enterprise branch needs to deploy basic WLAN services for mobile office so that branch users can access internal network resources anywhere at any time.

Voice, video, and data services are transmitted within the coverage of the AP. Users expect that video services are preferentially forwarded by the AP and have the highest priority to use wireless network resources.

Figure 8-18 Networking diagram for configuring priority mapping



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic WLAN services so that users can connect to the wireless network.
2. Configure priority mapping in the traffic profile so that video services have higher priorities over voice and data services and preferentially use the bandwidth.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm** and retain the default configurations in the profile.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security** and retain the default configurations. The authentication mode is open system authentication and the encryption mode is no encryption.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic** and configure priority mapping in the profile.

NOTE

By default, the priority of voice packets is set to 6 or 7 and the priority of video packets is set to 4 or 5.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] 8021p up-mapping 0 1 2 3 6 7 4 5
[AP-wlan-traffic-prof-traffic] 8021p-map-up 0 1 2 3 6 7 4 5
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 6 Verify the configuration.

After the configuration is complete, run the **display vap service-set name test** command. The command output shows that the VAP has been created.

```
[AP] display vap service-set name test
  All VAP Information(Total-1):
  SS: Service-set     BP: Bridge-profile
  ------------------------------------------------------------------------
  Radio ID  SS ID  BP ID  WLAN ID  BSSID           Type
  0         1      -      1        DCD2-FC21-5D40  service
  ------------------------------------------------------------------------
  Total: 1
```

STAs discover the WLAN with SSID **test** and attempt to associate with the WLAN. You can run the **display station assoc-info interface wlan-radio0/0/0 service-set 1** command on the AP. The command output shows that the STAs associate with the WLAN **test**.

```
[AP] display station assoc-info interface wlan-radio0/0/0 service-set 1
  ------------------------------------------------------------------------------
  STA MAC          AP-ID   RADIO-ID  SS-ID   SSID
  ------------------------------------------------------------------------------
  14cf-9208-9abf   0       0         1        test
  ------------------------------------------------------------------------------
  Total stations: 1
```

Run the **display traffic-profile name traffic** command on the AP to view the traffic profile configuration. You can find that the priority of video packets is higher than that of voice packets, so video services preempt channels.

```
[AP-wlan-view] display traffic-profile name traffic
  Profile ID         : 1
  Profile name       : traffic
  Client Limit Rate  : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  VAP Limit Rate     : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  802.1p Mapping Mode: mapping
  ----------------------------
  User-priority  802.1p
  0              0
  1              1
  2              2
  3              3
  4              6
  5              7
  6              4
  7              5
  ----------------------------
  ToS to User-priority Mapping List:
  ----------------------------
  ToS  User-priority
  0       0
  1       1
  2       2
  3       3
  4       6
  5       7
  6       4
```

```
7       5
----------------------------
Service-set bind the traffic-profile:
-------------------------------------------------
  1
-------------------------------------------------
Total: 1
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
  8021p-map-up 0 1 2 3 6 7 4
5
  8021p up-mapping 0 1 2 3 6 7 4
5
 security-profile name security id 1
 service-set name test id 1
  wlan-bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

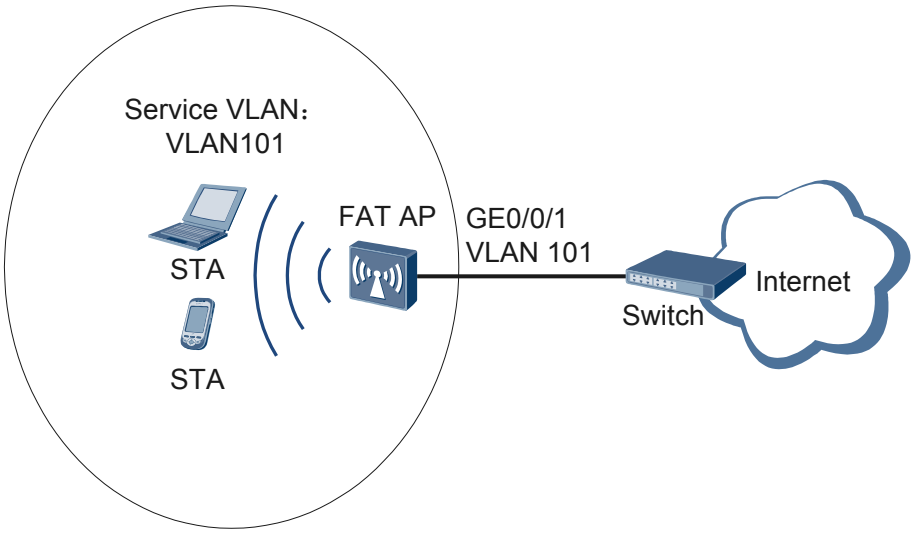
8.3.10.3 Example for Configuring Traffic Policing

Networking Requirements

As shown in **Figure 8-19**, a Fat AP accesses the Internet through wired connections and connects to STAs wirelessly. An enterprise branch needs to deploy basic WLAN services for mobile office so that branch users can access internal network resources anywhere at any time.

The enterprise network administrator needs to set the rate limit of upstream traffic on each STA associated with the AP to 2 Mbit/s and the limit of total rates of upstream traffic on all STAs associated with the VAP to 30 Mbit/s.

Figure 8-19 Networking diagram for configuring traffic policing



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic WLAN services so that users can connect to the wireless network.
2. Set the rate for upstream packets in the traffic profile used by the AP to implement traffic policing on upstream packets on a specified STA and on all STAs associated with the VAP.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
```

```
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm** and retain the default configurations in the profile.

```
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Create a security profile named **security** and retain the default configurations. The authentication mode is open system authentication and the encryption mode is no encryption.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic** and set traffic policing parameters in the profile.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] rate-limit client up 2048
[AP-wlan-traffic-prof-traffic] rate-limit vap up 30720
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 6 Verify the configuration.

After the configuration is complete, run the **display vap service-set name test** command. The command output shows that the VAP has been created.

```
[AP] display vap service-set name test
  All VAP Information(Total-1):
  SS: Service-set     BP: Bridge-profile
  ------------------------------------------------------------------------
  Radio ID  SS ID  BP ID  WLAN ID  BSSID           Type
  0         1      -      1        DCD2-FC21-5D40  service
  ------------------------------------------------------------------------
  Total: 1
```

STAs discover the WLAN with SSID **test** and attempt to associate with the WLAN. You can run the **display station assoc-info interface wlan-radio0/0/0 service-set 1** command on the AP. The command output shows that the STAs associate with the WLAN **test**.

```
[AP] display station assoc-info interface wlan-radio0/0/0 service-set 1
  ------------------------------------------------------------------------------
  STA MAC          AP-ID   RADIO-ID  SS-ID   SSID
  ------------------------------------------------------------------------------
  14cf-9208-9abf   0       0         1        test
  ------------------------------------------------------------------------------
  Total stations: 1
```

Run the **display traffic-profile name traffic** command on the AP to view the traffic profile configuration. You can see that the rate limit of upstream traffic on a specified STA is 2048 kbit/s (2 Mbit/s) and the total rate limits of upstream traffic on all STAs associated with the VAP is 30720 kbit/s (30 Mbit/s).

```
[AP-wlan-view] display traffic-profile name traffic
  Profile ID         : 1
  Profile name       : traffic
  Client Limit Rate  : 2048 Kbps(up)
                     : 4294967295 Kbps(down)
  VAP Limit Rate     : 30720 Kbps(up)
                     : 4294967295 Kbps(down)
  802.1p Mapping Mode: mapping
  ----------------------------
  User-priority  802.1p
  0              0
  1              1
  2              2
  3              3
  4              4
  5              5
  6              6
  7              7
  ----------------------------
  ToS to User-priority Mapping List:
  ----------------------------
  ToS  User-priority
  0       0
  1       1
  2       2
  3       3
  4       4
  5       5
  6       6
  7       7
  ----------------------------
  Service-set bind the traffic-profile:
  ------------------------------------------------
    1
  ------------------------------------------------
  Total: 1
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
  rate-limit client up
2048
  rate-limit vap up 30720
 security-profile name security id 1
 service-set name test id 1
  wlan-bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

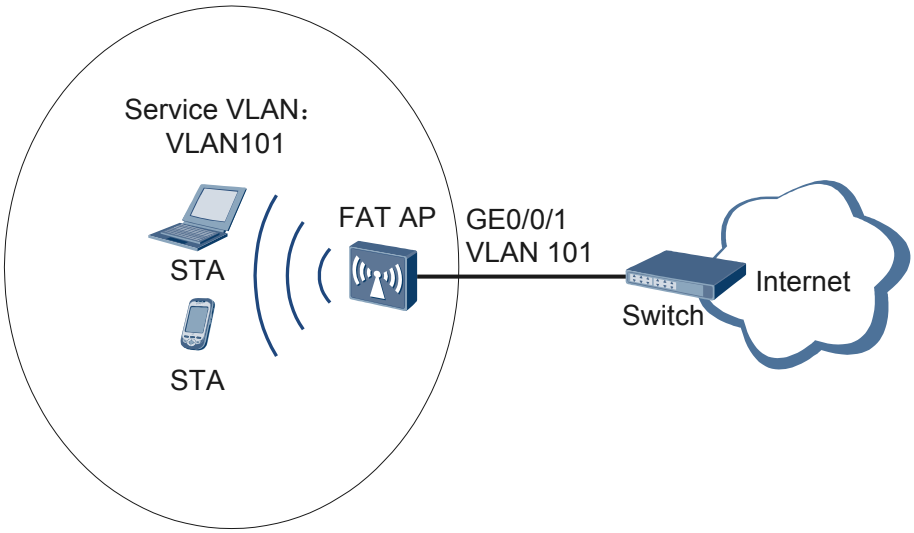
8.3.10.4 Example for Configuring ACL-based Packet Filtering

Networking Requirements

As shown in **Figure 8-20**, a Fat AP accesses the Internet through wired connections and connects to STAs wirelessly. An enterprise branch needs to deploy basic WLAN services for mobile office so that branch users can access internal network resources anywhere at any time.

The enterprise network administrator expects that an ACL can be configured to prohibit packets with the source IP address 192.168.11.10 and destination IP address 192.168.11.11.

Figure 8-20 Networking diagram for configuring ACL-based packet filtering



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure basic WLAN services so that users can connect to the wireless network.
2. Configure an ACL to filter packets.

Procedure

Step 1 Configure the AP to communicate with the upstream device.

NOTE

Configure AP uplink interfaces to transparently transmit packets of service VLANs as required and communicate with the upstream device.

Add AP uplink interface GE0/0/1 to VLAN 101.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
```

Step 2 Configure the AP as a DHCP server to allocate IP addresses to STAs.

Configure the AP as the DHCP server to allocate an IP address to STAs from the IP address pool on VLANIF 101.

```
[AP] dhcp enable
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.11.1 24
[AP-Vlanif101] dhcp select interface
[AP-Vlanif101] quit
```

Step 3 Configure AP system parameters.

Configure the country code.

```
[AP] wlan global country-code cn
 Warning: Modify the country code may delete all vap and stations will offline,
are you sure to continue?[Y/N]:y
```

Step 4 Configure WLAN service parameters.

Create a WMM profile named **wmm** and set WMM parameters.

```
[AP] wlan
[AP-wlan-view] wmm-profile name wmm id 1
[AP-wlan-wmm-prof-wmm] quit
```

Create a radio profile named **radio** and bind WMM profile **wmm** to the radio profile.

```
[AP-wlan-view] radio-profile name radio id 1
[AP-wlan-radio-prof-radio] wmm-profile name wmm
[AP-wlan-radio-prof-radio] quit
[AP-wlan-view] quit
```

Create WLAN-BSS interface 1.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 101
[AP-Wlan-Bss1] port hybrid untagged vlan 101
[AP-Wlan-Bss1] quit
```

Configure an advanced ACL.

```
[AP] acl 3001
[AP-acl-adv-3001] rule deny ip source 192.168.11.10 0 destination 192.168.11.11 0
[AP-acl-adv-3001] quit
```

Create a security profile named **security** and retain the default configurations. The authentication mode is open system authentication and the encryption mode is no encryption.

```
[AP] wlan
[AP-wlan-view] security-profile name security id 1
[AP-wlan-sec-prof-security] quit
```

Create a traffic profile named **traffic** and retain the default configurations in the profile.

```
[AP-wlan-view] traffic-profile name traffic id 1
[AP-wlan-traffic-prof-traffic] quit
```

Create a service set named **test** and bind the WLAN-BSS interface, security profile, and traffic profile to the service set.

```
[AP-wlan-view] service-set name test id 1
[AP-wlan-service-set-test] ssid test
[AP-wlan-service-set-test] wlan-bss 1
[AP-wlan-service-set-test] traffic-filter inbound acl 3001
[AP-wlan-service-set-test] security-profile name security
[AP-wlan-service-set-test] traffic-profile name traffic
[AP-wlan-service-set-test] quit
[AP-wlan-view] quit
```

Step 5 Configure a VAP.

```
[AP] interface wlan-radio 0/0/0
[AP-Wlan-Radio0/0/0] radio-profile name radio
 Warning: Modify the Radio type may cause some parameters of Radio resume defaul
t value, are you sure to continue?[Y/N]:y
[AP-Wlan-Radio0/0/0] service-set name test
[AP-Wlan-Radio0/0/0] quit
```

Step 6 Verify the configuration.

After the configuration is complete, run the **display vap service-set name test** command. The command output shows that the VAP has been created.

```
[AP] display vap service-set name test
  All VAP Information(Total-1):
  SS: Service-set     BP: Bridge-profile
  ------------------------------------------------------------------------
  Radio ID  SS ID  BP ID  WLAN ID  BSSID           Type
  0         1      -      1        DCD2-FC21-5D40  service
  ------------------------------------------------------------------------
  Total: 1
```

STAs discover the WLAN with SSID **test** and attempt to associate with the WLAN. You can run the **display station assoc-info interface wlan-radio0/0/0 service-set 1** command on the AP. The command output shows that the STAs associate with the WLAN **test**.

```
[AP] display station assoc-info interface wlan-radio0/0/0 service-set 1
  ------------------------------------------------------------------------------
  STA MAC          AP-ID   RADIO-ID  SS-ID   SSID
  ------------------------------------------------------------------------------
  14cf-9208-9abf   0       0         1        test
  ------------------------------------------------------------------------------
  Total stations: 1
```

Run the **display traffic-filter applied-record** command on the AP to check applications of ACL-based packet filtering, and you can find that the ACL has been applied to the service set.

```
[AP] display traffic-filter applied-record
-------------------------------------------------------------
Interface                   Direction  AppliedRecord
-------------------------------------------------------------
-------------------------------------------------------------
Service-set type:
-------------------------------------------------------------
Service-set                 Direction  AppliedRecord
-------------------------------------------------------------
test                        inbound    acl 3001
-------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
acl number 3001
 rule deny ip source 192.168.11.10 0 destination 192.168.11.11 0
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
```

```
 security-profile name security id 1
 service-set name test id 1
  wlan-bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
  traffic-filter inbound acl 3001
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

8.3.11 FAQ

8.3.11.1 What Is the Relationship Between WMM and 802.11e?

802.11e defines Quality of Service (QoS) for the wireless LAN, which provides the required service quality for voice and multimedia applications and enhances network performance. Wi-Fi Multimedia (WMM) defines four access categories, including voice, video, best effort, and background to optimize network communication quality and ensure stable access of corresponding applications to network resources. The WMM standard is a subset of IEEE 802.11e.

9 Configuration Guide - Device Management

About This Chapter

This document describes the principles and configurations of the Device Management features, and provides configuration examples of these features.

9.1 Displaying the Device Status

This chapter describes the functions of display commands and how to use the display commands to view the device running status.

9.1.1 Displaying Information About the device

You can use the display commands to view component information about the device.

Context

When a fault occurs on the device, you can view device information to check whether the device is working properly.

Procedure

- Run
  display device [**slot** *slot-id*]

  The component information and device status are displayed.

----End

9.1.2 Displaying the ESN

You can use the display commands to view the ESN.

Context

A device has a unique Equipment Serial Number (ESN).

Procedure

- Run:
  display esn

  The ESN of the device is displayed.

----End

9.1.3 Displaying Versions

You can use the display commands to view version information about the device.

Context

You can view version information about the device to determine whether the device needs to be upgraded or whether the upgrade succeeds.

Procedure

- Run:
  ```
  display version [ slot slot-id ]
  ```
  The version information of the device is displayed.

----End

9.1.4 Displaying the Temperature

You can use the display commands to view the temperature of the device.

Context

A high or low temperature may damage the hardware. To learn about the temperature of the device, use the display commands to view the temperature.

Procedure

- Run:
  ```
  display temperature { all | slot slot-id }
  ```
  The temperature of the device is displayed.

----End

9.1.5 Displaying CPU Usage

You can use the display commands to view CPU usage statistics and configurations.

Context

CPU usage is an important index to evaluate device performance. A high CPU usage will cause service faults You can use the display commands to view CPU usage statistics and configurations to check whether devices are working properly.

CPU usage configurations include the CPU usage alarm threshold and recovery threshold.

- When CPU usage reaches the alarm threshold, the system generates a CPU usage alarm.
- When CPU usage falls within the recovery threshold, the system generates a clear alarm.

Procedure

- Run:
  ```
  display cpu-usage
  ```
  The CPU usage statistics is displayed.
- Run:
  ```
  display cpu-usage configuration
  ```
  The CPU usage configurations are displayed.

----End

9.1.6 Displaying Memory Usage

You can use the display commands to view memory usage statistics and threshold.

Context

Memory usage is an important index to evaluate device performance. A high memory usage will cause service faults. You can use the display commands to view memory usage to check whether devices are working properly.

You can view the memory usage alarm threshold to learn about the conditions for triggering alarms.

- When memory usage reaches the alarm threshold, the system generates an alarm.
- When memory usage falls within the alarm threshold, the system generates a clear alarm.

Procedure

- Run:
  display memory-usage [**slot** *slot-id*]

  The memory usage statistics is displayed.
- Run:
  display memory-usage threshold

  The memory usage threshold is displayed.

----End

9.1.7 Displaying Interface Status

You can use the display commands to view the configuration and status of a specified interface.

Context

View the configuration of an interface.

- After performing operations in a interface view, you can view the configuration about this interface to check whether the configuration is correct.

View the status of an interface.

- You can view the status of an interface to monitor the interface or locate interface faults.

Procedure

- View the configuration of a specified interface.
  1. Run:
     system-view
     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*
     The interface view is displayed.

3. Run:
   display this
   The configuration of the current interface is displayed.

- View the status of an interface using either of the following methods.

  Method 1:

  1. Run:
     display interface [*interface-type* [*interface-number*]]
     The status of the specified interface is displayed.

  Method 2:

  1. Run:
     system-view
     The system view is displayed.
  2. Run:
     interface *interface-type interface-number*
     The interface view is displayed.
  3. Run:
     display this interface
     The status of the specified interface is displayed.

----End

9.1.8 Displaying Electronic Labels

You can use the display commands to view electronic labels.

Context

Electronic labels identify the hardware of devices.

Procedure

- Run:
  display elabel [*slot-id*] [**brief**]

  The electronic labels of the device is displayed.

----End

9.1.9 Displaying the Current Configuration

You can use the display commands to view the current configuration of the device.

Context

To learn about services currently running on the device, run the following command to view the device configuration.

Procedure

- Run:
  ```
  display current-configuration
  ```
  The information of the current configuration is displayed.

----End

9.1.10 Displaying Diagnostic Information

You can use the display commands to view diagnostic information for fault location.

Context

When a fault occurs in the system or during routine maintenance, you can run the display commands to collect the running information about all modules.

NOTICE

Viewing diagnostic information helps locate faults but may affect system performance. For example, CPU usage may become high. Therefore, do not view diagnostic information when the system is running properly.

Procedure

- Run:
  ```
  display diagnostic-information [ file-name ]
  ```
  The diagnostic information is displayed.

----End

9.1.11 Displaying Health Status

You can use the display commands to view the health status of the device.

Context

To learn about the device temperature, CPU usage, memory usage, and storage medium usage, use the fallowing command to view the health status.

Procedure

- Run:
  ```
  display health
  ```
  The health status of the device is displayed.

----End

9.2 Hardware Management

Scientific hardware management reduces the operations performed on hardware resources, including inserting, removing, installing and uninstalling the hardware, and improves hardware resource reliability.

9.2.1 Hardware Management Overview

Scientific hardware management allows you to use commands to operate and manage hardware resources, for example, back up electronic labels, and set the CPU and memory usage alarm thresholds.

Scientific hardware management reduces the operations performed on hardware resources, including inserting, removing, installing and uninstalling the hardware, and improves hardware resource reliability.

9.2.2 Backing Up Electronic Labels

You can back up electronic labels to improve network maintenance efficiency.

Context

Electronic labels can help locate network faults and replace hardware in batches. Therefore, backing up electronic labels is a must.

- When a network fault occurs, you can rapidly learn about hardware information using electronic labels, which improves hardware maintenance efficiency. In addition, you can efficiently analyze and trace the defects in the hardware by analyzing electronic labels statistics on the faulty hardware.
- Before replacing hardware in batches, you can use the electronic labels recorded in the archive systems of customers' devices to obtain accurate hardware deployment information. Then you can evaluate the impact of hardware replacement and define policies to efficiently replace hardware in batches.

Electronic labels can be backed up to the FTP server, TFTP server, or storage media. Before backing up electronic labels to the FTP or TFTP server, ensure that there are reachable routes between the device and FTP server (or TFTP server).

Procedure

- Run:
  backup elabel *filename* [*slot-id*]

  Electronic labels are backed up to the flash memory, USB flash drive, or SD card.
- Run:
  backup elabel ftp *ftp-server-address filename username password* [*slot-id*]

  Electronic labels are backed up to the FTP server.
- Run:
  backup elabel tftp *tftp-server-address filename* [*slot-id*]

Electronic labels are backed up to the TFTP server.

----End

9.2.3 Configuring the CPU Usage Alarm Threshold

You can configure the CPU usage alarm threshold to monitor CPU usage.

Context

When the system has a large number of routes, many CPU resources will be used. This degrades system performance and results in the delay in processing data or causes a high packet loss rate. During data processing, if the device can generate an alarm when high CPU usage occurs, you can effectively monitor CPU usage and optimize system performance to ensure system stability.

- CPU usage alarm threshold

  When CPU usage reaches this threshold, the system generates an alarm.
- CPU usage alarm recovery threshold

  When CPU usage falls within this threshold, the system generates a clear alarm.

Procedure

Step 1 (Optional) Run:

```
display cpu-usage configuration
```

The CPU usage configurations are displayed.

Step 2 Run:

```
system-view
```

The system view is displayed.

Step 3 Run:

```
set cpu-usage threshold threshold-value [ restore restore-threshold-value ]
```

The CPU usage alarm threshold and CPU usage alarm recovery threshold are set.

By default, the CPU usage alarm threshold is 95% and the CPU usage alarm recovery threshold is 75%.

If *restore-threshold-value* is not specified, the CPU usage alarm recovery threshold is calculated as follows:

- When the CPU usage alarm threshold is lower than 60%, the default CPU usage alarm recovery threshold is 1% lower than the CPU usage alarm threshold.
- When the CPU usage alarm threshold is higher than or equal to 60%, the default CPU usage alarm recovery threshold is 5% lower than the CPU usage alarm threshold.

----End

9.2.4 Configuring the Memory Usage Alarm Threshold

You can configure the memory usage alarm threshold to monitor memory usage.

Context

Memory usage is an important indicator to evaluate device performance. A high memory usage will cause service faults. During data processing, if the device can generate an alarm when high memory usage occurs, you can effectively monitor memory usage and optimize system performance to ensure system stability.

- Memory usage alarm threshold

  When memory usage reaches this threshold, the system generates an alarm.
- Memory usage alarm recovery threshold

  When memory usage falls within this threshold, the system generates a clear alarm.

Procedure

Step 1 (Optional) Run:

display memory-usage threshold

The memory usage configuration is displayed.

Step 2 Run:

system-view

The system view is displayed.

Step 3 Run:

set memory-usage threshold *threshold-value*

The memory usage alarm threshold is set.

By default,

- If the device memory is smaller than 128 MB, the memory usage alarm threshold is 83%.
- If the device memory is larger than or equal to 128 MB, the memory usage alarm threshold is 90%.

----End

9.3 Information Center Configuration

The information center works as the information hub. It records system running information in real time, which helps the network administrator and developers to monitor network operation and analyze network faults.

9.3.1 Information Center Overview

This section describes definition of Information Center and purpose of this feature.

Definition

The information center works as the information hub. Logs, traps, and debugging messages generated by the device are sent to the information center for unified management and flexible output.

Purpose

When an exception or a fault occurs on the device, users need to immediately and accurately collect information generated during device running. The information center records information generated by each module during device running, including logs, traps, and debugging messages. You can configure the information center to classify and filter information based on information types and severities so that information can be flexibly output to different destinations such as the console, user terminal, and log host. By doing this, users or network administrators can collect device information from different destinations so that they can easily monitor the device running status and locate faults.

9.3.2 Principles

This section describes implementation of information center feature.

The information center receives information generated by the device and controls information output based on defined severity.

9.3.2.1 Information Classification

The device generates three types of messages: logs, traps, and debugging messages. **Table 9-1** lists information classification.

Table 9-1 Information classification

Information Type	Description
Log	Logs record user operations, system faults, and system security. Logs include user logs, and diagnostic logs. ● User logs: record user operations and system operating information. ● Diagnostic logs: record information used for fault location.
Trap	Traps are notifications generated when the device detects faults. Traps record system status information. Different from logs, traps need to be notified to administrators in a timely manner.
Debugging message	Debugging messages show internal operating information of the system and help you trace the device running status. Debugging messages are generated only after the debugging of a module is enabled.

9.3.2.2 Information Hierarchy

If too much information is generated, it is difficult to differentiate information about normal operation and information about faults. Through information hierarchy, users do not need to handle unwanted information.

Information has eight severities. The lower the severity level, the more severe the information. **Table 9-2** lists severities.

Table 9-2 Description of information severities

Value	Severity	Description
0	Emergencies	A fault causes the device to fail to run normally unless it is restarted. For example, the device restarts because of a program exception or a fault about memory usage.
1	Alert	A fault needs to be rectified immediately. For example, memory usage of the system reaches the upper limit.
2	Critical	A fault needs to be analyzed and processed. For example, the memory usage falls below the lower threshold; BFD detects that a device is unreachable.
3	Error	An improper operation is performed or exceptions occur during service processing. The fault does not affect services but needs to be analyzed. For example, users enter incorrect commands or passwords; error protocol packets are received.
4	Warning	Some events or operations may affect device running or cause service processing faults, which requires full attention. For example, a routing process is disabled; BFD detects packet loss; error protocol packets are detected.
5	Notification	A key operation is performed to keep the device running normally. For example, the **shutdown** command is run; a neighbor is discovered; protocol status changes.
6	Informational	A normal operation is performed. For example, a display command is run.
7	Debugging	A normal operation is performed, which requires no attention.

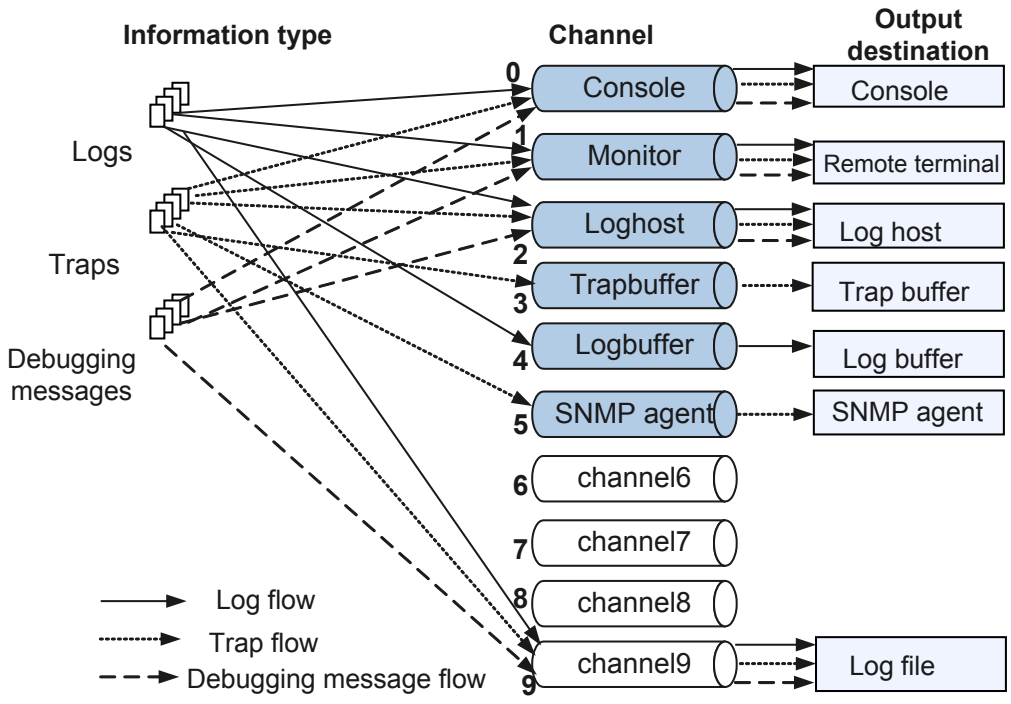
When information filtering based on severity levels is enabled, only the information whose severity level threshold is less than or equal to the configured value is output.For example, if the severity level value is configured to 6, only information with a severity level ranging from 0 to 6 is output.

9.3.2.3 Information Output

Information generated by the device can be output to the remote terminal, console, log buffer, log file, and SNMP agent. To output information in different directions, 10 information channels are defined for the information center. These channels work independently from one another.

You can configure output rules so that information can be output from different objects to different objects based on types and severities, as shown in **Figure 9-1**.

Figure 9-1 Information center



By default, logs, traps, and debugging messages are output from default channels. You can change channel names or relationships between channels and output directions as required. For example, the name of channel 6 is user1 and channel 6 is used to send information to the log host. The information sent to the log host is output from channel 6 but not channel 2.

Table 9-3 lists relationships between default channels and output directions.

Table 9-3 Relationship between default channels and output directions

Channel Number	Default Channel Name	Output Direction	Description
0	Console	Console	Outputs logs, traps, and debugging messages to the local console.
1	Monitor	Remote terminal	Outputs logs, traps, and debugging messages to the VTY terminal for remote maintenance.
2	loghost	Log host	Outputs logs, traps, and debugging messages. The information is saved to the log host in file format for easy reference.
3	trapbuffer	Trap buffer	Outputs traps.

Channel Number	Default Channel Name	Output Direction	Description
4	logbuffer	Log buffer	Outputs logs.
5	snmpagent	SNMP agent	Outputs traps.
6	channel6	Unspecified	Reserved. You can specify an output destination for this channel.
7	channel7	Unspecified	Reserved. You can specify an output destination for this channel.
8	channel8	Unspecified	Reserved. You can specify an output destination for this channel.
9	channel9	Logfile	Outputs logs, traps, and debugging messages.

9.3.2.4 Information Filtering

To control information output flexibly, the information center provides the information filtering function. After the device works properly, each module reports information during service processing. To filter unwanted information about a service module or of certain severity, configure the filtering function.

The information center filters information in a channel through the information filtering table. The information filtering table is used to filter information output to different directions based on information types, severities, and sources.

The content of the information filtering table is as follows:

- Number of the module that generates information
- Log output status
- Log output severity
- Trap output status
- Trap output severity
- Debugging message output status
- Debugging message severity

9.3.2.5 Information Output Format

- **Output format of logs**

  Figure 9-2 shows the format of logs.

  Figure 9-2 Output format of logs

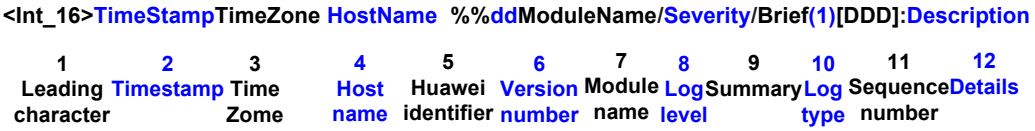
  

Table 9-4 describes each field in a log.

Table 9-4 Description of each field in a log

Field	Description	Remarks
<Int_16>	Leading character.	This character is added to the information to be sent to the syslog server, not the information saved on a local device.
TimeStamp	Time to send logs.	Five timestamp formats are available: ● boot: indicates that the timestamp is expressed in the format of relative time, a period of time since system start. The format is xxxxxx.yyyyyy. xxxxxx is the higher order 32 bits of the milliseconds elapsed since the start of the system; yyyyyy is the lower order 32 bits of the milliseconds elapsed since the start of the system. ● date: indicates the current date and time. It is expressed in mm dd yyyy hh:mm:ss format. ● short-date: indicates the short date. This timestamp differs from **date** is that the year is not displayed. ● format-date: indicates that the timestamp is expressed in YYYY-MM-DD hh:mm:ss format. ● none: indicates that no timestamp is contained in information. Logs use the date format.
TimeZone	Local zone.	Indicates local time zone information. This information is consistent with the Time Zone field of the **display clock** command output.
HostName	Host name.	-
%%	Huawei identifier.	The log is output by Huawei products.
dd	Version number.	Version number of the log.
ModuleName	Module name.	Name of the module that outputs information to the information center.
Serverity	Log severity.	Log severity.
Brief	Brief description.	Brief description about logs.
(l)	Information type.	The information types are as follows: ● l: log. ● D: debugging log.

Field	Description	Remarks
DDD	Log sequence number.	By default, the information center can output logs to the console, log buffer, SNMP agent, and log file. In the logbuffer, the value depends on the log buffer size. For example, the log buffer can store a maximum of 100 logs. The log sequence number ranges from 0 to 99.
Description	Description.	Log content.

- **Trap output format**

  Figure 9-3 shows the trap output format.

  Figure 9-3 Trap output format

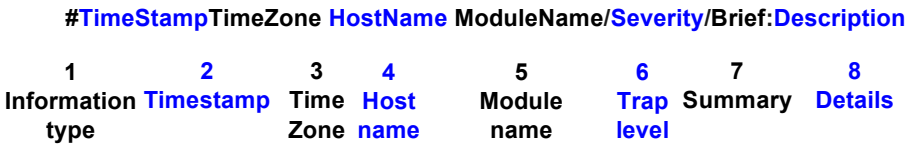
  

  Table 9-5 describes each field in a trap.

  Table 9-5 Description of each field in a trap

Field	Description	Remarks
#	Information type.	The number sign (#) indicates a trap and only appears in the trapbuffer.

Field	Description	Remarks
TimeStamp	Timestamp, that is, time to output log information.	Five timestamp formats are available: ● boot: indicates that the timestamp is expressed in the format of relative time, a period of time since system start. The format is xxxxxx.yyyyyy. xxxxxx is the higher order 32 bits of the milliseconds elapsed since the start of the system; yyyyyy is the lower order 32 bits of the milliseconds elapsed since the start of the system. ● date: indicates the current date and time. It is expressed in mm dd hh:mm:ss yyyy format. ● short-date: indicates the short date. This timestamp differs from **date** is that the year is not displayed. ● format-date: indicates that the timestamp is expressed in YYYY-MM-DD hh:mm:ss format. ● none: indicates that no timestamp is contained in information. Traps use the date format.
TimeZone	Local zone.	Indicates local time zone information. This information is consistent with the Time Zone field of the **display clock** command output.
HostName	Host name.	The host name and module name are separated by a space.
ModuleName	Module name.	Name of the module that outputs information to the information center.
Severity	Severity.	Trap severity.
Brief	Brief description.	Brief description about traps.
Description	Description.	Trap content.

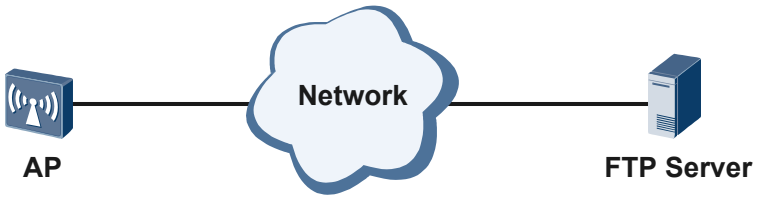
9.3.3 Applications

This section describes applications of the information center feature.

Outputting Logs to a Log File

As shown in **Figure 9-4**, the information center is configured on the device, and the device is connected to an FTP server. The information center stores the logs of the specified severity in a log file, and the log file needs to be transferred to the FTP server. The logs help an administrator learn the device running status or troubleshoot the device.

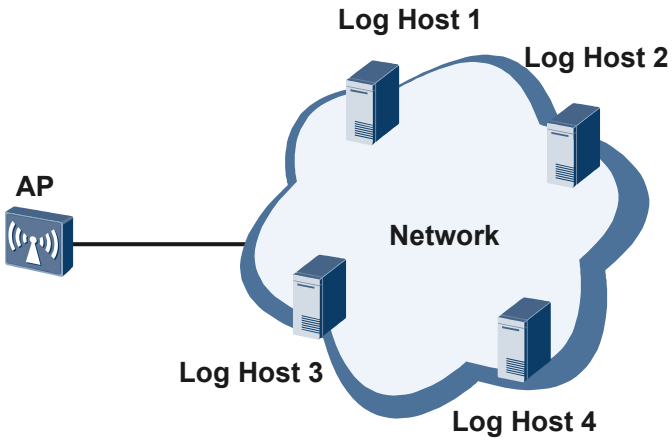
Figure 9-4 Outputting logs to a log file



Outputting Logs to a Log Host

As shown in **Figure 9-5**, the information center is configured on the device, and the device is connected to multiple log hosts. The information center sends logs of different severities to different log hosts. The logs help an administrator learn the device running status.

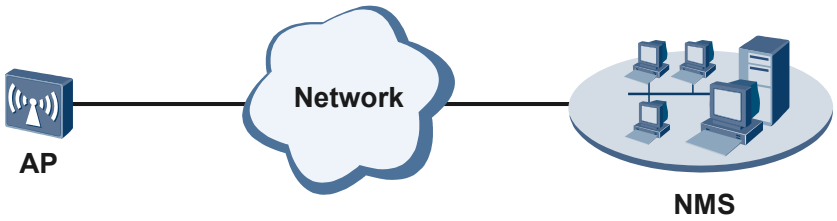
Figure 9-5 Outputting logs to a log host



Outputting Traps to the NMS

As shown in **Figure 9-6**, the information center is configured on the device, and the device is connected to a network management system (NMS). The information center sends traps to the NMS, and the NMS monitors the device running status based on the traps.

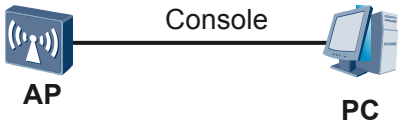
Figure 9-6 Outputting traps to the NMS



Outputting Debugging Messages to the Console

As shown in **Figure 9-7**, the information center is configured on the device. The information center sends debugging messages to the console, and the maintenance personnel debugs the device based on the debugging messages.

Figure 9-7 Outputting debugging messages to the console



9.3.4 Default Configuration

This section describes default parameter settings of the information center.

Table 9-6 Default parameter settings of the information center

Parameter	Default Setting
Information center	Enabled
Maximum number of logs in the log buffer	512
Maximum number of traps in the trap buffer	256
Log file size	1 MB
Maximum number of log files that can be saved	200
Log host IP address	None
Timestamp format	date

Default Output Rules of Information Channels

Default output rules define information modules to which different types of information can be output, lowest information severity, and information channels. See **Table 9-7**.

Table 9-7 Default output rules

Output Channel	Module Enabled to Output Information	Log		Trap		Debugging Message	
		Status	Lowest Output Severity	Status	Lowest Output Severity	Status	Lowest Output Severity
0 (console)	default (all modules)	Enabled	warning	Enabled	debugging	Enabled	debugging
1 (remote terminal)	default (all modules)	Enabled	warning	Enabled	debugging	Enabled	debugging
2 (log host)	default (all modules)	Enabled	informational	Enabled	debugging	Disabled	debugging
3 (trap buffer)	default (all modules)	Disabled	informational	Enabled	debugging	Disabled	debugging
4 (log buffer)	default (all modules)	Enabled	warning	Disabled	debugging	Disabled	debugging
5 (SNMP agent)	default (all modules)	Disabled	debugging	Enabled	debugging	Disabled	debugging
6 (channel 6)	default (all modules)	Enabled	debugging	Enabled	debugging	Disabled	debugging
7 (channel 7)	default (all modules)	Enabled	debugging	Enabled	debugging	Disabled	debugging
8 (channel 8)	default (all modules)	Enabled	debugging	Enabled	debugging	Disabled	debugging

Output Channel	Module Enabled to Output Information	Log		Trap		Debugging Message	
		Status	Lowest Output Severity	Status	Lowest Output Severity	Status	Lowest Output Severity
9 (channel 9)	default (all modules)	Enabled	debugging	Enabled	debugging	Disabled	debugging

9.3.5 Configuring Information Center

This section describes how to configure the information center.

9.3.5.1 Configuring Log Output

Logs of a specific module can be output to the log buffer, log file, console, terminal, or log host.

Pre-configuration Tasks

Before enabling log output, complete the following task:

Starting the AP

Configuration Process

Table 9-8 lists the configuration process for enabling log output.

Table 9-8 Configuration process for enabling log output

No.	Configuration Task	Description	Remarks
1	**9.3.5.1.1 Enabling the Information Center**	You can configure the information center only after the information center is enabled. By default, the information center is enabled.	Steps 2 to 4 are optional and can be performed in any sequence.
2	**9.3.5.1.2 (Optional) Naming an Information Channel**	You can easy-to-remember names for channels to facilitate information center usage.	

No.	Configuration Task	Description	Remarks
3	9.3.5.1.3 (Optional) Configuring Log Filtering	If some logs are unnecessary, configure the AP not to output these logs.	
4	9.3.5.1.4 (Optional) Setting the Timestamp Format of Logs	To adjust the time format and time precision for information output, configure the timestamp.	
5	9.3.5.1.6 Configuring the Device to Output Logs to the Log Buffer	To view logs in the log buffer, configure the AP to output logs to the log buffer.	Steps 5 to 9 can be configured in any sequence. You can view logs in the log buffer, log file, console, terminal, or log host.
6	9.3.5.1.7 Configuring the Device to Output Logs to a Log File	After logs are output to a log file, you can download the log file anytime to monitor device running based on the logs.	
7	9.3.5.1.8 Configuring the Device to Output Logs to the Console	After logs are output to the console, you can view logs on the console (host from which you can log in to the AP through the console interface) to monitor device running.	
8	9.3.5.1.9 Configuring the Device to Output Logs to a Terminal	After logs are output to a user terminal, you can view logs on the user terminal (host from which you log in to the AP through STelnet) to monitor device running.	
9	9.3.5.1.10 Configuring the Device to Output Logs to a Log Host	After configuring the AP to output logs to a log host, you can view logs saved on the log host to monitor device running.	

9.3.5.1.1 Enabling the Information Center

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center enable
```

The information center is enabled.

By default, the information center is enabled.

----End

9.3.5.1.2 (Optional) Naming an Information Channel

Context

You can rename channels, which facilitates memorization and usage.

NOTE

Channel names must be unique. It is recommended that channel names represent channel functions.

The following lists default channel names.

Table 9-9 Default channel names

Channel Number	Default Channel Name
0	console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer
5	snmpagent
6	channel6
7	channel7
8	channel8
9	channel9

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center channel channel-number name channel-name
```

A name is configured for the information channel with the specified number.

----End

9.3.5.1.3 (Optional) Configuring Log Filtering

Context

If some logs are unnecessary, configure the device not to output these logs. When the filtering function is enabled, the information center does not send the specified logs that satisfy the filtering condition to any channel. As a result, all output directions cannot receive the specified logs.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center filter-id { id | bymodule-alias modname alias } * &<1-50>
```

or

The filtering function is configured for specified logs.

NOTE

- Currently, the device can filter logs or modules with a maximum of 50 log IDs or modules. If there are more than 50 log IDs or modules, the system displays a message indicating that the filtering table is full. To configure the filtering function, run the **undo info-center filter-id** { **all** | { *id* | **bymodule-alias** *modname alias* } * &<1-50> } command to delete original IDs or modules, and reconfigure the log ID or module.
- To add multiple IDs or modules at a time, use a space to separate IDs or modules. The system displays a message to report the result of adding each ID or module.
- You cannot add the same ID or module repeatedly.
- When you add an unregistered or nonexistent log ID or alias name, the system displays a message indicating that the system fails to filter the log with the specified log ID or alias name.

----End

9.3.5.1.4 (Optional) Setting the Timestamp Format of Logs

Context

To adjust the time format and time precision for information output, configure the timestamp.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center timestamp log { { date | short-date | format-date } [ precision-time
{ tenth-second | millisecond } ] | boot | none }
```

The timestamp format of logs is configured.

By default, the timestamp format of logs is **date**.

----End

9.3.5.1.5 (Optional) Disabling the Log Counter Function

Context

Logs generated on the AP contain sequence numbers. That is, the log counter function is enabled by default. For example, you can run the **display logbuffer** command to view the sequence numbers of logs.

```
<Huawei> display logbuffer
Logging buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 512
Channel number: 4, Channel name: logbuffer
Dropped messages: 0
Overwritten messages: 167
Current messages: 512

May 10 2012 13:42:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[0]:Some packets are
dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=912)
May 10 2012 13:32:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[1]:Some packets are
dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 13:22:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[2]:Some packets are
dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 13:12:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[3]:Some packets are
dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=912)
May 10 2012 13:02:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[4]:Some packets are
dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
...
```

If the AP has been running for a long time, many logs may be generated.

- To enable the AP not to encapsulate sequence numbers in logs sent to the log buffer, log file, console, or terminal, disable the log counter function.
- To re-collect statistics on logs sent to the log buffer, log file, console, or terminal, disable the log counter function, disable the log counter function, and then enable the log counter function.
- To view logs sent to the log buffer, log file, console, or terminal, disable the log counter function, enable the log counter function so that logs contain sequence numbers in ascending order.

NOTE

- If logs are sent to the console, log file, or terminal, logs are counted independently and sequence numbers in the logs are in ascending order. That is, the sequence number of the log that was generated first is 0 and the log that is generated later has a larger sequence number.
- If logs are sent to the log buffer, sequence numbers in logs are in descending order. That is, the sequence number in the log that is generated recently is 0 and the log that was generated earlier has a larger sequence number.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center local log-counter disable
```

The log counter function is disabled.

By default, the log counter function is enabled.

----End

9.3.5.1.6 Configuring the Device to Output Logs to the Log Buffer

Context

To view logs in the log buffer, configure the device to output logs to the log buffer.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center logbuffer
```

The device is enabled to output information to the log buffer.

By default, the device is enabled to output logs to the log buffer.

Step 3 Run:

```
info-center logbuffer channel { channel-number | channel-name }
```

The channel used by the device to output logs to the log buffer is specified.

By default, the device uses channel 4 to output logs to the log buffer.

Step 4 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } log { state { off | on } | level severity } *
```

A rule for outputting logs to a channel is set.

By default, channel 4 is enabled to output logs and the lowest log severity is **warning**.

Step 5 (Optional) Run:

```
info-center logbuffer size logbuffer-size
```

The maximum number of logs in the log buffer is set.

By default, a log buffer can store a maximum of 512 logs.

----End

9.3.5.1.7 Configuring the Device to Output Logs to a Log File

Context

After logs are output to a log file, you can view the log file anytime to monitor device running based on the logs.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center logfile channel { channel-number | channel-name }
```

A channel through which logs are output to a log file is specified.

By default, the device uses channel 9 to output logs to a log file.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } log { state { off | on } | level severity } *
```

A rule for outputting logs to a channel is set.

By default, channel 9 is enabled to output logs and the lowest log severity is **debugging**.

Step 4 (Optional) Run:

```
info-center logfile path path
```

The path where log files are saved is specified.

Step 5 (Optional) Run:

```
info-center logfile size size
```

The log file size is set.

By default, the log file size is 1 MB.

NOTE

- If the size of a log file generated on the device exceeds the configured log file size, the system decompresses the log file into a zip file.
- You can run the **save logfile** command to save information to a log file.

Step 6 (Optional) Run:

```
info-center max-logfile-number filenumbers
```

The maximum number of log files that can be saved is set.

By default, a maximum of 200 log files can be saved.

If the number of log files generated on the AP exceeds the limit, the system deletes the oldest log file.

----End

9.3.5.1.8 Configuring the Device to Output Logs to the Console

Context

After logs are output to the console, you can view logs on the console (host from which you can log in to the device through the console interface) to monitor device running.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center console channel { channel-number | channel-name }
```

A channel through which logs are output to the console is specified.

By default, the device uses channel 0 to output logs to the console.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } log { state { off | on } | level severity } *
```

A rule for outputting logs to a channel is set.

By default, channel 0 is enabled to output logs and the lowest log severity is **warning**.

Step 4 Run:

```
quit
```

Return to the user view.

Step 5 Run:

```
terminal monitor
```

Display of logs, traps, and debugging message output is enabled on the user terminal.

By default, terminal display is disabled.

Step 6 Run:

```
terminal logging
```

Log display is enabled on the user terminal.

By default, log display is enabled on the user terminal.

----End

9.3.5.1.9 Configuring the Device to Output Logs to a Terminal

Context

After logs are output to a user terminal, you can view logs on the user terminal (host from which you log in to the device through Telnet) to monitor device running.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center monitor channel { channel-number | channel-name }
```

A channel through which logs are output to a user terminal is specified.

By default, the AP uses channel 1 to output logs to a user terminal.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } log { state { off | on } | level severity } *
```

A rule for outputting logs to a channel is set.

By default, channel 1 is enabled to output logs and the lowest log severity is **warning**.

Step 4 Run:

```
quit
```

Return to the user view.

Step 5 Run:

```
terminal monitor
```

Display of logs, traps, and debugging message output is enabled on the user terminal.

By default, terminal display is disabled.

Step 6 Run:

```
terminal logging
```

Log display is enabled on the user terminal.

By default, log display is enabled on the user terminal.

----End

9.3.5.1.10 Configuring the Device to Output Logs to a Log Host

Context

After configuring the device to output logs to a log host, you can view logs saved on the log host to monitor device running.

Pre-configuration Tasks

There is a reachable route between the device and the log host.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Run:

info-center loghost *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | { **language** *language-name* | **binary** [*port*] }] *

The device is configured to output logs to the log host.

Step 3 Run:

info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } **log** { **state** { **off** | **on** } | **level** *severity* } *

A rule for outputting logs to a channel is set.

By default, channel 2 is enabled to output logs and the lowest log severity is **informational**.

Step 4 (Optional) Run:

info-center loghost source *interface-type interface-number*

The source interface used by the device to send logs to a log host is specified.

By default, the source interface is the interface that sends logs.

After the source interface is specified, the log host determines the device that sends messages. The log host then can easily retrieve received messages.

----End

9.3.5.1.11 Checking the Configuration

Procedure

- Run the **display channel** [*channel-number* | *channel-name*] command to view the channel configuration.
- Run the **display info-center filter-id** [*id* | **bymodule-alias** *modname alias*] command to view information filtered by the information center.
- Run the **display info-center logfile path** command to check the path where log files are saved.
- Run the **display logbuffer** command to check logs recorded in the log buffer.
- Run the **display logfile** *file-name* [*offset* | **hex**] * command to check the log file.

----End

9.3.5.2 Configuring Trap Output

Traps of a specific module can be output to the trap buffer, log file, console, terminal, log host, or SNMP agent.

Pre-configuration Tasks

Before enabling trap output, complete the following task:

Starting the AP

Configuration Process

Table 9-10 lists the configuration process for enabling trap output.

Table 9-10 Configuration process for enabling trap output

No.	Name	Description	Remarks
1	**9.3.5.2.1 Enabling the Information Center**	You can configure the information center only after the information center is enabled. By default, the information center is enabled.	Steps 2 to 4 are optional and can be performed in any sequence.
2	**9.3.5.2.2 (Optional) Naming an Information Channel**	You can rename channels, which facilitates memorization and usage.	
3	**9.3.5.2.3 (Optional) Configuring Trap Filtering**	If some traps are unnecessary, configure the AP not to output these traps.	
4	**9.3.5.2.4 (Optional) Setting the Timestamp Format of Traps**	To adjust the time format and time precision for information output, configure the timestamp.	
5	**9.3.5.2.5 Configuring the Device to Output Traps to the Trap Buffer**	To view traps in the trap buffer, configure the AP to output traps to the trap buffer.	Steps 5 to 10 can be configured in any sequence. You can configure the device to output traps to one or more destinations according to your needs.
6	**9.3.5.2.6 Configuring the Device to Output Traps to a Log File**	After traps are output to a log file, you can download the log file anytime to view traps generated by the AP to monitor device running.	
7	**9.3.5.2.7 Configuring the Device to Output Traps to the Console**	After traps are output to the console, you can view traps on the console (host from which you can log in to the AP through the console interface) to monitor device running.	

No.	Name	Description	Remarks
8	9.3.5.2.8 Configuring the Device to Output Traps to a Terminal	After traps are output to a user terminal, you can view traps on the user terminal (host from which you log in to the AP through STelnet) to monitor device running.	
9	9.3.5.2.9 Configuring the Device to Output Traps to a Log Host	After configuring the AP to output traps to a log host, you can view traps saved on the log host to monitor device running.	
10	9.3.5.2.10 Configuring the Device to Output Traps to an SNMP Agent	When an exception or a fault occurs on the AP, the network administrator wants to learn device running. You can configure the AP to output traps to an NMS server so that the network administrator can monitor the AP in real time and locate faults immediately. Before configuring the AP to output traps to an NMS server, configure the AP to output traps to an SNMP agent. Then the SNMP agent sends traps to the NMS server.	

9.3.5.2.1 Enabling the Information Center

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center enable
```

The information center is enabled.

By default, the information center is enabled.

----End

9.3.5.2.2 (Optional) Naming an Information Channel

Context

You can rename channels, which facilitates memorization and usage.

NOTE

Channel names must be unique. It is recommended that channel names represent channel functions.

The following lists default channel names.

Table 9-11 Default channel names

Channel Number	Default Channel Name
0	console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer
5	snmpagent
6	channel6
7	channel7
8	channel8
9	channel9

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center channel channel-number name channel-name
```

A name is configured for the information channel with the specified number.

----End

9.3.5.2.3 (Optional) Configuring Trap Filtering

Context

If some traps are unnecessary, configure the device not to output these traps. When the filtering function is enabled, the information center does not send the specified traps that satisfy the

filtering condition to any channel. As a result, all output directions cannot receive the specified traps.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center filter-id { id | bymodule-alias modname alias } * &<1-50>
```

The filtering function is configured for specified traps.

NOTE

- Currently, the device can filter logs or modules with a maximum of 50 log IDs or modules. If there are more than 50 log IDs or modules, the system displays a message indicating that the filtering table is full. To configure the filtering function, run the **undo info-center filter-id** { **all** | { *id* | **bymodule-alias** *modname alias* } * &<1-50> } command to delete original IDs or modules, and reconfigure the log ID or module.
- To add multiple IDs or modules at a time, use a space to separate IDs or modules. The system displays a message to report the result of adding each ID or module.
- You cannot add the same ID or module repeatedly.
- When you add an unregistered or nonexistent ID or alias name, the system displays a message indicating that the system fails to filter the trap with the specified ID or alias name.

----End

9.3.5.2.4 (Optional) Setting the Timestamp Format of Traps

Context

To adjust the time format and time precision for information output, configure the timestamp.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center timestamp trap { { date | short-date | format-date } [ precision-time { tenth-second | millisecond } ] | boot | none }
```

The timestamp format of traps is set.

By default, the timestamp format of traps is **date**.

----End

9.3.5.2.5 Configuring the Device to Output Traps to the Trap Buffer

Context

To view traps in the trap buffer, configure the device to output traps to the trap buffer.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center trapbuffer
```

The device is enabled to output traps to the trap buffer.

By default, the device is enabled to output traps to the trap buffer.

Step 3 Run:

```
info-center trapbuffer channel { channel-number | channel-name }
```

The channel used by the device to output traps to the trap buffer is specified.

By default, the device uses channel 3 to output traps to the trap buffer.

Step 4 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } trap { state { off | on } | level severity } *
```

A rule for outputting traps to a channel is set.

By default, channel 3 is enabled to output traps and the lowest severity is **debugging**.

Step 5 (Optional) Run:

```
info-center trapbuffer size trapbuffer-size
```

The maximum number of traps in the trap buffer is set.

By default, the trap buffer can store a maximum of 256 traps.

----End

9.3.5.2.6 Configuring the Device to Output Traps to a Log File

Context

After traps are output to a log file, you can view the log file anytime to monitor device running based on the traps.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center logfile channel { channel-number | channel-name }
```

A channel through which traps are output to a log file is specified.

By default, the device uses channel 9 to output traps to a log file.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } trap { state { off | on } | level severity } *
```

A rule for outputting traps to a channel is set.

By default, channel 9 is enabled to output traps and the lowest severity is **debugging**.

Step 4 (Optional) Run:

```
info-center logfile path path
```

The path where log files are saved is specified.

Step 5 (Optional) Run:

```
info-center logfile size size
```

The log file size is set.

By default, the log file size is 1 MB.

NOTE

- If the size of a log file generated on the device exceeds the configured log file size, the system decompresses the log file into a zip file.
- You can run the **save logfile** command to manually save traps in the log file buffer to a log file.

Step 6 (Optional) Run:

```
info-center max-logfile-number filenumbers
```

The maximum number of log files that can be saved is set.

By default, a maximum of 200 log files can be saved.

If the number of log files generated on the AP exceeds the limit, the system deletes the oldest log file.

----End

9.3.5.2.7 Configuring the Device to Output Traps to the Console

Context

After traps are output to the console, you can view traps on the console (host from which you can log in to the device through the console interface) to monitor device running.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center console channel { channel-number | channel-name }
```

A channel through which traps are output to the console is specified.

By default, the device uses channel 0 to output traps to the console.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } trap { state { off | on } | level severity } *
```

A rule for outputting traps to a channel is set.

By default, channel 0 is enabled to output traps and the lowest severity is **debugging**.

Step 4 Run:

```
quit
```

Return to the user view.

Step 5 Run:

```
terminal monitor
```

Display of logs, traps, and debugging message output is enabled on the user terminal.

By default, terminal display is disabled.

Step 6 Run:

```
terminal trapping
```

Traps display is enabled on the user terminal.

By default, traps display is enabled on the user terminal.

----End

9.3.5.2.8 Configuring the Device to Output Traps to a Terminal

Context

After traps are output to a user terminal, you can view traps on the user terminal (host from which you log in to the device through Telnet) to monitor device running.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center monitor channel { channel-number | channel-name }
```

A channel through which traps are output to a user terminal is specified.

By default, the device uses channel 1 to output traps to a user terminal.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-
name } trap { state { off | on } | level severity } *
```

A rule for outputting traps to a channel is set.

By default, channel 1 is enabled to output traps and the lowest severity is **debugging**.

Step 4 Run:

```
quit
```

Return to the user view.

Step 5 Run:

```
terminal monitor
```

Display of logs, traps, and debugging message output is enabled on the user terminal.

By default, terminal display is disabled.

Step 6 Run:

```
terminal trapping
```

Traps display is enabled on the user terminal.

By default, traps display is enabled on the user terminal.

----End

9.3.5.2.9 Configuring the Device to Output Traps to a Log Host

Context

After configuring the device to output traps to a log host, you can view traps saved on the log host to monitor device running.

Pre-configuration Tasks

There is a reachable route between the device and the log host.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center loghost ip-address [ channel { channel-number | channel-name } |
facility local-number | { language language-name | binary [ port ] } ] *
```

The device is configured to output traps to the log host.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-
name } trap { state { off | on } | level severity } *
```

A rule for outputting traps to a channel is set.

By default, channel 2 is enabled to output traps and the lowest severity is **debugging**.

Step 4 (Optional) Run:

```
info-center loghost source interface-type interface-number
```

The source interface used by the device to send logs to a log host is specified.

By default, the source interface is the interface that sends logs.

After the source interface is specified, the log host determines the device that sends messages. The log host then can easily retrieve received messages.

----End

9.3.5.2.10 Configuring the Device to Output Traps to an SNMP Agent

Context

When an exception or a fault occurs on the device, the network administrator needs to learn the device running status. You can configure the device to output traps to an NMS server so that the network administrator can monitor the device in real time and locate faults immediately. Before configuring the device to output traps to an NMS server, configure the device to output traps to an SNMP agent. Then the SNMP agent sends traps to the NMS server.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center snmp channel { channel-number | channel-name }
```

The channel used by the device to output traps to an SNMP agent is specified.

By default, the device uses channel 5 to output traps to an SNMP agent.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } trap { state { off | on } | level severity } *
```

A rule for outputting traps to a channel is set.

By default, channel 5 is enabled to output traps and the lowest severity is **debugging**.

Step 4 Run:

```
snmp-agent
```

The SNMP agent function is enabled.

By default, the SNMP agent function is disabled.

The SNMP agent can work properly and receive traps only when the SNMP agent function is enabled.

NOTE

For details on how to configure the SNMP agent, see **10.1 SNMP Configuration** in the *Huawei Wireless Access Points Configuration Guide - Network Management*.

----End

9.3.5.2.11 Checking the Configuration

Procedure

- Run the **display channel** [*channel-number* | *channel-name*] command to view the channel configuration.
- Run the **display info-center filter-id** [*id* | **bymodule-alias** *modname alias*] command to view information filtered by the information center.
- Run the **display info-center logfile path** command to check the path where log files are saved.
- Run the **display logfile** *file-name* [*offset* | **hex**] * command to check the log file.
- Run the **display trapbuffer** [**size** *value*] command to check traps recorded in the trap buffer.

----End

9.3.5.3 Configuring Debugging Message Output

Debugging messages of a specific module can be output to the log file, console, terminal, or log host.

Pre-configuration Tasks

Before enabling debugging message output, complete the following task:

Starting the AP

NOTICE

Debugging occupies CPU resources on the device, affecting system running. After debugging, run the **undo debugging all** command to disable it immediately.

Configuration Process

Table 9-12 lists the configuration process for enabling debugging message output.

Table 9-12 Configuration process for enabling debugging message output

No.	Configuration Task	Description	Remarks
1	**9.3.5.3.1 Enabling the Information Center**	You can configure the information center only after the information center is enabled. By default, the information center is enabled.	Steps 2 and 3 are optional and can be performed in any sequence.
2	**9.3.5.3.2 (Optional) Naming an Information Channel**	You can easy-to-remember names for channels to facilitate information center usage.	
3	**9.3.5.3.3 (Optional) Setting the Timestamp Format of Debugging Messages**	To adjust the time format and time precision for information output, configure the timestamp.	
4	**9.3.5.3.4 Configuring the Device to Output Debugging Messages to the Log File**	After debugging messages are output to a log file, you can download the log file anytime to monitor device running based on debugging messages.	Steps 4 to 7 can be performed in any sequence. You can view debugging messages in the console or terminal.
5	**9.3.5.3.5 Configuring the Device to Output Debugging Messages to the Console**	After debugging messages are output to the console, you can view debugging messages on the console (host from which you can log in to the through the console interface) to monitor device running.	
6	**9.3.5.3.6 Configuring the Device to Output Debugging Messages to the Terminal**	After debugging messages are output to a user terminal, you can view debugging messages on the user terminal (host from which you log in to the AP through STelnet) to monitor device running.	

No.	Configuration Task	Description	Remarks
7	9.3.5.3.7 Configuring the Device to Output Debugging Messages to the Log Host	After configuring the AP to output debugging messages to a log host, you can view debugging messages saved on the log host to monitor device running.	

9.3.5.3.1 Enabling the Information Center

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center enable
```

The information center is enabled.

By default, the information center is enabled.

----End

9.3.5.3.2 (Optional) Naming an Information Channel

Context

You can rename channels, which facilitates memorization and usage.

NOTE

Channel names must be unique. It is recommended that channel names represent channel functions.

The following lists default channel names.

Table 9-13 Default channel names

Channel Number	Default Channel Name
0	console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer

Channel Number	Default Channel Name
5	snmpagent
6	channel6
7	channel7
8	channel8
9	channel9

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center channel channel-number name channel-name
```

A name is configured for the information channel with the specified number.

----End

9.3.5.3.3 (Optional) Setting the Timestamp Format of Debugging Messages

Context

To adjust the time format and time precision for information output, configure the timestamp.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center timestamp debugging { { date | short-date | format-date } [ precision-time { tenth-second | second } ] | boot | none }
```

The timestamp format of debugging messages is set.

By default, the timestamp format of debugging messages is **date**.

----End

9.3.5.3.4 Configuring the Device to Output Debugging Messages to the Log File

Context

After debugging messages are output to a log file, you can download the log file anytime to monitor device running based on debugging messages.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center logfile channel { channel-number | channel-name }
```

The channel used by the device to output debugging messages to a log file is specified.

By default, the device uses channel 9 to output debugging messages into a log file.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } debug { state { off | on } | level severity } *
```

A rule for outputting debugging messages to a channel is set.

By default, channel 9 is disabled to output debugging messages and the lowest severity is **debugging**.

Step 4 (Optional) Run:

```
info-center logfile path path
```

The path where log files are saved is specified.

Step 5 (Optional) Run:

```
info-center logfile size size
```

The log file size is set.

By default, the log file size is 1 MB.

NOTE

If the size of a log file generated on the device exceeds the configured log file size, the system decompresses the log file into a zip file.

Step 6 (Optional) Run:

```
info-center max-logfile-number filenumbers
```

The maximum number of log files that can be saved is set.

By default, a maximum of 200 log files can be saved.

If the number of log files generated on the AP exceeds the limit, the system deletes the oldest log file.

----End

9.3.5.3.5 Configuring the Device to Output Debugging Messages to the Console

Context

After debugging messages are output to the console, you can view debugging messages on the console (host from which you can log in to the device through the console interface) to monitor device running.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center console channel { channel-number | channel-name }
```

A channel used by the device to output debugging messages to the console is specified.

By default, the device uses channel 0 to output debugging messages to the console.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } debug { state { off | on } | level severity } *
```

A rule for outputting debugging messages to a channel is set.

By default, channel 0 is enabled to output debugging messages and the lowest severity is **debugging**.

Step 4 Run:

```
quit
```

Return to the user view.

Step 5 Run:

```
terminal monitor
```

Display of logs, traps, and debugging message output is enabled on the user terminal.

By default, terminal display is disabled.

Step 6 Run:

```
terminal debugging
```

Debugging message display is enabled on the user terminal.

By default, debugging message display is disabled on the user terminal.

----End

9.3.5.3.6 Configuring the Device to Output Debugging Messages to the Terminal

Context

After debugging messages are output to a user terminal, you can view debugging messages on the user terminal (host from which you log in to the device through STelnet) to monitor device running.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center monitor channel { channel-number | channel-name }
```

A channel used by the device to output debugging messages to a user terminal is specified.

By default, the device uses channel 1 to output debugging messages to a user terminal.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } debug { state { off | on } | level severity } *
```

A rule for outputting debugging messages to a channel is set.

By default, channel 1 is enabled to output debugging messages and the lowest severity is **debugging**.

Step 4 Run:

```
quit
```

Return to the user view.

Step 5 Run:

```
terminal monitor
```

Display of logs, traps, and debugging message output is enabled on the user terminal.

By default, terminal display is disabled.

Step 6 Run:

```
terminal debugging
```

Debugging message display is enabled on the user terminal.

By default, debugging message display is disabled on the user terminal.

----End

9.3.5.3.7 Configuring the Device to Output Debugging Messages to the Log Host

Context

After configuring the device to output debugging messages to a log host, you can view debugging messages saved on the log host to monitor device running.

Prerequisites

- There is a reachable route between the device and the log host.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
info-center loghost ip-address [ channel { channel-number | channel-name } | facility local-number | { language language-name | binary [ port ] } ] *
```

The device is configured to output debugging messages to the log host.

Step 3 Run:

```
info-center source { module-name | default } channel { channel-number | channel-name } debug { state { off | on } | level severity } *
```

A rule for outputting debugging messages to a channel is set.

By default, channel 2 is disabled to output debugging messages and the lowest severity is **debugging**.

Step 4 (Optional) Run:

```
info-center loghost source interface-type interface-number
```

The source interface used by the device to send logs to a log host is specified.

By default, the source interface is the interface that sends logs.

After the source interface is specified, the log host determines the device that sends messages. The log host then can easily retrieve received messages.

----End

9.3.5.3.8 Checking the Configuration

Procedure

- Run the **display channel** [*channel-number* | *channel-name*] command to view the channel configuration.
- Run the **display info-center filter-id** [*id* | **bymodule-alias** *modname alias*] command to view information filtered by the information center.
- Run the **display info-center logfile path** command to check the path where log files are saved.
- Run the **display logfile** *file-name* [*offset* | **hex**] * command to check the log file.

----End

9.3.6 Maintaining the Information Center

This section describes how to maintain the information center.

9.3.6.1 Clearing Statistics

Context

NOTICE

Statistics of the information center cannot be restored after you clear them. Exercise caution when running the commands.

Procedure

- To clear the statistics of the information center, run the **reset info-center statistics** command in the user view.
- To clear the statistics in the log buffer, run the **reset logbuffer** command in the user view.
- To clear the statistics in the trap buffer, run the **reset trapbuffer** command in the user view.

----End

9.3.6.2 Monitoring the Information Center

Procedure

- Run the **display info-center** command to view output configuration of the information center.
- Run the **display info-center statistics** command to view statistics of the information center.
- Run the **display logbuffer** command to view logs recorded in the log buffer.
- Run the **display logfile** *file-name* [*offset* | **hex**] * command to view the log file.
- Run the **display trapbuffer** [**size** *value*] command to view traps recorded in the trap buffer.

----End

9.3.7 Configuration Examples

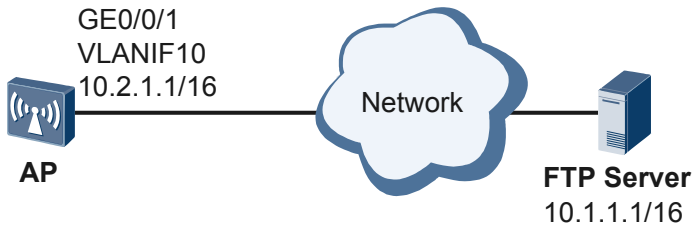
This section provides several configuration examples of the information center, covering networking requirements, configuration notes, and configuration roadmap.

9.3.7.1 Example for Outputting Logs to the Log File

Networking Requirements

As shown in **Figure 9-8**, the device connects to the FTP Server through the Internet and has a reachable route to the FTP server. The network administrator wants to use the FTP server to view logs generated by the device and learn the device running status.

Figure 9-8 Networking diagram of outputting log information to the log file



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the information center.
2. Configure a channel and a rule for outputting logs to a log file so that logs are saved in the log file.
3. Configure the device to transfer the log file to the FTP server so that the network administrator can use the FTP server to view logs generated by the device.

Procedure

Step 1 Enable the information center.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] info-center enable
```

Step 2 Configure a channel and a rule for outputting logs to a log file.

Configure a channel for outputting logs to a log file.

```
[AP] info-center logfile channel channel6
```

NOTE

By default, channel 9 is used to send logs to a log file. If the default setting is used, skip this step.

Configure a rule for outputting logs to a log file.

```
[AP] info-center source ip channel channel6 log level warning
```

Step 3 Configure the IP address of the interface that connects the device to the FTP server.

```
[AP] vlan 10
[AP-vlan10] quit
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[AP-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[AP-GigabitEthernet0/0/1] quit
[AP] interface vlanif10
[AP-Vlanif10] ip address 10.2.1.1 255.255.0.0
[AP-Vlanif10] quit
[AP] quit
```

Step 4 Configure the device to transfer the log file to the FTP server.

Log in to the FTP server with the user name **huawei** and password **huawei**.

```
<AP> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
```

Transfer the log file to the FTP server.

```
[AP-ftp] put flash:/logfile/log.log
200 PORT command okay
150 Opening ASCII mode data connection for log.log.
226 Transfer complete.
FTP: 2761463 byte(s) sent in 26.062 second(s) 105.95Kbyte(s)/sec.
[AP-ftp] quit
```

Step 5 Verify the configuration.

View information recorded by the channel.

```
<AP> display info-center
Information Center: enabled
Log host:
Console:
        channel number: 0, channel name: console
Monitor:
        channel number: 1, channel name: monitor
SNMP Agent:
        channel number: 5, channel name: snmpagent
Log buffer:
        enabled
        max buffer size: 1024, current buffer size: 512
        current messages: 204, channel number: 4, channel name: logbuffer
        dropped messages: 0, overwritten messages: 0
Trap buffer:
        enabled
        max buffer size: 1024, current buffer size: 256
        current messages: 256, channel number: 3, channel name: trapbuffer
        dropped messages: 0, overwritten messages: 29
Logfile:
        channel number: 6, channel name: channel6, language: English
Information timestamp setting:
        log - date, trap - date, debug - date

 Sent messages = 1514, Received messages = 1514
```

View the received logs on the FTP server.

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
 info-center source IP channel 6 log level warning
 info-center logfile channel 6
#
vlan batch 10
#
interface
Vlanif10
 ip address 10.2.1.1 255.255.0.0
#
interface
GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
ip route-static 10.1.0.0 255.255.0.0 10.2.1.2
#
return
```

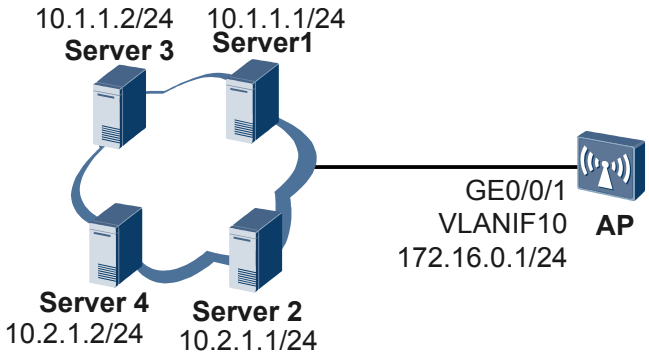
9.3.7.2 Example for Outputting Logs to a Log Host

Networking Requirements

As shown in **Figure 9-9**, the AP connects to four log hosts and has reachable routes to the log hosts. Log hosts are required to have reliability and receive logs of different types so that the

network administrator can monitor logs generated by different modules on the device in real time.

Figure 9-9 Networking diagram of outputting log information to the log host



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the information center.
2. Configure the AP to send logs of notification generated by the FIB and IP modules to Server1, and specify Server3 as the backup of Server1. Configure the AP to send warning logs generated by the PPP and AAA modules to Server2, and specify Server4 as the backup of Server2.
3. Configure the log host on the server so that the network administrator can receive logs generated by the AP on the log host.

Procedure

Step 1 Enable the information center.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] info-center enable
```

Step 2 Configure a channel and a rule for outputting logs to a log host.

Name a channel.

```
[AP] info-center channel 6 name loghost1
[AP] info-center channel 7 name loghost2
```

Configure a channel for outputting logs to a log host.

```
[AP] info-center loghost 10.1.1.1 channel loghost1
[AP] info-center loghost 10.2.1.1 channel loghost2
[AP] info-center loghost 10.1.1.2 channel loghost1
[AP] info-center loghost 10.2.1.2 channel loghost2
```

Configure rules for outputting logs to log hosts.

```
[AP] info-center source fib channel loghost1 log level notification
[AP] info-center source ip channel loghost1 log level notification
```

```
[AP] info-center source ppp channel loghost2 log level warning
[AP] info-center source aaa channel loghost2 log level warning
```

Step 3 Specify the source interface for sending logs.

Specify the source interface for sending logs.

```
[AP] vlan 10
[AP-vlan10] quit
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port hybrid pvid vlan 10
[AP-GigabitEthernet0/0/1] port hybrid untagged vlan 10
[AP-GigabitEthernet0/0/1] quit
[AP] interface vlanif10
[AP-Vlanif10] ip address 172.16.0.1 255.255.255.0
[AP-Vlanif10] quit
[AP] info-center loghost source vlanif 10
```

Step 4 Configure the log host on the server.

The AP can generate many logs, which may exceed its limited storage space. To address this problem, configure a log server to store all the logs.

The log host can run the Unix or Linux operating system or run a third party's log software. For detailed configuration procedure, see the related manual.

Step 5 Verify the configuration.

View the configured lost host.

```
<AP> display info-center
Information Center: enabled
Log host:
        the interface name of the source address:Vlanif10
        10.1.1.1, channel number: 6, channel name: loghost1
        language: english, host facility: local7
        10.2.1.1, channel number: 7, channel name: loghost2
        language: english, host facility: local7
        10.1.1.2, channel number: 6, channel name: loghost1
        language: english, host facility: local7
        10.2.1.2, channel number: 7, channel name: loghost2
        language: english, host facility: local7
Console:
         channel number : 0, channel name : console
Monitor:
         channel number : 1, channel name : monitor
SNMP Agent:
         channel number : 5, channel name : snmpagent
Log buffer:
        enabled
        max buffer size: 1024, current buffer size: 512
        current messages: 218, channel number: 4, channel name: logbuffer
        dropped messages: 0, overwritten messages: 0
Trap buffer:
        enabled
        max buffer size: 1024, current buffer size: 256
        current messages: 256, channel number: 3, channel name: trapbuffer
        dropped messages: 0, overwritten messages: 150
Logfile:
        channel number: 9, channel name: channel9, language: English
Information timestamp setting:
         log - date, trap - date, debug - date

 Sent messages = 683, Received messages = 682
```

View the received logs on the NMS. The configuration details are not mentioned here.

----End

Configuration Files

- Configuration file of the AP

```
#
 info-center channel 6 name loghost1
 info-center channel 7 name loghost2
 info-center source FIB channel 6 log level notification
 info-center source IP channel 6 log level notification
 info-center source PPP channel 7 log level warning
 info-center source AAA channel 7 log level warning
 info-center loghost source Vlanif10
 info-center loghost 10.1.1.1 channel 6
 info-center loghost 10.2.1.1 channel 7
 info-center loghost 10.1.1.2 channel 6
 info-center loghost 10.2.1.2 channel 7
#
vlan batch 10
#
interface
Vlanif10
 ip address 172.16.0.1
255.255.255.0
#
interface
GigabitEthernet0/0/1
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
#
 ip route-static 10.1.1.0 255.255.255.0 172.16.0.2
 ip route-static 10.2.1.0 255.255.255.0 172.16.0.2
#
return
```

9.3.7.3 Example for Outputting Traps to the SNMP Agent

Networking Requirements

As shown in **Figure 9-10**, the AP connects to the NMS station. The network administrator wants to view traps generated by the AP on the NMS station to monitor device running and locate faults.

Figure 9-10 Networking diagram for outputting traps to the SNMP agent

Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the information center.
2. Configure a channel and a rule for outputting traps to the SNMP agent so that the SNMP agent can receive traps generated by the AP.
3. Configure the AP to output traps to the NMS station so that the NMS station can receive traps generated by the AP.

Procedure

Step 1 Enable the information center.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] info-center enable
```

Step 2 Configure a channel and a rule for outputting traps to the SNMP agent.

Configure a channel for outputting traps to the SNMP agent.

```
[AP] info-center snmp channel channel7
```

Configure a rule for outputting traps to the SNMP agent.

```
[AP] info-center source ip channel channel7 trap level informational state on
```

NOTE

By default, the device uses the SNMP agent to output traps of all modules.

Step 3 Configure the SNMP agent to output traps to the NMS station.

Enable the SNMP agent and set the SNMP version to SNMPv2c.

```
[AP] snmp-agent sys-info version v2c
```

Configure the SNMPv2c read-write community name.

```
[AP] snmp-agent community write huawei123
```

Configure the trap function.

```
[AP] snmp-agent trap enable
Info: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y
[AP] snmp-agent target-host trap-hostname nms address 10.1.1.1 trap-paramsname
trapnms
[AP] snmp-agent target-host trap-paramsname trapnms v2c securityname public
[AP] quit
```

Step 4 Verify the configuration.

View the channel used by the SNMP agent to output traps.

```
<AP> display info-center
Information Center: enabled
Log host:
Console:
        channel number: 0, channel name: console
Monitor:
        channel number: 1, channel name: monitor
SNMP Agent:
        channel number: 7, channel name: channel7
Log buffer:
        enabled
        max buffer size: 1024, current buffer size: 512
        current messages: 242, channel number: 4, channel name: logbuffer
        dropped messages: 0, overwritten messages: 0
```

```
Trap buffer:
        enabled
        max buffer size: 1024, current buffer size: 256
        current messages: 256, channel number: 3, channel name: trapbuffer
        dropped messages: 0, overwritten messages: 2190
Logfile:
        channel number: 9, channel name: channel9, language: English
Information timestamp setting:
        log - formate-date, trap - date, debug - date

 Sent messages = 5647, Received messages = 5647
```

View traps output through the channel used by the SNMP agent.

```
<AP> display channel 7
channel number: 7, channel name: channel7
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging
c16a0000 IP       Y      debugging     Y      informational N      debugging
```

View traps output to the NMS station by the SNMP agent.

```
<AP> display snmp-agent target-host
   Traphost list:
   Target host name: nms
   Traphost address: 10.1.1.1
   Traphost portnumber: 162
   Target host parameter: trapnms

   Total number is 1

   Parameter list trap target host:
   Parameter name of the target host: trapnms
   Message mode of the target host: SNMPV2C
   Trap version of the target host: v2c
   Security name of the target host: public

   Total number is 1
```

----End

Configuration Files

- Configuration file of the AP

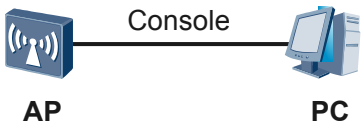
```
#
 snmp-agent local-engineid 800007DB030819A6D0269A
 snmp-agent community write %$%$sqZd.Z5;=9}%}USLx>3D,!HA%$%$
 snmp-agent sys-info version v2c
 snmp-agent target-host trap-hostname nms address 10.1.1.1 udp-port 162 trap-
paramsname trapnms
 snmp-agent target-host trap-paramsname trapnms v2c securityname public
 snmp-agent trap enable
 snmp-agent
#
 info-center source IP channel 7 trap level informational
 info-center snmp channel 7
#
return
```

9.3.7.4 Example for Outputting Traps to the Console

Networking Requirements

As shown in **Figure 9-11**, the PC connects to the AP through a console interface. It is required that debugging messages of the ARP module be displayed on the PC.

Figure 9-11 Networking diagram for outputting debugging messages to the console



Configuration Roadmap

The configuration roadmap is as follows:

1. Enable the information center.
2. Configure a channel and a rule for outputting debugging messages to the console so that debugging messages generated by the AP can be sent to the console.
3. Enable terminal display so that users can use the terminal to view debugging messages generated by the AP.

Procedure

Step 1 Enable the information center.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] info-center enable
```

Step 2 Configure a channel and a rule for outputting debugging messages to the console.

Configure a channel for outputting debugging messages to the console.

```
[AP] info-center console channel console
```

Configure a rule for outputting debugging messages to the console.

```
[AP] info-center source arp channel console debug level debugging state on
[AP] quit
```

Step 3 Enable terminal display.

```
<AP> terminal monitor
Info: Current terminal monitor is on.
<AP> terminal debugging
Info: Current terminal debugging is on.
```

Step 4 Debug the ARP module.

```
<AP> debugging arp packet
```

Step 5 Verify the configuration.

View debugging message output through the channel used by the SNMP agent.

```
<AP> display channel 0
channel number: 0, channel name: console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging
c16e0000 ARP      Y      warning       Y      debugging     Y      debugging
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
 info-center source ARP channel 0
#
return
```

9.4 Fault Management Configuration

The fault management configuration allows users to collect fault information and locate faults quickly and efficiently at the NMS side.

9.4.1 Introduction to Fault Management

This section describes the definition and functions of fault management.

Definition

Fault management efficiently manages and reports alarms or events generated on a device in a centralized manner.

Purpose

The network expands and becomes more complex. When a module on a device is faulty, a great number of alarms may be generated on one or more devices. The alarms, however, may be lost when being sent to the NMS due to limited capability of handling alarms on the devices or the NMS. As a result, certain needed alarms cannot be displayed, which inconveniences network management.

To collect valid fault information on the NMS in an efficient way, configure the alarm severity and alarm reporting delay function to efficiently manage and report alarms and events in a centralized manner.

9.4.2 Principles

This section describes the implementation principle of fault management.

9.4.2.1 Concepts

- Alarm:

An alarm is generated when a device notifies users of a fault. Maintenance personnel learn the device running status and locate faults based on alarms.

- Active alarm:

  An active alarm is the notification of generating an alarm. For example, the hwFanInvalid alarm indicates that the fan is faulty.

- Clear alarm:

  A clear alarm is the notification of clearing an alarm. For example, the hwFanInvalidResume alarm indicates that the fan fault is rectified.

  NOTE

  Each active alarm maps a clear alarm.

- Root-cause alarm:

  A root-cause alarm causes other alarms. For example, an unreachable route is caused by the interface fault. The alarm generating due to an interface fault is a root-cause alarm.

- Non-root-cause alarm:

  Non-root-cause alarms are caused by the root-cause alarm. For example, an unreachable route is caused by the interface fault. The alarm generating due to the unreachable route is a non-root-cause alarm.

- Intermittent alarm:

  If the interval between the generation time and clearance time of an alarm is shorter than a specified value (called intermittent threshold that is specified based on the products and alarms), the alarm is called an intermittent alarm. An intermittent alarm lasts a short time of period from generation to clearance.

- Flapping alarm:

  If the number of times that an alarm on an object is generated in a specified period is larger than the flapping threshold that is specified based on the product and alarm, the generated alarms are called flapping alarms.

- Event:

  An event is anything that occurs on a managed object. For example, an object is added, deleted, modified, or its status is changed.

9.4.2.2 Principles

When receiving alarms or events generated on the device, the fault management module stores them based on the default severities, records the generation time.

After the fault management function is configured, you can:

- Change the alarm severities on the device and configure filtering rules on the NMS to filter out unnecessary alarms.
- Enable the alarm or events reporting delay function to prevent alarms or events from being reported repeatedly. When the alarm or event reporting delay period expires, only the last alarm or events is reported.
- Alarm correlation can identify root-cause and non-root-cause alarms. Non-root-cause alarms are filtered out. The system reports only root-cause alarms to the NMS, improving the efficiency for locating faults.

9.4.2.3 Alarm Severity

As defined in X.733, alarms are classified into six severities, as described in **Table 9-14**. A small value indicates a higher severity.

Table 9-14 Descriptions of alarm severities

Value	Severity	Description
1	Critical	Indicates that a fault affecting services has occurred and it must be rectified immediately.
2	Major	Indicates that services are being affected and related measures need to be taken urgently.
3	Minor	Indicates that a fault occurs but does not affect services. To avoid a minor alarm from getting severer, related measures must be immediately taken.
4	Warning	Indicates that a potential or impending service-affecting fault is detected before any significant effects have been felt. Take corrective actions to diagnose and rectify the fault.
5	Indeterminate	Indicates that the severity of an alarm cannot be determined.
6	Cleared	Indicates that one or more previous alarms have been cleared.

9.4.2.4 Alarm Correlation

When an NE on the network is faulty, the system reports the predictable network faults to the NMS. Each fault triggers multiple alarms, affecting the efficiency for locating faults. Some alarms are triggered by the same fault, so they are associated with each other. The alarm correlation function can analyze the association among alarms generated in the system and determine root-cause and non-root-cause alarms. After alarm correlation suppression is configured, the system reports only root-cause alarms to the NMS, improving the efficiency for locating faults. Alarm correlation reduces the number of reported non-root-cause alarms, reduces the network load, and helps quickly locate faults.

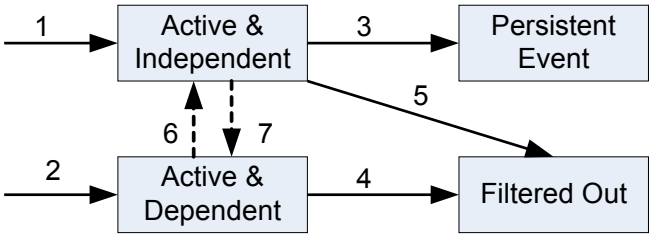
Alarm correlation includes alarm correlation analysis and alarm correlation suppression.

- **Alarm correlation analysis**

  Alarm correlation analysis is performed based on the alarm definition, including the fault time window, fault rectification time window, what the root-cause alarm is, and the method of association with the root-cause alarm. After receiving an alarm, the fault management module analyzes the alarm correlation within the duration specified by the fault time window, and sends the alarm with the analysis result to the NMS.

  Figure 9-12 shows the alarm correlation analysis flow.

Figure 9-12 Alarm correlation analysis flow



The status of an alarm can be:

- Active & Independent: An active root-cause alarm is in the period specified by the fault time window.
- Active & Dependent: An active non-root-cause alarm is in the period specified by the fault time window.
- Persistent Event: An alarm enters the active alarm queue.
- Filtered Out: An alarm and its clear alarm are both deleted from the active alarm queue.

The process of alarm correlation analysis is as follows:

1. If an alarm is considered as a root-cause alarm, it is suppressed for a period specified by the fault time window.
2. If an alarm is considered as a non-root-cause alarm, it is suppressed for a period specified by the fault time window of its parent alarm.
3. When the duration specified by the fault time window of the root-cause alarm expires, the system sends both the root-cause and non-root-cause alarms.
4. If the clear alarm of a non-root-cause alarm is generated within the duration specified by the fault time window, the system deletes them both.
5. If the clear alarm of a root-cause alarm is generated within the duration specified by the fault time window, the system deletes them both.
6. If the root-cause alarm of an alarm is not generated within the duration specified by the fault time window, the system considers this alarm as a root-cause alarm.
7. If the root-cause alarm of an alarm is generated within the duration specified by the fault time window, the system considers this alarm as a non-root-cause alarm.

- **Alarm correlation suppression**

  When alarm correlation analysis is complete, an alarm carries an identifier indicating a root-cause alarm or a non-root-cause alarm. Before sending an alarm to the SNMP agent, the system checks whether NMS-based alarm suppression has been configured for non-root-cause alarms.

  - If so, the system filters out non-root-cause alarms and sends only root-cause alarms to the NMS.
  - If not, the system sends both root-cause alarms and non-root-cause alarms to the NMS.

9.4.3 Default Configuration

This section describes default parameter settings of the device.

Table 9-15 Default configuration of fault management

Parameter	Default Setting
Alarm reporting delay function	Enabled
Alarm correlation analysis	Disabled
Event reporting delay function	Enabled

9.4.4 Configuring Fault Management

This section describes how to configure fault management.

9.4.4.1 Configuring Alarm Management

Alarm management includes setting alarm severities, alarm correlation suppression, and enabling alarm reporting delay.

Pre-configuration Tasks

Before configuring alarm management, complete the following task:

Powering on the device and ensuring a successful self-check

9.4.4.1.1 Setting the Alarm Severity

Context

The system defines default alarm severity for each alarm. Users can change the alarm severity. When receiving alarms reported by a device, the NMS can configure filtering rules to display only alarms of a specified severity.

As defined in X.733, alarms are classified into six severities, as described in **Table 9-16**. A small value indicates a higher severity.

Table 9-16 Descriptions of alarm severities

Value	Severity	Description
1	Critical	Indicates that a fault affecting services has occurred and it must be rectified immediately.
2	Major	Indicates that services are being affected and related measures need to be taken urgently.
3	Minor	Indicates that a fault occurs but does not affect services. To avoid a minor alarm from getting severer, related measures must be immediately taken.

Value	Severity	Description
4	Warning	Indicates that a potential or impending service-affecting fault is detected before any significant effects have been felt. Take corrective actions to diagnose and rectify the fault.
5	Indeterminate	Indicates that the severity of an alarm cannot be determined.
6	Cleared	Indicates that one or more previous alarms have been cleared.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
alarm
```

The alarm view is displayed.

Step 3 (Optional) Run:

```
display alarm information [ name alarm-name ]
```

The alarm severity is displayed.

Step 4 Run:

```
alarm-name alarm-name severity severity
```

The alarm severity is changed.

The system has defined default alarm severity for each alarm.

----End

9.4.4.1.2 Configuring the Alarm Reporting Delay Function

Context

When an alarm is reported repeatedly, users cannot locate faults in an efficient manner. After the alarm reporting delay function is enabled and the delay is configured, a large number of invalid alarms are prevented from being reported.

After the alarm reporting delay function is enabled,

- If no clear alarm is generated during the period, the alarm is reported to the NMS when the period expires.
- If a clear alarm is generated during this period, the alarm and its clear alarm are both deleted from the alarm queue and will not be reported to the NMS.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
alarm
```

The alarm view is displayed.

Step 3 Run:

```
delay-suppression enable
```

The alarm reporting delay function is enabled.

By default, the alarm reporting delay function is enabled.

Step 4 (Optional) Run:

```
display alarm information [ name alarm-name ]
```

The delay in reporting alarms is displayed.

Step 5 (Optional) Run:

```
suppression alarm-name alarm-name cause-period cause-seconds
```

The delay in reporting alarms is configured.

The system defines a default delay in reporting alarms.

----End

9.4.4.1.3 Configuring Alarm Correlation Suppression

Context

Before configuring alarm correlation suppression, enable alarm correlation analysis to analyze alarm types including root-cause and non-root-cause. For a non-root-cause alarm, the system marks the sequence number of its root-cause alarm on the non-root-cause alarm. After alarm correlation suppression is configured, the system filters out non-root-cause alarms and reports only root-cause alarms to the NMS.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
alarm
```

The alarm view is displayed.

Step 3 Run:

```
correlation-analyze enable
```

Alarm correlation analysis is enabled.

By default, alarm correlation analysis is disabled.

Step 4 Run the following commands to configure NMS-based or interface-based alarm correlation suppression.

NOTE

You can configure one or both of NMS-based and interface-based alarm correlation suppression functions.

- Configuring NMS-based alarm correlation suppression
  1. Run:

     quit

     The system view is displayed.
  2. Run:

     alarm correlation-suppress enable target-host *ip-address* **securityname** *securityname*

     Alarm correlation suppression based on the NMS IPv4 address is enabled.
- Configuring interface-based alarm correlation suppression

  Run:

  mask interface *interface-type interface-number*

  Interface-based alarm correlation suppression is enabled.

  By default, interface-based alarm correlation suppression is disabled.

  NOTE

  After interface-based alarm correlation suppression is configured, root-cause and non-root-cause LinkDown alarms generated on the interface are not reported to the NMS.

----End

9.4.4.1.4 Checking the Configuration

Context

- Run the **display alarm information** [**name** *alarm-name*] command to view the specified alarm configuration.
- Run the **display this** command in the alarm view to view the alarm configuration.

9.4.4.2 Configuring the Event Reporting Delay Function

The event reporting delay function prevents events from being reported repeatedly.

Context

After the event reporting delay function is enabled and the period of delay is configured, the system discards the event that is generated several times during the delay. When the delay expires, the system reports the only first event.

Pre-configuration Tasks

Before configuring the event reporting delay function, complete the following tasks:

Powering on the device and ensuring a successful self-check

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
event
```

The event view is displayed.

Step 3 Run:

```
delay-suppression enable
```

The event reporting delay function is enabled.

By default, the event reporting delay function is enabled.

Step 4 (Optional) Run:

```
display event information [ name event-name ]
```

The period of delay in reporting events is displayed.

Step 5 (Optional) Run:

```
suppression event-name event-name period seconds
```

The period of delay in reporting events is configured.

The system has defined a default period of delay in reporting events.

NOTE

Run the **undo suppression event-name** and **display event information** commands in sequence to view the default period of reporting delay.

----End

Checking the Configuration

- Run the **display event information** [**name** *event-name*] command to view the event configuration.
- Run the **display this** command in the event view to view the event configuration.

9.4.5 Maintenance

This section describes how to monitor and clear alarms and events.

9.4.5.1 Clearing Alarms and Events

Context

NOTICE

The cleared alarm or event statistics cannot be restored. Confirm the action before you run the command.

Procedure

- Clearing alarms
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     alarm

     The alarm view is displayed.
  3. Run:
     clear alarm active { **all** | **sequence-number** *sequence-number* }

     Active alarms on the device are cleared.
- Clearing events
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     event

     The event view is displayed.
  3. Run:
     clear event all

     Events on the device are cleared.

----End

9.4.5.2 Monitoring Alarms and Events

Procedure

- Monitoring alarms
  - Run:
    display alarm active

    Active alarms on the device are displayed.

- Run:

  ```
  display alarm history
  ```

  Historical alarms on the device are displayed.

- Monitoring events
  - Run:

    ```
    display event
    ```

    Events on the device are displayed.

----End

9.4.6 Configuration Examples

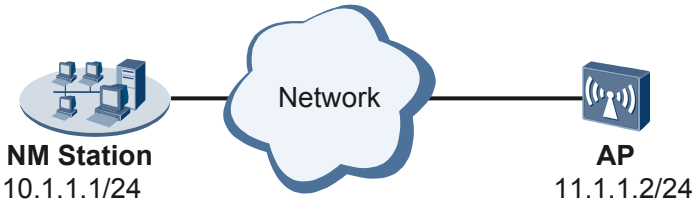
This section describes fault management configurations based on the configuration flowchart, including networking requirements, configuration roadmap, and configuration procedure.

9.4.6.1 Example for Configuring Alarm Management

Networking Requirements

As shown in **Figure 9-13**, the route between the device and the NMS is reachable. Users want to view alarms generated by the device on the NMS in real time. Users must monitor the LinkDown alarm to ensure the normal interconnection of the device.

Figure 9-13 Networking for configuring alarm management



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the alarm severity to **major**, allowing users to monitor LinkDown alarms on the NMS in real time based on the alarm filtering rules.
2. Configure the alarm reporting delay function to prevent repetitive or flapping alarms from being reported to the NMS.
3. Configure NMS-based alarm correlation suppression to report only root-cause alarms to the NMS.

Procedure

Step 1 Configure an SNMPv3 user and an NMS host.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] snmp-agent
[AP] snmp-agent sys-info version v3
[AP] snmp-agent mib-view linkdown include linkDown
```

```
[AP] snmp-agent group v3 huawei privacy notify-view linkdown
[AP] snmp-agent usm-user v3 user huawei authentication-mode md5
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
[AP] snmp-agent usm-user v3 user huawei privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
[AP] snmp-agent target-host trap-paramsname params v3 securityname user privacy
[AP] snmp-agent target-host trap-hostname nms address 10.1.1.1 udp-port 162 trap-paramsname params
[AP] snmp-agent trap enable feature-name IFNET trap-name linkDown
```

NOTE

In actual applications, you can select a version of the SNMP protocol based on the network requirements. For details, see **10.1 SNMP Configuration** in the *Huawei Wireless Access Points Configuration Guide-Network Management*.

Step 2 Set the severity for the linkDown alarm to **major**.

```
[AP] alarm
[AP-alarm] alarm-name linkDown severity major
```

Step 3 Enable the alarm reporting delay function.

```
[AP-alarm] delay-suppression enable
```

NOTE

By default, the alarm reporting delay function is enabled.

Step 4 Configure NMS-based alarm correlation suppression.

```
[AP-alarm] correlation-analyze enable
Info: Enable analyze correlation between alarms successfully
[AP-alarm] quit
[AP] alarm correlation-suppress enable target-host 10.1.1.1 securityname user
[AP] quit
```

Step 5 Verify the configuration.

Run the **display alarm information** command to view the alarm configuration.

```
<AP> display alarm information name linkDown
*********************************
  AlarmName: linkDown
  AlarmType: Alarm
  AlarmLevel: Major
  Suppress Period: 3s
  CauseAlarmName: NA
  Match VB Name: ifIndex
*********************************
```

Run the **display this** command in the alarm view to view the alarm configuration.

```
<AP> system
[AP] alarm
[AP-alarm] display this
#
alarm
 correlation-analyze enable
 alarm-name linkDown severity major
#
return
```

----End

Configuration Files

- Configuration file of the AP

```
#
sysname AP
#
 snmp-agent local-engineid 800007DB030819A6CDA894
 snmp-agent sys-info version v3
 snmp-agent group v3 huawei privacy notify-view linkdown
 snmp-agent target-host trap-hostname nms address 10.1.1.1 udp-port 162 trap-
par
amsname params
 snmp-agent target-host trap-paramsname params v3 securityname user privacy
 snmp-agent mib-view linnkdown include linkDown
 snmp-agent usm-user v3 user huawei authentication-mode md5
B07A9F99B3226D1200DC
D724E7E1D234
 snmp-agent usm-user v3 user huawei privacy-mode aes128
B07A9F99B3226D1200DCD724
E7E1D234
 snmp-agent trap enable feature-name IFNET trap-name linkDown
 snmp-agent
#
alarm
 correlation-analyze enable
 alarm-name linkDown severity major
#
return
```

9.4.7 References

This topic lists the references of fault management.

The following table lists the references of this document.

Document	Description	Remarks
X.733	CCITT standards for information technology–Open system interconnection–System management: alarm reporting function	-
G.7710	ITU-T standards for common equipment management function requirements	-

9.5 NTP Configuration

Network Time Protocol (NTP) synchronizes time among a set of distributed time servers and clients.

9.5.1 NTP Overview

This section describes the definition, purpose, and version evolution of NTP.

Definition

The Network Time Protocol (NTP) is an application layer protocol in the TCP/IP protocol suite. NTP is used to synchronize the time among a set of distributed time servers and clients. NTP is implemented based on the Internet Protocol (IP) and User Datagram Protocol (UDP). NTP packets are transmitted using UDP port 123.

Purpose

As network topologies become increasingly complex, clock synchronization becomes more important for devices on the entire network. If a system clock is modified manually by network administrators, the workload is heavy and the modification is error-prone, which affects clock precision. NTP is formulated as a networking protocol for clock synchronization between devices on a network.

NTP applies to the following situations where all the clocks of the devices on a network need to be consistent:

- In network management, analysis of logs or debugging messages collected from different routers requires time for reference.
- An accounting system requires that the clocks of all the devices be consistent.
- When several systems work together to process a complicated event, they have to refer to the same clock to ensure a correct execution order.
- Incremental backup between a backup server and clients requires that their clocks be synchronized.
- Some applications need to obtain the time in which a user logs in a system and a document is modified.

Version Evolution

NTP is evolved from the Time Protocol and the ICMP Timestamp message but is specifically designed to maintain accuracy and robustness. **Table 9-17** shows the NTP version evolution.

Table 9-17 NTP version evolution

Version	Date	Protocol Number	Description
NTPv1	June 1988	RFC 1059	NTPv1 puts forward complete NTP rules and algorithms for the first time, but it does not support authentication and control messages.
NTPv2	September 1989	RFC 1119	NTPv2 supports authentication and control messages.

Version	Date	Protocol Number	Description
NTPv3	March 1992	RFC 1305	NTPv3 uses correctness principles and improves clock selection and filter algorithms, and it is widely used.

9.5.2 Principles

This section describes the implementation of NTP.

9.5.2.1 Operating Principle

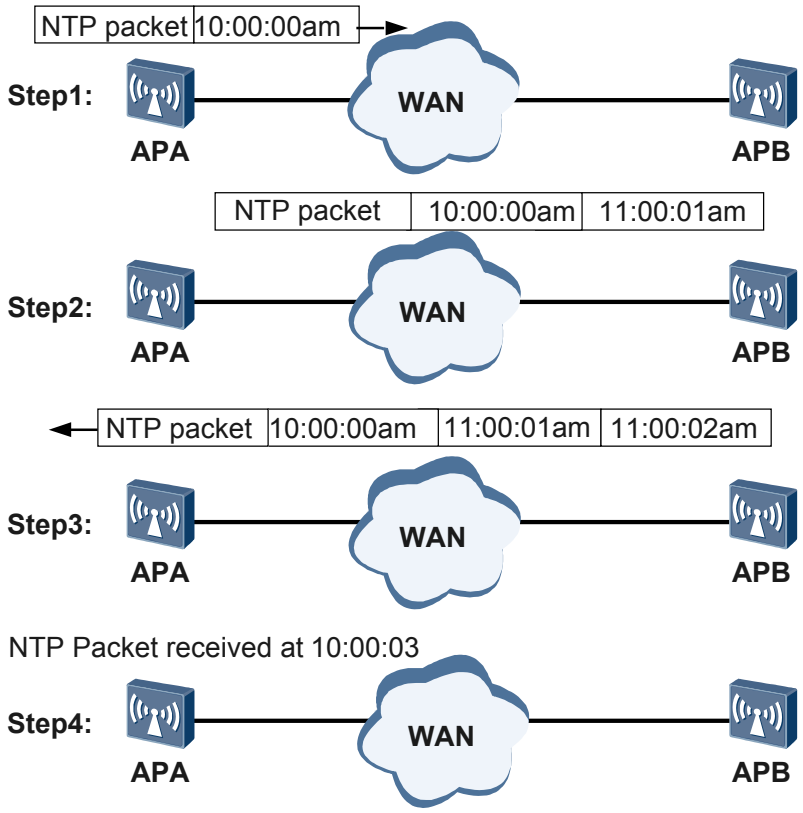
Figure 9-14 shows NTP implementation:

APA and APB are connected through a wide area network (WAN). Each of them has its own system clock, which is synchronized automatically through NTP.

Presuming that:

- Before the clocks of APA and APB are synchronized, the clock of APA is 10:00:00 a.m. and the clock of APB is 11:00:00 a.m.
- APB acts as an NTP time server, and APA must synchronize its clock with that of APB.
- It takes one second to unidirectionally transmit an NTP message between APA and APB.
- Both APA and APB take one second to process an NTP message.

Figure 9-14 Diagram of NTP implementation



The process of synchronizing the system clock is as follows:

1. APA sends an NTP message to APB. The message carries an initial timestamp, 10:00:00 a.m. (T1), indicating the time when it leaves APA.
2. When the NTP message reaches APB, APB adds the timestamp 11: 00:01 a.m. (T2) to the NTP message, indicting the time when APB receives the message.
3. When the NTP message leaves APB, APB adds the transmit timestamp 11:00:02 a.m. (T3) to the NTP message, indicating the time when the message leaves APB.
4. When APA receives this response message, it adds a new receive timestamp, 10:00:03 a.m. (T4).

   APA uses the information in the received message to calculate the following two important parameters:

   - Roundtrip delay of the NTP message: Delay = (T4 - T1) - (T3 - T2)
   - Clock offset of APA by taking APB as a reference: Offset = ((T2 - T1) + (T3 - T4))/2
5. After the calculation, APA knows that the roundtrip delay is 2 seconds and the clock offset of APA is 1 hour. APA sets its own clock based on these two parameters to synchronize its clock with that of APB.

NOTE

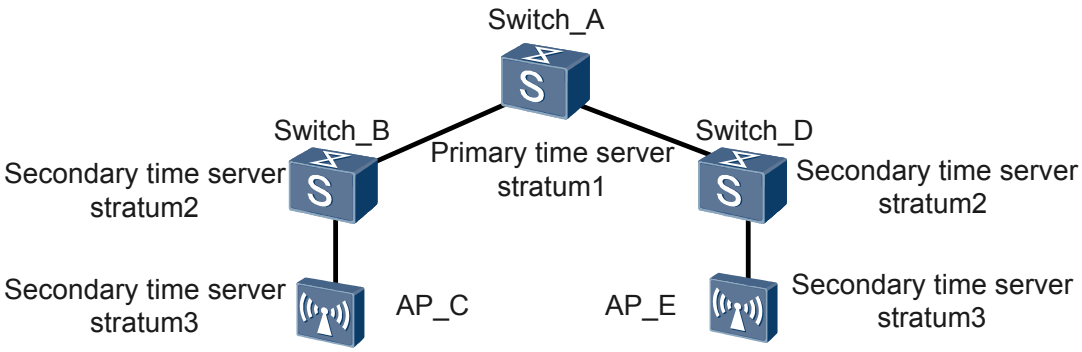
The preceding example is only a brief description of the operating principle of NTP. In fact, NTP uses the standard algorithms in RFC 1305 to ensure the precision of clock synchronization.

9.5.2.2 Network Architecture

The NTP network architecture involves the following concepts:

- **Synchronization subnet** consists of the primary time server, secondary time servers, and interconnecting transmission paths, as shown in **Figure 9-15**.
- **Primary time server** directly synchronizes its clock with a standard reference clock using a cable or radio. The standard reference clock is usually a radio clock or the Global Positioning System (GPS).
- **Secondary time server** synchronizes its clock with the primary time server or other secondary time servers on the network. A secondary time server transmits the time information to other hosts on a LAN through NTP.
- **Stratum** is a hierarchical standard for clock synchronization. It represents precision of a clock. The value of a stratum ranges from 1 to 16. A smaller value indicates higher precision. The value 1 indicates the highest clock precision, and 16 indicates that the clock is not synchronized.

Figure 9-15 NTP network architecture



Under normal circumstances, the primary time server and the secondary time servers in a synchronization subnet are arranged in a hierarchical-master-slave structure. In this structure, the primary time server is located at the root, and the secondary time servers are arranged close to leaf nodes. As their strata increase, the precision decreases accordingly. The extent to which the precision of the secondary time servers decreases depends on stability of network paths and the local clock.

NOTE

When the synchronization subnet has multiple primary time servers, the optimal server can be selected using an algorithm.

Such a design ensures that:

- When faults occur in one or more primary/secondary time servers or network paths interconnecting them, the synchronization subnet will automatically be reconstructed into another hierarchical-master-slave structure to obtain the most precise and reliable time.
- When all primary time servers in the synchronization subnet become invalid, a standby primary time server runs.

When all primary time servers in the synchronization subnet become invalid, other secondary time servers are synchronized among themselves. These secondary time servers become

independent of the synchronization subnet and automatically run at the last determined time and frequency.

9.5.2.3 Operating Mode

A device may use multiple NTP operating modes to perform time synchronization.

- **Unicast Server/Client Mode**
- **Peer Mode**
- **Broadcast Mode**
- **Multicast Mode**

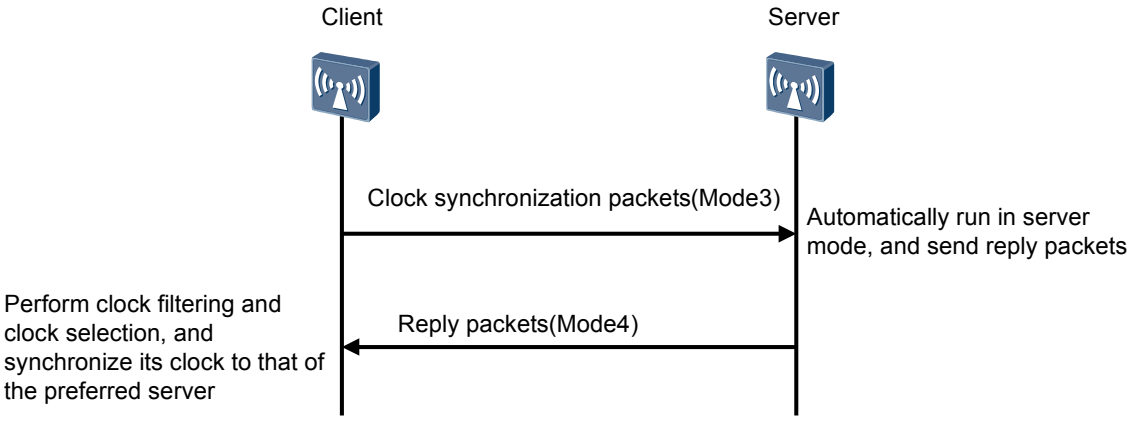
You can select an appropriate operating mode as required.

Unicast Server/Client Mode

The unicast server/client mode runs on a higher stratum on a synchronous subnet. In this mode, devices need to obtain the IP address of the server in advance.

- Client: A host running in client mode (client for short) periodically sends packets to the server. The Mode field in the packets is set to 3, indicating that the packets are coming from a client. After receiving a reply packet, the client filters and selects clock signals, and synchronizes its clock with the server that provides the optimal clock. A client does not check the reachability and stratum of the server. Usually, a host running in this mode is a workstation on a network. It synchronizes its clock with the clock of a server but does not change the clock of the server.
- Server: A host running in server mode (server for short) receives the packets from clients and responds to the packets received. The Mode field in reply packets is set to 4, indicating that the packets are coming from a server. Usually, the host running in server mode is a clock server on a network. It provides synchronization information for clients but does not change its own clock.

Figure 9-16 Unicast Client/Server Mode



During and after the restart, the host operating in client mode periodically sends NTP request messages to the host operating in server mode. After receiving the NTP request message, the server swaps the position of destination IP address and source IP address, and the source port

number and destination port number, fills in the necessary information, and sends the message to the client. The server does not need to retain state information when the client sends the request message. The client freely adjusts the interval for sending NTP request messages according to the local conditions.

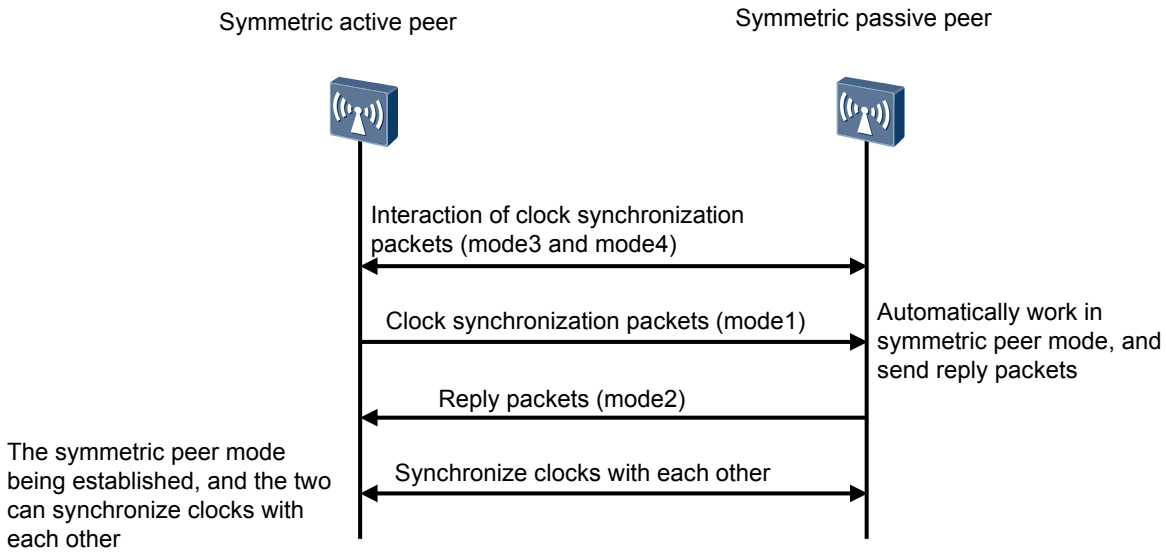
Peer Mode

The peer mode runs on a lower stratum on a synchronous subnet. In this mode, a active peer and a passive peer can synchronize with each other. The peer with a higher stratum (a lower level) synchronizes with a peer with a lower stratum (a higher level).

In peer mode, the active peer initiates an NTP packet with the Mode field set to 3 (the client mode), and the passive peer responds with an NTP packet with the Mode field set to 4 (the server mode). This interaction creates a network delay so that devices at both ends enter the peer mode.

- Active peer: A host that functions as a active peer sends packets periodically. The value of the Mode field in a packet is set to 1. This indicates that the packet is sent by a active peer, without considering whether its peer is reachable and which stratum its peer is on. The active peer can provide time information about the local clock for its peer, or synchronize the time information about the local clock based on that of the peer clock.
- Passive peer: A host that functions as a passive peer receives packets from the active peer and sends reply packets. The value of the Mode field in a reply packet is set to 2. This indicates that the packer is sent by a passive peer. The passive peer can provide time information about the local clock for its peer, or synchronize the time information about the local clock based on that of the peer clock.

Figure 9-17 Peer mode



NOTE

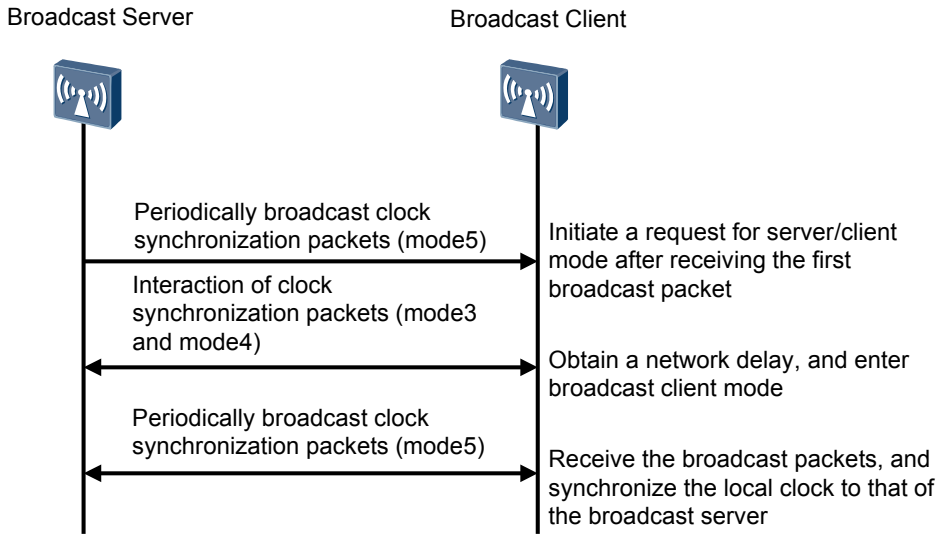
The passive peer does not need to be configured. A host sets up a connection and sets relevant state variables only when it receives an NTP packet.

Broadcast Mode

The broadcast mode is applied to the high speed network that has multiple workstations and does not require high accuracy. In a typical scenario, one or more clock servers on the network periodically send broadcast packets to the workstations. The delay of packet transmission in a LAN is at the milliseconds level.

- Broadcast server: A host that runs in broadcast mode sends clock synchronization packets to the broadcast address 255.255.255.255 periodically. The value of the Mode field in a packet is set to 5. This indicates that the packet is sent by a host that runs in broadcast mode, without considering whether its peer is reachable and which stratum its peer is on. The host running in broadcast mode is usually a clock server running high-speed broadcast media on the network, which provides synchronization information for all of its peers but does not alter the clock of its own.
- Broadcast client: The client listens to the clock synchronization packets sent from the server. When the client receives the first clock synchronization packet, the client and server exchange NTP packets whose values of Mode fields are 3 (sent by the client) and the NTP packets whose values of Mode fields are 4 (sent by the server). In this process, the client enables the server/client mode for a short time to exchange information with the remote server. This allows the client to obtain the network delay between the client and the server. Then, the client returns the broadcast mode, and continues to sense the incoming clock synchronization packets to synchronize the local clock.

Figure 9-18 Broadcast mode



Multicast Mode

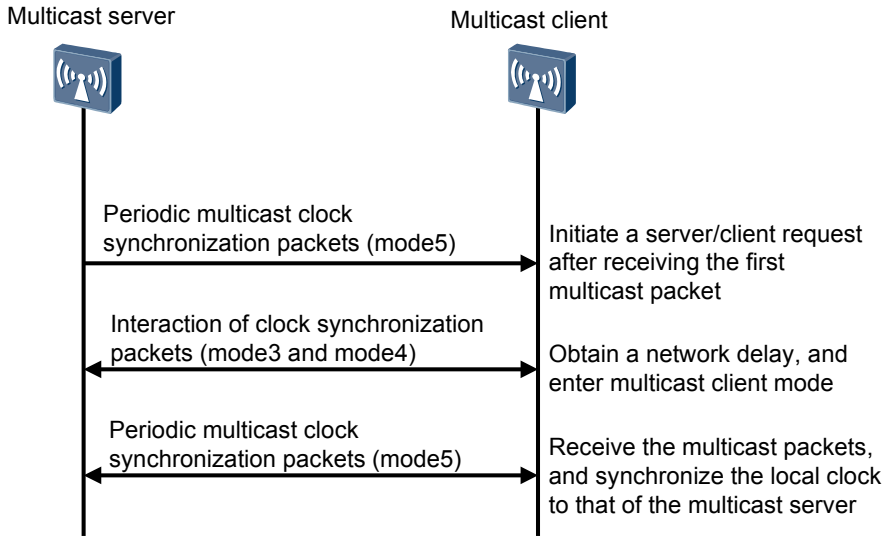
Multicast mode is useful when there are large numbers of clients distributed in a network. This normally results in large number of NTP packets in the network. In the multicast mode, a single NTP multicast packet can potentially reach all the clients on the network and reduce the control traffic on the network.

- Multicast server: A server running in multicast mode sends clock synchronization packets to a multicast address periodically. The value of the Mode field in a packet is set to 5. This

indicates that the packet is sent by a host that runs in multicast mode. The host running in multicast mode is usually a clock server running high-speed broadcast media on the network, which provides synchronization information for all of its peers but does not alter the clock of its own.

- Multicast client: The client listens to the multicast packets from the server. When the client receives the first broadcast packet, the client and server exchange NTP packets whose values of Mode fields are 3 (sent by the client) and the NTP packets whose values of Mode fields are 4 (sent by the server). In this process, the client enables the server/client mode for a short time to exchange information with the remote server. This allows the client to obtain the network delay between the client and the server. Then, the client returns the multicast mode, and continues to sense the incoming multicast packets to synchronize the local clock.

Figure 9-19 Multicast mode



9.5.2.4 NTP Access Control

When a time server on a synchronization subnet is faulty or encounters a malicious attack, timekeeping on other clock servers on the subnet should not be affected. To meet this requirement, NTP provides the following security mechanisms to ensure network security: access authority and NTP authentication.

Access Authority

A device provides access authority, which is simpler and more secure, to protect a local clock.

NTP access control is implemented based on an access control list (ACL). NTP supports four levels of access authority, and a corresponding ACL rule can be specified for each level. If an NTP access request hits the ACL rule for a level of access authority, they are successfully matched and the access request enjoys the access authority at this level.

When an NTP access request reaches the local end, the access request is successively matched with the access authority from the maximum one to the minimum one. The first successfully matched access authority takes effect. The matching order is as follows:

1. peer: indicating the maximum access authority. A time request may be made for the local clock and a control query may be performed on the local clock. The local clock can also be synchronized to a remote server.
2. server: indicating that a time request may be made for the local clock and a control query may be performed on the local clock, but the local clock cannot be synchronized with the clock of the remote server.
3. synchronization: indicating that only a time request can be made for the local clock.
4. query: indicating the minimum access authority. Only a control query can be performed on the local clock.

Authentication

The NTP authentication function can be enabled on networks demanding high security. Different keys may be configured in different operating modes.

When a user enables the NTP authentication function in a certain NTP operating mode, the system records the key ID in this operating mode.

- **Sending process**

  The system determines whether authentication is required in this operating mode. If authentication is not required, the system directly sends a packet. If authentication is required, the system encrypts the packet using the key ID and an encryption algorithm and sends it.

- **Receiving process**

  After receiving a packet, the system determines whether the packet needs to be authenticated. If the packet does not need to be authenticated, the system directly performs subsequent processing on the packet. If the packet needs to be authenticated, the system authenticates the packet using the key ID and a decryption algorithm. If the authentication fails, the system directly discards the packet. If the authentication succeeds, the system processes the received packet.

9.5.3 Default Configuration

This section describes the default system configuration and default parameters.

Table 9-18 Default configuration of the device

Parameter	Default Values
NTP function	Enabled
NTP authentication	Disabled
NTP access control	No access control authority is set.

9.5.4 Configuring the NTP

9.5.4.1 Configuring Basic NTP Functions

You can configure basic NTP functions to enable devices on the network to synchronize clocks.

Pre-configuration Tasks

Before the basic NTP functions are configured, complete the following task:

- Configuring the network layer address and routing protocol of an interface to ensure that NTP packets can reach the destination.

Configuration Procedure

Basic NTP configuration contains the configuration of the NTP primary clock and operating mode.

9.5.4.1.1 Configuring NTP Operating Modes

Context

The following NTP operating modes are supported by a device:

Operating Mode	Usage Scenario	Deployment Location and Synchronization Direction
Unicast client/server mode	The unicast client/server mode is used on a higher stratum on a synchronization subnet. In this mode, the IP address of the server needs to be obtained in advance.	You need to configure only the client. The server needs to be configured with only an NTP primary clock. Note that the client can be synchronized to the server but the server cannot be synchronized to the client.
Symmetric peer mode	The symmetric peer mode is used on a lower stratum on the synchronization subnet. In this mode, a symmetric active peer and a symmetric passive peer can be synchronized with each other. To be specific, a symmetric peer of a higher stratum is synchronized to a symmetric peer of a lower stratum.	You need to configure only the symmetric active peer. The symmetric passive peer does not need to be configured with an NTP command. In symmetric peer mode, a symmetric peer of a higher stratum is synchronized to a symmetric peer of a lower stratum.

Operating Mode	Usage Scenario	Deployment Location and Synchronization Direction
Broadcast mode	When the IP address of a server or a symmetric peer is not determined, or when the clocks of a large number of devices need to be synchronized on a network, clock synchronization can be implemented in the broadcast mode.	Relevant commands need to be run on the server and the client. Note that the client can be synchronized to the server but the server cannot be synchronized to the client.

NOTE

If a source address from which NTP packets are sent is specified on the server, the address must be the same as the server IP address configured on the client. Otherwise, the client cannot process the NTP packets sent by the server, resulting in failed clock synchronization.

Procedure

- **Unicast Client/Server Mode**

  NOTE

  In the unicast client/server mode, you need to configure only the client. The server needs to be configured with only an NTP primary clock.

  Only after the clock on the server is synchronized, the server can function as a clock server to which other devices can be synchronized. When the clock stratum of the server is greater than or equal to the clock stratum of the client, the client is not synchronized to the server.

  You can run the **ntp-service unicast-server** command repeatedly to configure multiple servers. The client selects the optimal clock source by selecting a preferred clock.

  Configure the unicast client.

  1. Run:

     ```
     system-view
     ```

     The system view is displayed.

  2. Run:

     ```
     ntp-service unicast-server ip-address [ version number | authentication-keyid key-id | source-interface interface-type interface-number | preference ] *
     ```

     An NTP server is configured.

     The value of *ip-address* is the IP address of the NTP server. It can be the IP address of a host instead of being a broadcast address, a multicast address, or the IP address of a reference clock.

     To specify the parameter **authentication-keyid**, see **9.5.4.4.4 Configuring NTP Authentication**.

- **Symmetric Peer Mode**

NOTE

Only the IP address of the symmetric passive peer needs to be specified on the symmetric active peer by a user, and both symmetric peers use this IP address to exchange NTP packets.

One of the symmetric active peer and the symmetric passive peer must be in the synchronized state. Otherwise, they cannot be synchronized.

You can run the **ntp-service unicast-peer** command repeatedly to configure multiple symmetric passive peers. When a symmetric active peer has multiple symmetric passive peers configured, the synchronization direction follows the principle that a symmetric peer of a larger stratum is synchronized with a symmetric peer of a smaller stratum.

Configure the symmetric active peer.

1. Run:

   ```
   system-view
   ```

   The system view is displayed.

2. Run:

   ```
   ntp-service unicast-peer ip-address [ version number | authentication-keyid key-id | source-interface interface-type interface-number | preference ] *
   ```

   The NTP peer with a specified IP address is configured.

   The value of *ip-address* must be a unicast address, and cannot be a broadcast address, a multicast address or the IP address of the local clock.

   To specify the parameter **authentication-keyid**, see **9.5.4.4.4 Configuring NTP Authentication**.

- **Broadcast Mode**

  NOTE

  The broadcast mode can be used only on a local area network (LAN).

  Only after the clock of the broadcast server is synchronized, the broadcast client can be synchronized with the broadcast server.

  Configure the NTP broadcast server.

  1. Run:

     ```
     system-view
     ```

     The system view is displayed.

  2. Run:

     ```
     interface  interface-type interface-number
     ```

     The interface for sending NTP broadcast packets is specified, and the interface view is displayed.

  3. Run:

     ```
     ntp-service broadcast-server [ version number | authentication-keyid key-id ] *
     ```

     The local access point is configured as the NTP broadcast server.

     To specify the parameter **authentication-keyid**, see **9.5.4.4.4 Configuring NTP Authentication**.

  Configure the NTP broadcast client.

1. Run:
   system-view

   The system view is displayed.
2. Run:
   interface *interface-type interface-number*

   The interface for receiving NTP broadcast packets is specified, and the interface view is displayed.
3. Run:
   ntp-service broadcast-client

   The local access point is configured as the NTP broadcast client.

----End

9.5.4.1.2 Checking the Configuration

Prerequisites

All configurations of basic NTP functions are completed.

Procedure

- Run the **display ntp-service status** command to check the NTP service status.
- Run the **display ntp-service sessions** [**verbose**] command to check the NTP session status.
- Run the **display ntp-service trace** command to check the path of reference clock source from the local device.

----End

9.5.4.2 Configuring the Local Source Interface for Sending and Receiving NTP Packets

You can configure a local source interface for sending and receiving NTP packets to prevent the IP addresses of other interfaces on the device becoming the destination address of a reply packet. This facilitates deployment of traffic control policies.

Prerequisites

All configurations of basic NTP functions have been completed.

NOTE

If the **ntp-service unicast-server** or the **ntp-service unicast-peer** command specifies the source interface of NTP packets, the specified source interface takes effect.

Procedure

Step 1 Run:
system-view

The system view is displayed.

Step 2 Run:

```
ntp-service source-interface interface-type interface-number
```

The local source interface for sending and receiving NTP packets is configured.

By default, the local source interface for sending NTP packets is not specified. The source IP address of an NTP packet is selected according to the route.

In the broadcast mode, the NTP service is performed on the source interface and the **ntp-service source-interface** command does not take effect.

If the specified NTP source interface is in Down state, the source IP address of a sent NTP packet is the primary IP address of the packet's outbound interface.

----End

Checking the Configuration

- Run the **display current-configuration | include ntp** command to check the configuration about the local source interface for sending and receiving NTP packets.

9.5.4.3 Limit on the Number of Local Dynamic Sessions

Excess dynamic sessions limit the number of static sessions. To address this problem, you can limit the number of dynamic sessions on the device.

Prerequisites

All configurations of basic NTP functions have been completed.

Context

In both unicast client/server mode and symmetric peer mode, command lines are used to establish a connection, which is a static session. Dynamic sessions are established in broadcast mode, so that the limit on the number of local dynamic sessions takes effect.

NOTE

The **ntp-service max-dynamic-sessions** command runs without affecting the existing NTP sessions. When the number of local dynamic NTP sessions exceeds the maximum number, a new session cannot be established.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ntp-service max-dynamic-sessions number
```

The number of local dynamic sessions that can be established is configured.

By default, a maximum of 100 NTP dynamic sessions can be established.

----End

Checking the Configuration

- Run the **display current-configuration | include ntp** command to check the number of local dynamic sessions that can be established.

9.5.4.4 Configuring NTP Access Control

On networks requiring high security, you can use NTP security functions to prevent malicious attacks from modifying NTP packets.

Prerequisites

All configurations of basic NTP functions have been completed.

Configuration Order

You can perform the following configuration tasks in any sequence as required.

9.5.4.4.1 Disabling a Specified Interface from Receiving NTP Packets

Context

You can disable the interface connected to external devices from receiving NTP packets in the following scenarios:

- An unreliable clock server exists on the interface. After the NTP functions are enabled, all interfaces can receive NTP packets by default. However, an unreliable clock source makes NTP clock data inaccurate.
- The NTP clock data are modified when the interface is attacked maliciously.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface for receiving NTP packets is specified.

Step 3 Run:

```
ntp-service in-interface disable
```

The interface is disabled from receiving NTP packets.

----End

9.5.4.4.2 Disabling the NTP Service Function

Context

You can disable NTP services to prevent the device from being synchronized with the clock of an external server or a symmetric peer, or when the device does not need to provide a clock reference source for external clients.

NOTE

The existing configuration is not deleted when the NTP service function is disabled.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
undo ntp-service enable
```

The NTP service function on the device is disabled.

By default, the NTP service function is enabled.

----End

9.5.4.4.3 Configuring NTP Access Control Authority

Context

NTP access control is a simple security measure. When an access request reaches the local end, the access request is successively matched with the access authority from the maximum one to the minimum one. The first successfully matched access authority takes effect. The matching order is: peer, server, synchronization, and query.

- **peer**: indicates the maximum access authority. The remote end can perform time requests and control queries for the local NTP service. The local clock can also be synchronized with the clock of the remote server.
- **server**: indicates that the remote end can send a time request and a control query to the local end. The local clock, however, cannot be synchronized with the clock of the remote server.
- **synchronization**: indicates that the remote end can perform only the time request to the local end.
- **query**: indicates the minimum access authority. The remote end can only perform the control query to the local end.

The access control authority is configured on different devices in different NTP operating modes, as described in **Table 9-19**.

Table 9-19 Configuration of the NTP access control authority

NTP Operating Mode	Restricted NTP Request Type	Configured Device
Unicast NTP client/ server mode	The client is restricted from synchronizing to the server.	Client
Unicast NTP client/ server mode	The server is restricted from processing the clock synchronization request sent by the client.	Server
NTP symmetric peer mode	A symmetric passive peer and a symmetric active peer are restricted from synchronizing with each other.	Symmetric active peer
NTP symmetric peer mode	The symmetric passive peer is restricted from processing the clock request sent by the symmetric active peer.	Symmetric passive peer
NTP broadcast mode	The client is restricted from synchronizing to the server.	NTP broadcast client

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure the basic ACL.

Before configuring the access control rights, you must create a basic ACL. For the creation procedure, see "ACL Configuration" in the *Huawei Wireless Access Points Configuration Guide-Security*.

Step 3 Run:

```
ntp-service access { peer | query | server | synchronization } acl-number
```

The access control authority of the NTP service is configured.

By default, no access control authority is set.

NOTE

Check the configuration of the ACL rule before configuring the NTP access control authority in the ACL. When the ACL rule is **permit**, the peer device with the source IP address specified in this rule can access the NTP service on the local device. The access right of the peer device is configured using the **ntp-service access** command. When the ACL rule is **deny**, the peer device with the source IP address specified in this rule cannot access the NTP service on the local device.

----End

9.5.4.4.4 Configuring NTP Authentication

Context

In some networks demanding high security, the authentication function needs to be enabled when you use the NTP protocol. Password authentication of a client and a server ensures that the client only synchronizes with a device that has been authenticated, improving the network security.

When configuring the NTP authentication function, note the following rules:

- The NTP authentication function must be enabled first; otherwise, authentication cannot be implemented.
- The NTP authentication function needs to be configured on both the client and the server. Otherwise, the NTP authentication function does not take effect.
- If the NTP authentication function is enabled, a trusted key is configured on the client.
- Keys configured on the server and the client must be identical.
- The device that wants to synchronize its clock should declare its key as reliable.Otherwise, NTP authentication will fail.

NOTE

In NTP symmetric peer mode, the symmetric active peer functions as a client and the symmetric passive peer functions as a server.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
ntp-service authentication enable
```

The NTP authentication function is enabled.

Step 3 Run:

```
ntp-service authentication-keyid key-id authentication-mode md5 password
```

The NTP authentication key is configured.

Step 4 Run:

```
ntp-service reliable authentication-keyid key-id
```

The reliable key is specified.

----End

Follow-up Procedure

After the configuration of the NTP authentication is completed, apply the NTP authentication key in **Configuring NTP Operating Modes**. That is, specify the parameter **authentication-keyid**.

9.5.4.4.5 Checking the Configuration

Prerequisites

The configuration of NTP access control is completed.

Procedure

- Run the **display current-configuration | include ntp** command to check the NTP configuration.
- Run the **display ntp-service status** command to check the NTP service status.
- Run the **display ntp-service sessions** [**verbose**] command to check the NTP session status.

----End

9.5.5 Maintaining NTP

In the maintenance of NTP, the running status of NTP is monitored.

9.5.5.1 Monitoring the Running Status of NTP

Context

To monitor the NTP running status after configurations of NTP are complete, run the following commands in any view.

Procedure

- Run:
  ```
  display ntp-service status
  ```
  Check the status information of NTP.
- Run:
  ```
  display ntp-service sessions [ verbose ]
  ```
  All session information maintained by the local NTP service is checked.
- Run:
  ```
  display ntp-service trace
  ```
  The path from the local device to the reference clock source is checked.

----End

9.5.6 Reference

This section lists references of NTP.

The following table provides reference standards and protocols for NTP.

Document No.	Description
RFC 1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
RFC 5905	Network Time Protocol Version 4: Protocol and Algorithms Specification
RFC 5906	Network Time Protocol Version 4: Autokey Specification

10 Configuration Guide - Network Management and Monitoring

About This Chapter

This document describes procedures and provides examples for configuring the Device Management features of the device.

10.1 SNMP Configuration
SNMP is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. There are three SNMP versions, SNMPv1, SNMPv2c, and SNMPv3. You can choose to configure one or more versions if needed.

10.2 RMON Configuration
Remote Network Monitoring (RMON), defined by IETF, is a widely used network management protocol. It provides packet statistics and alarm functions for Ethernet interfaces. The management devices use RMON to remotely monitor and manage network elements. RMON2 is an enhancement of RMON. Currently, the device can collect and analyze statistics on IP packets.

10.3 Mirroring Configuration
Packet mirroring copies packets to a specified destination so that you can analyze packets to monitor the network and rectify faults.

10.4 LLDP Configuration
The Link Layer Discovery Protocol (LLDP) allows you to obtain details about the network topology, changes in the topology, and detect incorrect configurations on the network.

10.5 Packet Capture Configuration
This section describes the concept and configuration of the packet capture function.

10.6 Service Diagnosis Configuration
The service diagnosis function monitors user status changes and protocol processing during user access and exports the monitored information to a terminal or server. Maintenance personnel can refer to and analyze the monitored information to locate user access faults.

10.1 SNMP Configuration

SNMP is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. There are three SNMP versions, SNMPv1, SNMPv2c, and SNMPv3. You can choose to configure one or more versions if needed.

10.1.1 SNMP Overview

This section describes the definition, purpose, version evolution and benefits of SNMP.

Definition

The Simple Network Management Protocol (SNMP) is a network management protocol widely used in the TCP/IP network. SNMP is a method of managing network elements through a network console workstation which runs network management software. SNMP has the following features:

- Simplicity: SNMP applies to small-scale networks requiring high speed and low costs because it uses a polling mechanism and provides basic functions. SNMP uses UDP packets, and is therefore supported by most devices.
- Powerfulness: SNMP ensures the transmission of management information between any two devices on the network, thereby allowing the network administrator to query information, locate faults on any device.

Purpose

As networks rapidly develop and applications become more diversified, network management becomes difficult due to the following factors:

- The number of network devices is dramatically increasing, which increases the network administrator's workload. In addition, networks' coverage areas are constantly being expanded, making real-time monitoring and fault location of network devices difficult.
- Various devices exist on the network, and management interfaces provided by different vendors differ from each other. This makes the network management complex.

To address this problem, SNMP was developed. SNMP supports efficient batch management on network devices and filters differences between products. SNMP allows unified management regardless of the device type and vendor.

Version Evolution

In May 1990, RFC 1157 was developed to define the first SNMP version: SNMPv1. RFC 1157 provides a systematic method for monitoring and managing the network. SNMPv1 cannot ensure the security of the network because it is based on community-name authentication, and only a few error codes are returned.

Later, Internet Engineering Task Force (IETF) released SNMPv2c. SNMPv2c introduced GetBulk and Inform and supported more standard error codes and data types (including the Counter64 and Counter32)

Because SNMPv2c did not provide a high level of security, the IETF released SNMPv3. SNMPv3 provides user security module-based (USM-based) encrypted authentication and view-based access control model (VACM).

Benefits

- Improves the work efficiency of the network administrator. The network administrator can use SNMP to query information, modify information, and locate faults on any device.
- Reduces management costs. SNMP provides basic functions for managing devices with different management tasks, physical attributes, and network types.
- Reduces the impact of feature operations on the device. SNMP is simple in terms of hardware/software installation, packet type, and packet format.

10.1.2 Principles

This section describes the implementation of SNMP.

10.1.2.1 SNMP Management Model

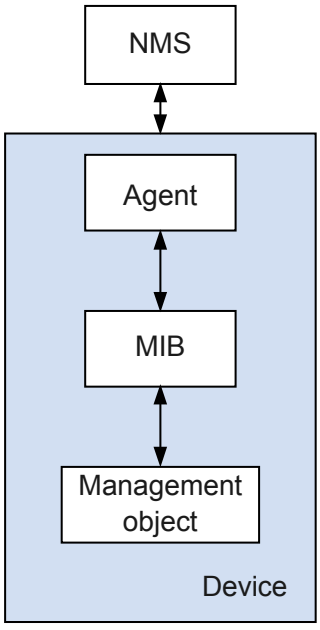
The SNMP system is composed of the NMS, agent, management object, and MIB.

The NMS is the network management center of the network and manages devices on the network.

Each managed device has the agent process, MIB, and multiple managed objects. The NMS interacts with the agent on the managed device. The agent performs operations on the MIB to perform the NMS request.

Figure 10-1 shows an SNMP management model.

Figure 10-1 SNMP management model



Elements in the network management system are as follows:

- **NMS**

  A manager on the network, or a system using SNMP to manage and monitor network devices. The NMS runs on NMS servers.

  - An NMS can send requests to an agent on a device to query or modify the value of one or multiple parameters.
  - An NMS can receive traps sent from the agent on a device to learn the current status of the device.

- **Agent**

  Agent is a process on the managed device. The agent maintains data on the managed device, receives and processes the request packets from the NMS, and then sends the response packets to the NMS.

  - Upon receiving requests of the NMS, the agent performs the required operation over the MIB and sends the operation result to the NMS.
  - When a fault or an event occurs on the device, the agent running on the device sends notifications to the NMS, reporting the current status of the device.

- **Management object**

  Object to be managed. A device may have multiple management objects, including a hardware component (such as an interface board) and parameters (such as a route selection protocol) configured for the hardware or software.

- **MIB**

  MIB is a database specifying variables that are maintained by the managed device and can be queried or set by the agent. MIB defines attributes of the managed device, including the name, status, access rights, and data type of objects.

  An agent can use the MIB to:

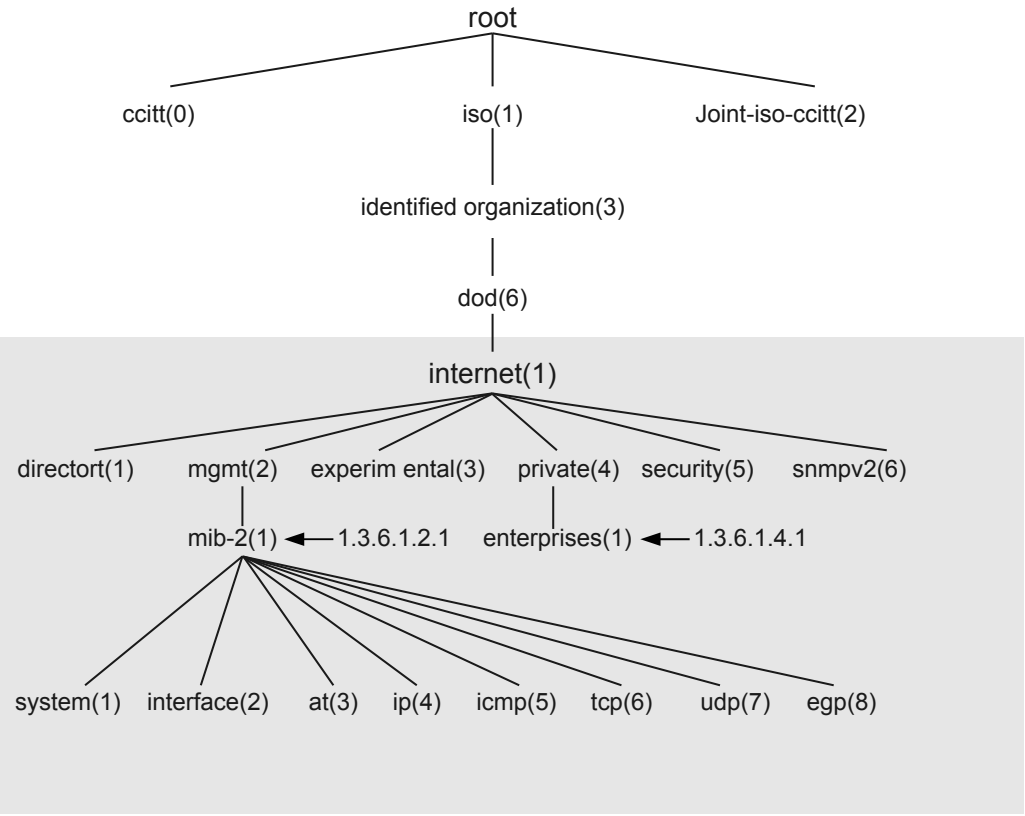
  - Learn the current status of the device.
  - Set the status parameter of the device.

  The SNMP MIB adopts a tree structure like the Domain Name System (DNS) with its root on the top without a name. **Figure 10-2** shows a part of the MIB, called object naming tree. Each object identifier (OID) maps a managed object, for example, the system OID is 1.3.6.1.2.1.1, and the interface OID is 1.3.6.1.2.1.2.

  The OID tree facilitates information management and improves management efficiency. With the OID tree, the network administrator can query information in batches.

  When configuring the agent, the user can configure the MIB object access control for the NMS based on the MIB view. A MIB view is a subset of a MIB.

Figure 10-2 OID tree

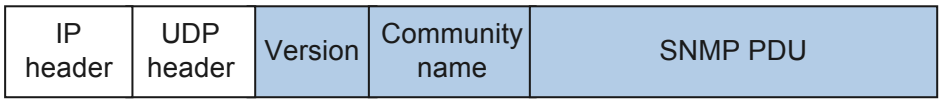


10.1.2.2 SNMPv1/SNMPv2c

SNMPv1/SNMPv2c Packet Format

As shown in **Figure 10-3**, an SNMPv1/SNMPv2c packet is composed of the version, community name, and SNMP Protocol Date Unit (PDU) fields.

Figure 10-3 SNMPv1/SNMPv2c packet format



The fields in an SNMPv1/SNMPv2c packet are defined as follows:

- Version: SNMP version. The SNMPv1 packet field is 0, and the SNMPv2c packet field is 1.
- Community name: used for authenticating operations between the agent and NMS. The community name is a string of characters and can be defined by users. The community name can be a read-only or write-only community name. To authenticate the GetRequest

or GetNextRequest operations, use the read-only community name; to authenticate the Set operation, use the write-only community name.

- SNMPv1/SNMPv2c PDU: includes the PDU type, request ID, and binding variable list. The SNMPv1 PDU includes GetRequest PDU, GetNextRequest PDU, SetRequest PDU, Response PDU, and Trap PDU. The SNMPv2c PDU inherits the SNMPv1 PDU and introduces the GetBulkRequest PDU.

  For simplification, the SNMP operations are described as the Get, GetNext, Set, Response, Trap, and GetBulk operations.

SNMPv1/SNMPv2c Operations

As shown in **Table 10-1**, SNMPv1/SNMPv2c defines six types of operations for exchanging information between the NMS and the agent.

Table 10-1 SNMPv1/SNMPv2c Operations

Operation	Description
Get	The management process reads one or several parameter values from the MIB of the agent process.
GetNext	The management process reads the next parameter value from the MIB of the agent process.
Set	The management process sets the parameter value of one or more MIBs of the agent process.
Response	The agent process returns one or more queried values. The agent performs this operation that corresponds to the GetRequest, GetNextRequest, SetRequest, and GetBulkRequest operations. Upon receiving a Get or Set request, the agent performs the Query or Modify operation using MIB tables and then sends the responses to the NMS.
Trap	The agent process notifies the NMS of a fault or event on the managed device.
GetBulk	The NMS queries managed devices in batches.

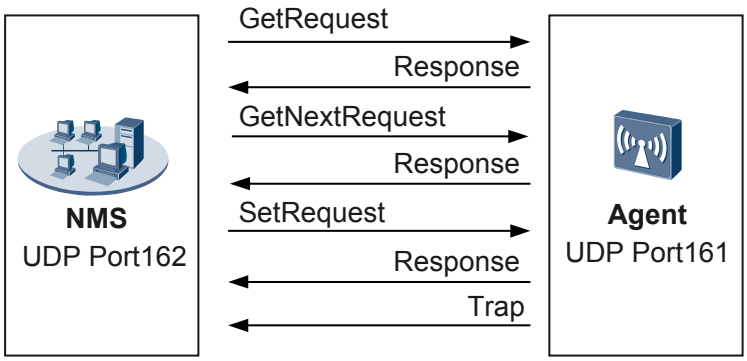
NOTE

SNMPv1 does not support the GetBulk operation.

Working Mechanisms of SNMPv1/SNMPv2c

The working mechanisms of SNMPv1 and SNMPv2c are similar, as shown in **Figure 10-4**.

Figure 10-4 Basic operations



- Get

  The following assumes that the NMS wants to use the read-only community name **public** to obtain the value of the object sysContact on the managed devices. The procedure is as follows:

  1. NMS: sends a GetRequest packet to the agent. The fields of the packet are set as follows: The version is the SNMP version in use; the community name is **public**; the PDU type is Get; the MIB object is sysContact.
  2. Agent: authenticates the version and community name of the packet. When authentication succeeds, the agent encapsulates the queried sysContact value into the PDU of the response packet. Then the agent sends the response packet to the NMS. If the agent fails to obtain the sysContact value, the agent will send an incorrect response packet to the NMS.

- GetNext

  The following assumes that the NMS wants to use the community name **public** to obtain the value of the object sysName (object next to sysContact) on the managed device. The procedure is as follows:

  1. NMS: sends a GetNext request packet to the agent. The fields of the packet are set as follows: The version is the SNMP version in use; the community name is **public**; the PDU type is GetNext; the MIB object is sysContact.
  2. Agent: authenticates the version and community name of the packet. When authentication succeeds, the agent encapsulates the queried sysName value into the PDU of the response packet. Then the agent sends the response packet to the NMS. If the agent fails to obtain the sysName value, the agent will send an incorrect response packet to the NMS.

- Set

  The following assumes that the NMS wants to use the read-only community name **private** to set the value of the object sysName on the managed device to **HUAWEI**. The procedure is as follows:

  1. NMS: sends a SetRequest packet to the agent. The fields of the packet are set as follows: The version is the SNMP version in use; the community name is **private**; the PDU type is Set; the MIB object is sysContact; the target value is **HUAWEI**.
  2. Agent: authenticates the version and community name of the packet. When authentication succeeds, the agent sets an object mapping the requested management

variable. If the setting succeeds, the agent sends a response packet to the NMS. If the setting fails, the agent will send an incorrect response packet to the NMS.

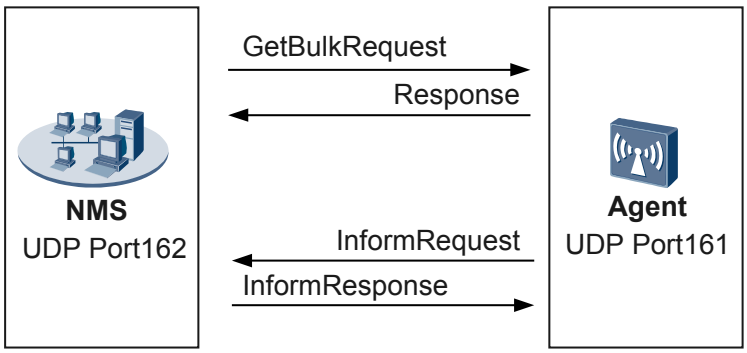
- Trap

  Trap is a spontaneous behavior of a managed device. Traps do not belong to the basic operations performed by the NMS on the managed device. If a managed device meets the triggering condition for generating a trap, the agent notifies the NMS of the exception by sending a trap. For example, when a managed device is started in hot startup mode, the agent sends a warmStart trap to the NMS.

  The agent sends the trap to the management process only when a module on the device meets the triggering condition for generating a trap. This method reduces exchange traffic by sending traps only when major events occur.

Figure 10-5 shows the operations that are added in SNMPv2c.

Figure 10-5 New operations in SNMPv2c



- GetBulk

  The GetBulk operation is equal to consecutively performed GetNext operations. You can set the number of times that the GetNext operations are performed during one GetBulk operation.

- Inform

  A managed device notifies the NMS of an inform. After the managed device sends an inform, the NMS must send an InformResponse packet to the managed device. If the managed device does not receive the response packet, the managed device performs the following operations:

  1. Save the alarm in the inform buffer.
  2. Repeatedly send the alarm until the NMS returns the response packet or the number of times that the managed device sends alarms exceeds the allowed range.
  3. An alarm log is generated on the managed device.

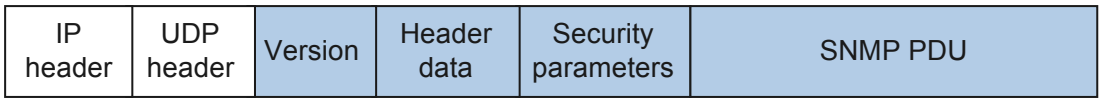
  Therefore, the informs may occupy many system resources.

10.1.2.3 SNMPv3

SNMPv3 Packet Format

SNMPv3 defines a new packet format shown in **Figure 10-6**.

Figure 10-6 SNMPv3 packet format



The following describes the composition of an SNMPv3 packet:

- Version: SNMP version. The SNMPv3 packet field is 2.
- Header: information such as the maximum message size supported by the transmitter, and security mode of messages.
- Security parameters: security information including the entity engine information, user name, authentication parameter, and encryption information.
- Context EgineID: SNMP ID. Together with the PDU type, it determines which application messages are to be sent.
- Context Name: determines the Context EgineID MIB view of the managed device.
- SNMPv3 PDU: includes the PDU type, request ID, and binding variable list. The SNMPv3 PDU includes GetRequest PDU, GetNextRequest PDU, SetRequest PDU, Response PDU, Trap PDU, and GetBulkRequest PDU.

SNMPv3 Architecture

SNMPv3 uses the SNMPv3 entity for the communication between different SNMP-enabled NMSs. An SNMPv3 entity consists of SNMPv3 engines and applications, and each SNMPv3 engine or application has multiple modules.

The modular architecture of the SNMP entity has the following advantages:

- Strong adaptability: This architecture is adaptable for both simple and complex networks.
- Easy management: This architecture consists of multiple independent sub-systems and applications. When a fault occurs in the system. it is easy to locate the sub-system to which the fault belongs based on the fault type.
- Excellent expandability: An SNMP system can be extended by increasing the number of modules on the SNMP entity. For example, a module can be added in the security sub-system for the application of a new security protocol.

SNMPv3 improves security by adopting the user security model (USM) and view-based access control model (VACM).

- USM: authenticates user identity and encrypts data. These two functions require that the NMS and the agent use a shared key.
  - Identify authentication: a process in which the agent (or the NMS) confirms whether the received message is from an authorized NMS (or agent) and whether the message is changed during transmission. RFC 2104 defines Keyed-Hashing for Message Authentication Code (HMAC), an effective tool that uses the security hash function and key to generate the message authentication code. This tool is widely used in the Internet. HMAC used in SNMP contains HWAC-MD5-96 and HWAC-SHA-96. The hash function of HWAC-MD5-96 is MD5 that uses 128-bit authKey to generate the key. The hash function of HWAC-SHA-96 is SHA-1 that uses 160-bit authKey to generate the key.

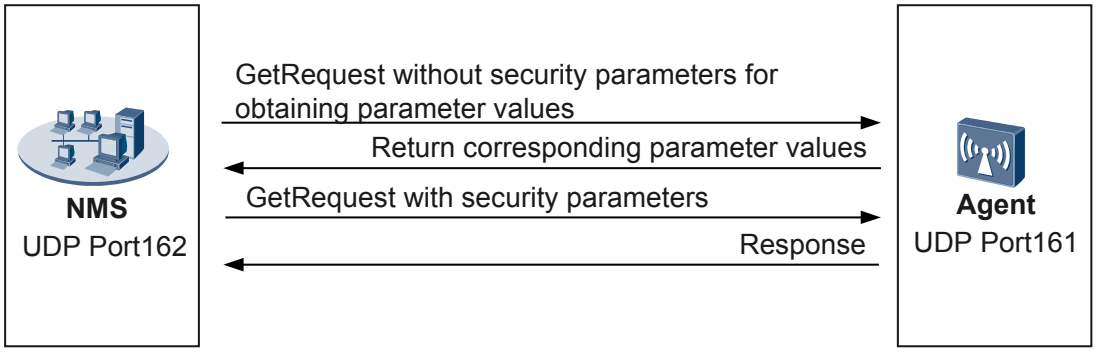
  - Like identity authentication, data encryption also requires the network management station and the agent to use a shared key for encryption or decryption. ESP encrypts the IP packet contents to prevent them from being intercepted during transmission. Encryption algorithms are implemented by using a symmetric key system, which uses the same key to encrypt and decrypt data. SNMP uses the following encryption algorithms:
    - Data Encryption Standard (DES): encrypts a 64-bit plain text by using a 56-bit key.
    - Advanced Encryption Standard (AES): encrypts a plain text by using a key of 128 bits, 192 bits, or 256 bits.
- VACM: controls access of user groups or community names based on the view. You must pre-configure a view and specify its authority. Then, when you configure a user, user group, or community, load this view to implement read/write restriction or trap function.

SNMPv3 Mechanism

The mechanism of SNMPv3 is similar to those of SNMPv1 and SNMPv2c, but SNMPv3 supports identity authentication and encryption. The following describes the SNMPv3 mechanism by using the Get operation as an example.

The following assumes that the NMS wants to obtain the value of the object sysContact on the managed device in authentication and encryption mode, as shown in **Figure 10-7**.

Figure 10-7 Get operation of SNMPv3



1. NMS: sends a GetRequest packet without security parameters to the agent and requests the values of Context EgineID, Context Name, and security parameter.
2. Agent: responds to the request from the NMS by providing the requested parameters.
3. NMS: sends a GetRequest packet to the agent. The packet fields are set as follows:
   - Version: SNMPv3.
   - Header: specifies authentication and encryption.
   - Security parameters: The NMS calculates the authentication and encryption parameters using the configured algorithm. These parameters and security parameters are filled in the corresponding fields.
   - PDU: Set corresponding fields using obtained Context EgineID and Context Name. The PDU type is set to Get, the MIB object is sysContact, and the configured encryption algorithm is used to encrypt the PDU.

4. Agent: authenticates the messages. When authentication succeeds, the agent decrypts the PDU. When encryption succeeds, the agent obtains the value of sysContact and encapsulates it to the PDU in the response packet. The agent encrypts the PDU and sends the response packet to the NMS. If the query, authentication, or encryption fails, the agent will send an incorrect response packet to the NMS.

10.1.3 Configuration Task Summary

This section compares SNMP versions in terms of their support for features and usage scenarios to provide a reference for your SNMP version selection during network deployment.

The device supports SNMPv1, SNMPv2c, and SNMPv3. **Table 10-2** lists the features supported by SNMP, and **Table 10-3** shows the support of different SNMP versions for the features. **Table 10-4** describes the usage scenarios of SNMP versions, which helps you choose a proper version for the communication between an NMS and managed devices based on the network operation conditions.

NOTE

When multiple NMSs using different SNMP versions manage the same device in a network SNMPv1, SNMPv2c, and SNMPv3 are configured on the device for its communication with all the NMSs.

Table 10-2 Description of features supported by SNMP

Feature	Description
Access control	This function is used to restrict a user's device administration rights. It gives specific users the rights to manage specified objects on devices and therefore provides fine management.
Authentication and privacy	The authentication and privacy packets are transmitted between the NMS and managed devices. This prevents data packets from being intercepted or modified, improving data sending security.
Error code	Error codes help the administrator to identify and rectify faults. It is easy for the administrator to manage the device if the error codes are more with variety.
Trap	Traps are sent from managed devices to the NMS. Traps help administrator to know device faults. The managed devices do not require the acknowledgement from the NMS after sending traps.
GetBulk	GetBulk allows an administrator to perform Get-Next operations in batches. In a large network, GetBulk reduces the workload of administrator and improves management efficiency.

Table 10-3 Different SNMP versions support for the features

Feature	SNMPv1	SNMPv2c	SNMPv3
Access control	Access control based on the community name and MIB view	Access control based on the community name and MIB view	Access control based on the user, user group, and MIB view
Authentication and privacy	Authentication based on the community name	Authentication based on the community name	Supported authentication and privacy modes are as follows: Authentication mode: ● MD5 ● SHA Encryption mode: ● DES56 ● AES128
Error code	6 error codes supported	16 error codes supported	16 error codes supported
Trap	Supported	Supported	Supported
GetBulk	Not supported	Supported	Supported

Table 10-4 Usage scenarios of different SNMP versions

Version	Usage Scenario
SNMPv1	This version is applicable to small-scale networks whose networking is simple and security requirements are low or whose security and stability are good, such as campus networks and small enterprise networks.
SNMPv2c	This version is applicable to medium and large-scale networks whose security requirements are not strict or whose security is good but whose services are so busy that traffic congestion may occur.
SNMPv3	This version is applicable to networks of various scales, especially the networks that have strict requirements on security and can be managed only by authorized administrators. For example, data between the NMS and managed device needs to be transmitted over a public network.

If you plan to build a network, choose an SNMP version based on your usage scenario. If you plan to expand or upgrade an existing network, choose an SNMP version to match the SNMP

version running on the NMS to ensure the communication between managed devices and the NMS.

10.1.4 Default Configuration

This topic describes the default settings of common parameters.

Table 10-5 lists the default settings of SNMP parameters.

Table 10-5 Default settings of SNMP parameters

Parameter	Default Value
SNMP agent	The SNMP agent function is disabled.
SNMP trap receive host	No host is configured to receive traps.
SNMP version	SNMPv1, SNMPv2c, and SNMPv3.
SNMPv3 authentication mode and encryption mode	No authentication and no encryption.

10.1.5 Configuring the SNMP

10.1.5.1 Configuring a Device to Communicate with an NMS by Running SNMPv1

After SNMPv1 is configured, a managed device and an NMS can run SNMPv1 to communicate with each other. To ensure communication, you need to configure the agent and NMS. This section describes the configuration on a managed device (the agent side). For details about configuration on an NMS, see the pertaining NMS operation guide.

Pre-configuration Tasks

Before configuring a device to communicate with an NMS by running SNMPv1, configure a routing protocol to ensure that at least one route exist between access point and NMS.

Procedure

When you configure the device to communicate with the NMS using SNMPv1, **Configuring Basic SNMPv1 Functions** is mandatory and optional steps can be performed in any sequence.

After the SNMP basic functions are configured, the NMS can communicate with managed devices.

- The access permission of the NMS that uses the configured community name is Viewdefault view. The internet MIB (OID: 1.3.6.1) can be operated in this view.
- The managed device sends traps generated by the modules that are enabled by default to the NMS.

If finer device management is required, follow directions below to configure a managed device:

- To allow a specified NMS that uses the community name to manage specified objects on the device, follow the procedure described in **Restricting Management Rights of the NMS**.
- To allow a specified module on the managed device to report traps to the NMS, follow the procedure described in **Configuring the Trap Function**.
- If the NMS and managed device are both Huawei products, follow the procedure described in **Enabling the SNMP Extended Error Code Function** to allow the device to send more types of error codes. This allows more specific error identification and facilitates your fault location and rectification.

10.1.5.1.1 Configuring Basic SNMPv1 Functions

Context

For the configuration of basic SNMP functions, **Step 1**, **Step 3**, **Step 4**, **Step 5** and **Step 6** are mandatory steps. After the configuration is complete, basic SNMP communication can be established between the NMS and managed device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 (Optional) Run:

```
snmp-agent
```

The SNMP agent function is enabled.

By default, the SNMP agent function is disabled. Executing the **snmp-agent** command can enable the SNMP agent function no matter whether parameters are specified in the command.

Step 3 Run:

```
snmp-agent sys-info version v1
```

The SNMP version is set to SNMPv1.

By default, SNMPv1, SNMPv2c and SNMPv3 are enabled.

Step 4 Run:

```
snmp-agent community { read | write } { community-name | cipher community-name }
```

The community name is set.

By default, the complexity check is enabled for a community name. If a community name fails the complexity check, the community name cannot be configured. To disable the complexity check for a community name, run the **snmp-agent community complexity-check disable** command.

NOTE

The AP has the following requirements for community name complexity:

- The default minimum length of a community name is six characters.
- A community name includes at least two kinds of characters, which can be uppercase letters, lowercase letters, digits, and special characters except question marks (?) and spaces.

After the read-and-write community name is set, the NMS with this name has the right of the Viewdefault view (OID: 1.3.6.1). To change the access right of the NMS, see **Restricting Management Rights of the NMS**.

NOTE

Ensure that the community name of the NMS is the same as that set on the agent. If the NMS and the agent have different community names, the NMS cannot access the agent.

Step 5 Run:

```
snmp-agent target-host trap-paramsname paramsname v1 securityname securityname
[ binding-private-value ] [ private-netmanager ]
```

Parameters for sending trap messages are set.

Step 6 Run:

```
snmp-agent target-host trap-hostname hostname address { ipv4-addr [ udp-port udp-
portid ] [ public-net ] } trap-paramsname paramsname
```

The destination host for receiving trap messages and error codes is specified.

Note the following when running the command:

- The default destination UDP port number is 162. To ensure secure communication between the NMS and managed devices, run the **udp-port** command to change the UDP port number to a non-well-known port number.
- If trap messages sent from the managed device to the NMS need to be transmitted over a public network, the parameter **public-net** needs to be configured.

Step 7 (Optional) Run:

```
snmp-agent sys-info { contact contact | location location }
```

The equipment administrators contact information or location is configured.

By default, the vendor's contact information is "R&D Shenzhen, Huawei Technologies co.,Ltd.". The default location is "Shenzhen China".

This step is required for the NMS administrator to view contact information and locations of the equipment administrator when the NMS manages many devices. This helps the NMS administrator to contact the equipment administrators for fault location and rectification.

To configure both the equipment administrators contact information and location, run the **snmp-agent sys-info** command twice.

----End

10.1.5.1.2 (Optional) Restricting Management Rights of the NMS

Context

When multiple NMSs using the same community name manage one device, perform this configuration based on the site requirements.

Scenario	Steps
All NMSs using this community name have the right of the ViewDefault view.	No action required
Specified NMSs using this community name have the right of the ViewDefault view.	**Step 1**, **Step 3**
All NMSs using this community name manage specified objects on the managed device.	**Step 1**, **Step 2**, **Step 3**
Specified NMSs using this community name manage specified objects on the managed devices.	**Step 1**, **Step 2**, **Step 3**

NOTE

The ViewDefault view is the 1.3.6.1 view.

When an ACL is used to control the NMS access rights, the constraints are as follows:

- When the ACL rule is **permit**, the NMS with the source IP address specified in this rule can access the local device.
- When the ACL rule is **deny**, the NMS with the source IP address specified in this rule cannot access the local device.
- If a packet matches no ACL rule, the NMS that sends the packet cannot access the local device.
- When no ACL rule is configured, all NMSs can access the local device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
snmp-agent mib-view view-name { exclude | include } subtree-name [ mask mask ]
```

A MIB view is created, and manageable MIB objects are specified.

By default, an NMS has right to access the objects in the ViewDefault view.

If both the **included** and **excluded** parameters are configured for MIB objects that have an inclusion relationship, whether to include or exclude the lowest MIB object will be determined by the parameter configured for the lowest MIB object. For example, the snmpV2, snmpModules, and snmpUsmMIB objects are from top down in the MIB table. If the **excluded** parameter is configured for snmpUsmMIB objects and **included** is configured for snmpV2, snmpUsmMIB objects will still be excluded.

Step 3 Configure NMS filtering based on community name.

1. (Optional) Configure the basic ACL.

   Before configuring the access control rights, you must create a basic ACL. For the creation procedure, see "ACL Configuration" in the *Huawei Wireless Access Points Configuration Guide-Security*.

2. Run:

   snmp-agent community { **read** | **write** } { *community-name* | **cipher** *community-name* } [**mib-view** *view-name* | **acl** *acl-number*] *

   The NMS's access right are specified.

   By default, the community name has the right of the ViewDefault view.

   - To grant only the read permission to low-level administrators, specify the parameter **read**. To grant the read and write permissions to high-level administrators, specify the parameter **write**.
   - If the NMSs using this community name have the right of the ViewDefault view, the parameter **mib-view** *view-name* is not required.
   - If all NMSs using this community name manage specified objects on the managed devices, the parameter **acl** *acl-number* is not required.
   - If some NMSs using this community name manage specified objects on the managed devices, the parameters **acl** and **mib-view** must be configured.

   NOTE

   Before specifying the NMS to manage devices with this community name, check the ACL rule. When the ACL rule is **permit**, the NMS with the source IP address specified in this rule can access the local device. When the ACL rule is **deny**, the NMS with the source IP address specified in this rule cannot access the local device.

----End

Follow-up Procedure

After the access right are configured, especially after the IP address of the NMS is specified, if the IP address changes (for example, the NMS changes its location, or IP addresses are reallocated due to network adjustment), you need to change the IP address of the NMS in the ACL. Otherwise, the NMS cannot access the device.

10.1.5.1.3 (Optional) Configuring the Trap Function

Context

Users can enable the trap function for a specified module. The interface status trap is generated when the interface status changes. You need to enable the trap function for the **standard** module globally and enable the interface status trap function on the specified interface.

Procedure

Step 1 Run:

system-view

The system view is displayed.

Step 2 Enable the trap function.

Enable the trap function for a module.

- Run:

  snmp-agent trap enable

  The trap function is enabled for all modules.
- Run:

  snmp-agent trap enable feature-name

  The trap function is enabled for a specified module.

Enable the trap function for an interface.

Run:

snmp-agent trap enable feature-name ifnet trap-name { **linkdown** | **linkup** }

The trap function is enabled on all interfaces.

By default, the trap function is disabled on all interfaces. When parameters **linkdown** and **linkup** are configured for all **ifnet** modules, the device sends a trap to the NMS upon an interface status change. When an interface frequently sends traps to the NMS because of frequent status changes, you can disable the interface status trap function on the interface to reduce the NMS loads. The procedure is as follows:

1. Run:

   interface *interface-type interface-number*

   The interface view is displayed.
2. Run:

   undo enable snmp trap updown

   The interface status trap function is disabled.
3. Run:

   quit

   Return to the system view.

Step 3 Run:

snmp-agent trap source *interface-type interface-number*

The source interface for traps is specified.

After the source interface is specified, the IP address of the source interface is used as the source IP address for sending traps. This helps the NMS identify the trap source. The source interface that sends traps must have an IP address; otherwise, the commands will fail to take effect. To ensure device security, it is recommended that you set the source IP address to the local loopback address.

The source interface specified on the access point for traps must be consistent with that specified on the NMS; otherwise, the NMS does not accept the traps sent from the access point.

Step 4 Run:

snmp-agent trap queue-size *size*

The queue length of traps sent to the destination host is set.

The default queue length of traps sent to the destination host is 100.

The queue length depends on the number of generated traps. If the access point frequently sends traps to the NMS, set a longer queue length to prevent traps from being lost.

Step 5 Run:

```
snmp-agent trap life seconds
```

The lifetime of traps is set.

The default lifetime of traps is 120 seconds.

The lifetime of each trap depends on the number of generated traps. If the access point frequently sends traps to the NMS, set a longer lifetime to prevent traps from being lost.

----End

10.1.5.1.4 (Optional) Enabling the SNMP Extended Error Code Function

Context

This section describes how to enable the extended error code function on the SNMP agent when both the NMS and managed device are Huawei products. After this function is enabled, more types of error codes are provided to help you locate and rectify faults quickly and accurately.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
snmp-agent extend error-code enable
```

The extended error code function is enabled on the SNMP agent.

By default, SNMP sends standard error codes. It can send extended error codes to the NMS only after the extended error code function is enabled.

----End

10.1.5.1.5 Checking the Configuration

Prerequisites

The configurations of basic SNMPv1 functions are complete.

Procedure

- Run the **display snmp-agent community** { **read** | **write** } command to check the configured community name.
- Run the **display snmp-agent sys-info version** command to check the enabled SNMP version.
- Run the **display acl** *acl-number* command to check the ACL rules.
- Run the **display snmp-agent mib-view** command to check the MIB view.

- Run the **display snmp-agent sys-info contact** command to check the equipment administrator's contact information.
- Run the **display snmp-agent sys-info location** command to check the location of the access point.
- Run the **display current-configuration | include trap** command to check the configuration of the trap function.
- Run the **display snmp-agent trap all** command to check current and default status of all traps in all features.
- Run the **display snmp-agent trap-source** command to check the source interface for sending traps.
- Run the **display snmp-agent target-host** command to check information about the target host.
- Run the **display snmp-agent extend error-code status** command to check whether the function that the device sends extended error codes to the NMS is enabled.

----End

10.1.5.2 Configuring a Device to Communicate with an NMS by Running SNMPv2c

After SNMPv2c is configured, a managed device and an NMS can run SNMPv2c to communicate with each other. To ensure communication, you need to configure the agent and NMS. This section describes the configuration on a managed device (the agent side). For details about configuration on an NMS, see the pertaining NMS operation guide.

Pre-configuration Tasks

Before configuring a device to communicate with an NMS by running SNMPv2c, configure a routing protocol to ensure that at least one route exist between access point and NMS.

Procedure

When you configure the device to communicate with the NMS using SNMPv2c, **Configuring Basic SNMPv2c Functions** is mandatory and optional steps can be performed in any sequence.

After the SNMP basic functions are configured, the NMS can communicate with managed devices.

- The access permission of the NMS that uses the configured community name is Viewdefault view. The internet MIB (OID: 1.3.6.1) can be operated in this view.
- The managed device sends traps generated by the modules that are enabled by default to the NMS.

If finer device management is required, follow directions below to configure a managed device:

- To allow a specified NMS that uses the community name to manage specified objects on the device, follow the procedure described in **Restricting Management Rights of the NMS**.
- To allow a specified module on the managed device to report traps to the NMS, follow the procedure described in **Configuring the Trap Function**.
- If the NMS and managed device are both Huawei products, follow the procedure described in **Enabling the SNMP Extended Error Code Function** to allow the device to send more

types of error codes. This allows more specific error identification and facilitates your fault location and rectification.

10.1.5.2.1 Configuring Basic SNMPv2c Functions

Context

For the configuration of basic SNMP functions, **Step 1**, **Step 3**, **Step 4**, **Step 5** and **Step 6** are mandatory steps. After the configurations are complete, the NMS and managed device can communicate with each other.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 (Optional) Run:

```
snmp-agent
```

The SNMP agent function is enabled.

By default, the SNMP agent function is disabled. Executing the **snmp-agent** command can enable the SNMP agent function no matter whether parameters are specified in the command.

Step 3 Run:

```
snmp-agent sys-info version v2c
```

The SNMP version is set to SNMPv2c.

By default, SNMPv1, SNMPv2c, and SNMPv3 are enabled.

Step 4 Run:

```
snmp-agent community { read | write } { community-name | cipher community-name }
```

The community name is configured for the device.

After the read-and-write community name is set, the NMS with this name has the right of the ViewDefault view (OID: 1.3.6.1). To change the access right of the NMS, see **10.1.5.2.2 (Optional) Restricting Management Rights of the NMS**.

NOTE

Ensure that the community name of the NMS is the same as that set on the agent. If the NMS and the agent have different community names, the NMS cannot access the agent.

Step 5 Run:

```
snmp-agent target-host trap-paramsname paramsname v2c securityname securityname
[ binding-private-value ] [ private-netmanager ]
```

Parameters for sending trap messages are set.

Step 6 Run:

```
snmp-agent target-host trap-hostname hostname address { ipv4-addr [ udp-port udp-
portid ] [ public-net ] } trap-paramsname paramsname
```

The destination host for receiving trap messages and error codes is specified.

Note the following when running the command:

- The default destination UDP port number is 162. To ensure secure communication between the NMS and managed devices, run the **udp-port** command to change the UDP port number to a non-well-known port number.
- If trap messages sent from the managed device to the NMS need to be transmitted over a public network, the parameter **public-net** needs to be configured.

Step 7 (Optional) Run:

```
snmp-agent sys-info { contact contact | location location }
```

The equipment administrators contact information or location is configured.

By default, the vendor's contact information is "R&D Shenzhen, Huawei Technologies co.,Ltd.". The default location is "Shenzhen China".

This step is required for the NMS administrator to view contact information and locations of the equipment administrator when the NMS manages many devices. This helps the NMS administrator to contact the equipment administrators for fault location and rectification.

To configure both the equipment administrators contact information and location, run the **snmp-agent sys-info** command twice.

----End

10.1.5.2.2 (Optional) Restricting Management Rights of the NMS

Context

When multiple NMSs using the same community name manage one device, perform this configuration based on the site requirements.

Scenario	Steps
All NMSs using this community name have the right of the ViewDefault view.	No action required
Specified NMSs using this community name have the right of the ViewDefault view.	**Step 1**, **Step 3**
All NMSs using this community name manage specified objects on the managed device.	**Step 1**, **Step 2**, **Step 3**
Specified NMSs using this community name manage specified objects on the managed devices.	**Step 1**, **Step 2**, **Step 3**

NOTE

The ViewDefault view is the 1.3.6.1 view.

When an ACL is used to control the NMS access rights, the constraints are as follows:

- When the ACL rule is **permit**, the NMS with the source IP address specified in this rule can access the local device.
- When the ACL rule is **deny**, the NMS with the source IP address specified in this rule cannot access the local device.
- If a packet matches no ACL rule, the NMS that sends the packet cannot access the local device.
- When no ACL rule is configured, all NMSs can access the local device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
snmp-agent mib-view view-name { exclude | include } subtree-name [ mask mask ]
```

A MIB view is created, and manageable MIB objects are specified.

By default, an NMS has right to access the objects in the ViewDefault view.

If both the **included** and **excluded** parameters are configured for MIB objects that have an inclusion relationship, whether to include or exclude the lowest MIB object will be determined by the parameter configured for the lowest MIB object. For example, the snmpV2, snmpModules, and snmpUsmMIB objects are from top down in the MIB table. If the **excluded** parameter is configured for snmpUsmMIB objects and **included** is configured for snmpV2, snmpUsmMIB objects will still be excluded.

Step 3 Configure NMS filtering based on community name.

1. (Optional) Configure the basic ACL.

   Before configuring the access control rights, you must create a basic ACL. For the creation procedure, see "ACL Configuration" in the *Huawei Wireless Access Points Configuration Guide-Security*.

2. Run:

   ```
   snmp-agent community { read | write } { community-name | cipher community-name } [ mib-view view-name | acl acl-number ] *
   ```

   The NMS's access right are specified.

   By default, the community name has the right of the ViewDefault view.

   - To grant only the read permission to low-level administrators, specify the parameter **read**. To grant the read and write permissions to high-level administrators, specify the parameter **write**.
   - If the NMSs using this community name have the right of the ViewDefault view, the parameter **mib-view** *view-name* is not required.
   - If all NMSs using this community name manage specified objects on the managed devices, the parameter **acl** *acl-number* is not required.
   - If some NMSs using this community name manage specified objects on the managed devices, the parameters **acl** and **mib-view** must be configured.

NOTE

Before specifying the NMS to manage devices with this community name, check the ACL rule. When the ACL rule is **permit**, the NMS with the source IP address specified in this rule can access the local device. When the ACL rule is **deny**, the NMS with the source IP address specified in this rule cannot access the local device.

----End

Follow-up Procedure

After the access right are configured, especially after the IP address of the NMS is specified, if the IP address changes (for example, the NMS changes its location, or IP addresses are reallocated due to network adjustment), you need to change the IP address of the NMS in the ACL. Otherwise, the NMS cannot access the device.

10.1.5.2.3 (Optional) Configuring the Trap Function

Context

Users can enable the trap function for a specified module. The interface status trap is generated when the interface status changes. You need to enable the trap function for the **standard** module globally and enable the interface status trap function on the specified interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Enable the trap function.

Enable the trap function for a module.

- Run:

  ```
  snmp-agent trap enable
  ```

  The trap function is enabled for all modules.

- Run:

  ```
  snmp-agent trap enable feature-name
  ```

  The trap function is enabled for a specified module.

Enable the trap function for an interface.

Run:

```
snmp-agent trap enable feature-name ifnet trap-name { linkdown | linkup }
```

The trap function is enabled on all interfaces.

By default, the trap function is disabled on all interfaces. When parameters **linkdown** and **linkup** are configured for all **ifnet** modules, the device sends a trap to the NMS upon an interface status change. When an interface frequently sends traps to the NMS because of frequent status changes, you can disable the interface status trap function on the interface to reduce the NMS loads. The procedure is as follows:

1. Run:
   interface *interface-type interface-number*
   The interface view is displayed.
2. Run:
   undo enable snmp trap updown
   The interface status trap function is disabled.
3. Run:
   quit
   Return to the system view.

Step 3 Run:
snmp-agent trap source *interface-type interface-number*

The source interface for traps is specified.

After the source interface is specified, the IP address of the source interface is used as the source IP address for sending traps. This helps the NMS identify the trap source. The source interface that sends traps must have an IP address; otherwise, the commands will fail to take effect. To ensure device security, it is recommended that you set the source IP address to the local loopback address.

The source interface specified on the access point for traps must be consistent with that specified on the NMS; otherwise, the NMS does not accept the traps sent from the access point.

Step 4 Run:
snmp-agent trap queue-size *size*

The queue length of traps sent to the destination host is set.

The default queue length of traps sent to the destination host is 100.

The queue length depends on the number of generated traps. If the access point frequently sends traps to the NMS, set a longer queue length to prevent traps from being lost.

Step 5 Run:
snmp-agent trap life *seconds*

The lifetime of traps is set.

The default lifetime of traps is 120 seconds.

The lifetime of each trap depends on the number of generated traps. If the access point frequently sends traps to the NMS, set a longer lifetime to prevent traps from being lost.

----End

10.1.5.2.4 (Optional) Enabling the SNMP Extended Error Code Function

Context

This section describes how to enable the extended error code function on the SNMP agent when both the NMS and managed device are Huawei products. After this function is enabled, more types of error codes are provided to help you locate and rectify faults quickly and accurately.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
snmp-agent extend error-code enable
```

The extended error code function is enabled on the SNMP agent.

By default, SNMP sends standard error codes. It can send extended error codes to the NMS only after the extended error code function is enabled.

----End

10.1.5.2.5 Checking the Configuration

Prerequisites

The configurations of basic SNMPv2c functions are complete.

Procedure

- Run the **display snmp-agent community** { **read** | **write** } command to check the configured community name.
- Run the **display snmp-agent sys-info version** command to check the enabled SNMP version.
- Run the **display acl** *acl-number* command to check the ACL rules.
- Run the **display snmp-agent mib-view** command to check the MIB view.
- Run the **display snmp-agent sys-info contact** command to check the equipment administrator's contact information.
- Run the **display snmp-agent sys-info location** command to check the location of the access point.
- Run the **display current-configuration** | **include trap** command to check trap configuration.
- Run the **display snmp-agent trap all** command to check current and default status of all traps in all features.
- Run the **display snmp-agent trap-source** command to check the source interface for sending traps.
- Run the **display snmp-agent target-host** command to check information about the target host.
- Run the **display snmp-agent extend error-code status** command to check whether the function that the device sends extended error codes to the NMS is enabled.

----End

10.1.5.3 Configuring a Device to Communicate with an NMS by Running SNMPv3

After SNMPv3 is configured, a managed device and an NMS can run SNMPv3 to communicate with each other. To ensure communication, you need to configure the agent and NMS. This

section describes the configuration on a managed device (the agent side). For details about configuration on an NMS, see the pertaining NMS operation guide.

Pre-configuration Tasks

Before configuring a device to communicate with an NMS by running SNMPv3, configure a routing protocol to ensure that at least one route exist between access point and NMS.

Procedure

When you configure the device to communicate with the NMS using SNMPv3, **Configuring Basic SNMPv3 Functions** is mandatory and optional steps can be performed in any sequence.

After the SNMP basic functions are configured, the NMS can communicate with managed devices.

- The access permission of the NMS that uses the configured user name is Viewdefault view. The internet MIB (OID: 1.3.6.1) can be operated in this view.
- The managed device sends traps generated by the modules that are enabled by default to the NMS.

The following lists the enhanced management functions:

- To allow a specified NMS that uses the user name to manage specified objects on the device, see **Restricting Management Rights of the NMS**.
- To allow a specified module on the managed device to report traps to the NMS, see **Configuring the Trap Function**.
- If the NMS and managed device are both Huawei products, follow the procedure described in **Enabling the SNMP Extended Error Code Function** to allow the device to send more types of error codes. This allows more specific error identification and facilitates your fault location and rectification.

10.1.5.3.1 Configuring Basic SNMPv3 Functions

Context

For the configuration of basic SNMP functions, **Step 1**, **Step 5**, **Step 6**, **Step 7** and **Step 8** are mandatory steps. After the configurations are complete, the NMS and managed device can communicate with each other.

Precaution

The security levels from the highest to the lowest must be trap host security, user security, and user group security.

Among the security levels, privacy has the highest level and none has the lowest level. The security level description is as follows:

- privacy: authentication and encryption
- authentication: only authentication
- none: no authentication and no encryption

If the security level of a user group is privacy, the security levels of user and trap host must be privacy. If the security level of a user group is authentication, the security levels of user and trap host can be privacy or authentication.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 (Optional) Run:

```
snmp-agent
```

The SNMP agent function is enabled.

By default, the SNMP agent function is disabled. Executing the **snmp-agent** command can enable the SNMP agent function no matter whether parameters are specified in the command.

Step 3 (Optional) Run:

```
snmp-agent sys-info version v3
```

The SNMP version is configured.

SNMPv1, SNMPv2c, and SNMPv3 are enabled by default.

Step 4 (Optional) Run:

```
snmp-agent local-engineid engineid
```

An engine ID is set for the local SNMP entity.

By default, the device automatically generates an engine ID using the internal algorithm. The engine ID is composed of enterprise number and the device information.

If the local engine ID is set or changed, the existing SNMPv3 user will be deleted.

Step 5 Run:

```
snmp-agent group v3 group-name { authentication | noauth  | privacy }
```

An SNMPv3 user group is configured.

If the NMS or network devices are in an insecure environment (for example, the network is vulnerable to attacks), **authentication** or **privacy** can be configured in the command to enable data authentication or privacy.

Step 6 Run:

```
snmp-agent usm-user v3 user-name group-name [ authentication-mode { md5 | sha } password | privacy-mode { aes128 | des56 } encrypt-password | acl acl-number ]
```

Information about an SNMP user is configured.

NOTE

AES128 algorithm is recommended to improve data transmission security.

Step 7 Run:

```
snmp-agent target-host trap-paramsname paramsname v3 securityname securityname { authentication | noauthnopriv | privacy } [ binding-private-value ][ private-netmanager ]
```

Parameters for sending trap messages are set.

Step 8 Run:

```
snmp-agent
target-host trap-hostname hostname address { ipv4-addr [ udp-port udp-portid ]
[ public-net ] } trap-paramsname paramsname
```

The destination host for receiving trap messages and error codes is specified.

Note the following when running the command:

- The default destination UDP port number is 162. To ensure secure communication between the NMS and managed devices, run the **udp-port** command to change the UDP port number to a non-well-known port number.
- If trap messages sent from the managed device to the NMS need to be transmitted over a public network, the parameter **public-net** needs to be configured.

Step 9 (Optional) Run:

```
snmp-agent sys-info { contact contact | location location }
```

The equipment administrators contact information or location is configured.

By default, the vendor's contact information is "R&D Shenzhen, Huawei Technologies co.,Ltd.". The default location is "Shenzhen China".

This step is required for the NMS administrator to view contact information and locations of the equipment administrator when the NMS manages many devices. This helps the NMS administrator to contact the equipment administrators for fault location and rectification.

To configure both the equipment administrators contact information and location, run the **snmp-agent sys-info** command twice.

----End

10.1.5.3.2 (Optional) Restricting Management Rights of the NMS

Context

When multiple NMSs in the same SNMPv3 user group manage one device, perform this configuration based on the site requirements.

Scenario	Steps
All NMSs in this SNMPv3 user group have the right of the ViewDefault view.	No action required
Specified NMSs in this SNMPv3 user group have the right of the ViewDefault view.	**Step 1**, **Step 2**, **Step 4** (based on the user group)
	Step 1, **Step 5**, **Step 6** (based on the user)
	Step 1, **Step 2**, **Step 4**, **Step 5**, **Step 6** (based on the user group and user)
All NMSs in this SNMPv3 user group manage specified objects on the managed devices.	**Step 1**, **Step 3**, **Step 4**

Scenario	Steps
Specified NMSs in this SNMPv3 user group manage specified objects on the managed devices.	**Step 1**, **Step 2**, **Step 3**, **Step 4** (based on the user group)
	Step 1, **Step 3**, **Step 4**, **Step 5**, **Step 6** (based on the user)
	Step 1, **Step 2**, **Step 3**, **Step 4**, **Step 5**, **Step 6** (based on the user group and user)

When an ACL is used to control the NMS access rights, the constraints are as follows:

- When the ACL rule is **permit**, the NMS with the source IP address specified in this rule can access the local device.
- When the ACL rule is **deny**, the NMS with the source IP address specified in this rule cannot access the local device.
- If a packet matches no ACL rule, the NMS that sends the packet cannot access the local device.
- When no ACL rule is configured, all NMSs can access the local device.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure a basic ACL for an SNMP user group to filter the NMS that does not match the ACL.

For the creation procedure, see "ACL Configuration" in the *Huawei Wireless Access Points Configuration Guide-Security*.

Step 3 Run:

```
snmp-agent mib-view view-name { exclude | include } subtree-name [ mask mask ]
```

A MIB view is created, and manageable MIB objects are specified.

By default, an NMS has right to access the objects in the ViewDefault view.

If both the **included** and **excluded** parameters are configured for MIB objects that have an inclusion relationship, whether to include or exclude the lowest MIB object will be determined by the parameter configured for the lowest MIB object. For example, the snmpV2, snmpModules, and snmpUsmMIB objects are from top down in the MIB table. If the **excluded** parameter is configured for snmpUsmMIB objects and **included** is configured for snmpV2, snmpUsmMIB objects will still be excluded.

Step 4 Run:

```
snmp-agent group v3 group-name { authentication | noauth | privacy } [ read-view read-view | write-view write-view | notify-view notify-view | acl acl-number ] *
```

The write-read right is configured for a user group.

By default, the read-only view of an SNMP group is the ViewDefault view, and the names of the read-write view and inform view are not specified.

To configure the NMS to receive traps specified by *notify-view*, you must first configure the destination host for receiving traps.

Step 5 Configure a basic ACL for an SNMP user to filter the NMS that does not match the ACL.

For the creation procedure, see "ACL Configuration" in the *Huawei Wireless Access Points Configuration Guide-Security*.

Step 6 Run:

```
snmp-agent usm-user v3 user-name group-name  [ authentication-mode { md5 | sha } password | privacy-mode { aes128 | des56 } encrypt-password | acl acl-number ]
```

Authentication and encryption are configured for SNMPv3 users in the specified user group.

- To allow all NMSs using the same SNMPv3 user name to access the agent, omit the parameter **acl**.
- To allow specified NMSs to use this user name to access the agent, configure the parameter **acl**.

----End

Follow-up Procedure

After the access right are configured, especially after the IP address of the NMS is specified, if the IP address changes (for example, the NMS changes its location, or IP addresses are reallocated due to network adjustment), you need to change the IP address of the NMS in the ACL. Otherwise, the NMS cannot access the device.

10.1.5.3.3 (Optional) Configuring the Trap Function

Context

Users can enable the trap function for a specified module. The interface status trap is generated when the interface status changes. You need to enable the trap function for the **standard** module globally and enable the interface status trap function on the specified interface.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Enable the trap function.

Enable the trap function for a module.

- Run:

  ```
  snmp-agent trap enable
  ```

  The trap function is enabled for all modules.
- Run:

  ```
  snmp-agent trap enable feature-name
  ```

  The trap function is enabled for a specified module.

Enable the trap function for an interface.

Run:

snmp-agent trap enable feature-name ifnet trap-name { **linkdown** | **linkup** }

The trap function is enabled on all interfaces.

By default, the trap function is disabled on all interfaces. When parameters **linkdown** and **linkup** are configured for all **ifnet** modules, the device sends a trap to the NMS upon an interface status change. When an interface frequently sends traps to the NMS because of frequent status changes, you can disable the interface status trap function on the interface to reduce the NMS loads. The procedure is as follows:

1. Run:
   interface *interface-type interface-number*
   The interface view is displayed.
2. Run:
   undo enable snmp trap updown
   The interface status trap function is disabled.
3. Run:
   quit
   Return to the system view.

Step 3 Run:

snmp-agent trap source *interface-type interface-number*

The source interface for traps is specified.

After the source interface is specified, the IP address of the source interface is used as the source IP address for sending traps. This helps the NMS identify the trap source. The source interface that sends traps must have an IP address; otherwise, the commands will fail to take effect. To ensure device security, it is recommended that you set the source IP address to the local loopback address.

The source interface specified on the access point for traps must be consistent with that specified on the NMS; otherwise, the NMS does not accept the traps sent from the access point.

Step 4 Run:

snmp-agent trap queue-size *size*

The queue length of traps sent to the destination host is set.

The default queue length of traps sent to the destination host is 100.

The queue length depends on the number of generated traps. If the access point frequently sends traps to the NMS, set a longer queue length to prevent traps from being lost.

Step 5 Run:

snmp-agent trap life *seconds*

The lifetime of traps is set.

The default lifetime of traps is 120 seconds.

The lifetime of each trap depends on the number of generated traps. If the access point frequently sends traps to the NMS, set a longer lifetime to prevent traps from being lost.

----End

10.1.5.3.4 (Optional) Enabling the SNMP Extended Error Code Function

Context

This section describes how to enable the extended error code function on the SNMP agent when both the NMS and managed device are Huawei products. After this function is enabled, more types of error codes are provided to help you locate and rectify faults quickly and accurately.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
snmp-agent extend error-code enable
```

The extended error code function is enabled on the SNMP agent.

By default, SNMP sends standard error codes. It can send extended error codes to the NMS only after the extended error code function is enabled.

----End

10.1.5.3.5 Checking the Configuration

Prerequisites

The configurations of basic SNMPv3 functions are complete.

Procedure

- Run the **display snmp-agent usm-user** [*user-name*] command to check user information.
- Run the **display snmp-agent group** [*group-name*] command to view information about the SNMP user group.
- Run the **display snmp-agent sys-info version** command to check the enabled SNMP version.
- Run the **display acl** *acl-number* command to check the ACL rules.
- Run the **display snmp-agent mib-view** command to check the MIB view.
- Run the **display snmp-agent sys-info contact** command to check the equipment administrator's contact information.
- Run the **display snmp-agent sys-info location** command to check the location of the access point.
- Run the **display current-configuration** | **include trap** command to check trap configuration.
- Run the **display snmp-agent trap all** command to check current and default status of all traps in all features.
- Run the **display snmp-agent trap-source** command to check the source interface for sending traps.

- Run the **display snmp-agent target-host** command to check information about the target host.
- Run the **display snmp-agent extend error-code status** command to check whether the function that the device sends extended error codes to the NMS is enabled.

----End

10.1.6 Maintaining SNMP

This chapter describes how to monitor SNMP running status after the SNMP configuration is complete.

10.1.6.1 Checking the Statistics About SNMP Packets

Procedure

- Run:
  ```
  display snmp-agent statistics
  ```
  The statistics about SNMP messages are displayed.

----End

10.1.7 Common Configuration Errors

This chapter describes the common SNMP configuration errors, including the fault symptoms and troubleshooting procedures.

10.1.7.1 The SNMP Host Cannot Connect to the NMS

Fault Description

The SNMP host cannot connect to the NMS.

Procedure

Check whether the SNMP configuration on the host is correct according to the following table.

Table 10-6 SNMP configuration

Item	Method	Procedure
Check whether the host supports the SNMP version used by the NMS for sending a login request.	Run the **display snmp-agent sys-info version** command to view the SNMP version of the host.	If the host does not support the SNMP version, run the **snmp-agent sys-info version** command to set the SNMP version on the host.

Item	Method	Procedure
View the community string configured on the host.	Run the **display snmp-agent community** command.	If the community string used by the NMS for sending a login request is different from that configured on the host, run the **snmp-agent community** command to configure a read-write community string, which must be the same as that configured on the host.
If SNMPv3 is used, check whether information about the SNMP user group and users is correct.	● Run the **display snmp-agent group** command to view information about the SNMPv3 user group.	If information is incorrect, modify the configurations. ● Run the **snmp-agent group** command to view information about the SNMPv3 user group. ● Run the **snmp-agent usm-user** command to view information about the SNMPv3 user.

10.1.7.2 NM Station Fails to Receive Traps Sent from the Host

Fault Description

The NM station fails to receive alarms sent from the host.

Procedure

Check whether the target host of SNMP traps on the access point is correctly configured.

If the target host of SNMP traps is configured incorrectly, see the following configuration examples.

Table 10-7 Typical configuration of the host that sends traps

Configuration Example	Command
Configure a host for sending trap messages. The host uses SNMPv2c. The port number is 162 by default, the security name is huawei, and the IP address is 192.168.1.1.	<Huawei> **system-view** [Huawei] **snmp-agent target-host trap-paramsname abc v2c securityname huawei** [Huawei] **snmp-agent target-host trap-hostname aaa address 192.168.1.1 trap-paramsnam abc**

Configuration Example	Command
Configures an SNMPv3 user named **huawei** that belongs to the user group named **huawei_group**. The alarm right (Notify-view) for the SNMPv3 user is Huawei_view, which indicates that the user has the right to access all the nodes under the ISO through SNMP.	# Configure a MIB view. <Huawei> **system-view** [Huawei] **snmp-agent mib-view Huawei_view include iso** # Configure a user group. [Huawei] **snmp-agent group v3 huawei_group noauth read-view Huawei_view write-view Huawei_view notify-view Huawei_view** # Configure users. [Huawei] **snmp-agent usm-user v3 huawei huawei_group**
Configure a host for sending trap messages. The host uses SNMPv3. The port number is 162 by default, the security name is huawei, and the IP address is 192.168.1.1 (huawei must be a real user).	<Huawei> **system-view** [Huawei] **snmp-agent target-host trap-paramsname abc v3 securityname huawei authentication** [Huawei] **snmp-agent target-host trap-hostname aaa address 192.168.1.1 trap-paramsname abc**
Check the status of the trap function. If the trap function is disabled, enable the trap function.	# Check the status of the trap function. [Huawei] **display snmp-agent trap all** # Enable the trap function. [Huawei] **snmp-agent trap enable**

10.1.8 Reference

This section lists references of SNMP.

The following table lists the references of this document.

Document	Description	Remarks
RFC 1155	Structure and identification of management information for TCP/IP-based internets	-
RFC 1157	Simple Network Management Protocol (SNMP)	-
RFC 1212	Concise MIB definitions	-
RFC 1215	Convention for defining traps for use with the SNMP	-
RFC 1448	Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)	-
RFC 1901	Introduction to Community-based SNMPv2	-
RFC 1907	Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)	-

Document	Description	Remarks
RFC 2271	An Architecture for Describing SNMP Management Frameworks	-
RFC 2570	Introduction to Version 3 of the Internet-standard Network Management Framework	-
RFC 2578	Structure of Management Information Version 2 (SMIv2)	-
RFC 2579	Textual Conventions for SMIv2	-
RFC 2580	Conformance Statements for SMIv2	-
RFC 3410	Introduction and Applicability Statements for Internet-Standard Management Framework	-
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	-
RFC 3413	Simple Network Management Protocol (SNMP) Applications	-
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 3512	Configuring Networks and Devices with Simple Network Management Protocol (SNMP)	-

10.2 RMON Configuration

Remote Network Monitoring (RMON), defined by IETF, is a widely used network management protocol. It provides packet statistics and alarm functions for Ethernet interfaces. The management devices use RMON to remotely monitor and manage network elements. RMON2 is an enhancement of RMON. Currently, the device can collect and analyze statistics on IP packets.

10.2.1 RMON and RMON2 Overview

RMON and RMON2 implementation is based on SNMP and uses the same network management station (NMS) as SNMP to manage network elements.

RMON

SNMP is a widely used network management protocol. It collects statistics about network communication by using the agent software embedded in the managed devices. The NMS polls the agent to provide network communication information. The agent then searches the

Management Information Base (MIB) and returns the required information to the NMS. The NMS can manage the network based on returned information. The MIB counter only records the statistics, but cannot analyze history information about routine communication. To display traffic volume and changes on a whole day, the NMS has to keep on polling and analyze network traffic based on the obtained information.

SNMP polling has the following disadvantages:

- Occupies a large number of network resources. Polling generates many communication packets. On a large-sized network, congestion may occur or even the network is blocked. Therefore, SNMP is not applicable to large-sized networks and cannot recycle large amount of data, such as routing information.
- Increases the burden of network administrators. The network administrators are responsible for collecting all data using the NMS software. It is difficult for an administrator to monitor more than three network segments.

IETF develops RMON to improve usability of network management information and lighten the burden on the NMS and network administrators. Compared with SNMP, RMON is more applicable to large-sized networks and can monitor traffic on one or multiple network segments. The characteristics of RMON are as follows:

- SNMP is the basis of RMON, and RMON is an enhancement of SNMP.

  RMON is implemented based on the SNMP structure and compatible with SNMP. It consists of NMS and agents. Network administrators can use the SNMP NMS to implement RMON without additional training.
- RMON enables SNMP to monitor remote network devices effectively and actively.

  Using RMON, managed devices automatically send traps when alarm thresholds are exceeded. Therefore, the management devices do not need to obtain MIB variables by continuous polling and comparison. The RMON reduces traffic volume between the management and managed devices, and allows large-size networks to be more easily and effectively managed.

RMON defines multiple monitors to collect network management information in either of the following ways:

- The NMS obtains management information directly from the RMON probe and controls network resources. This allows the NMS to obtain all RMON MIB information.
- A RMON agent is embedded into a network device, so that the device can provide the RMON probe function. The NMS uses SNMP protocol to exchange data with the RMON agent and collect network management information. Due to the limitation on resources, the NMS can only obtain information about statistics, history, alarms, and events groups.

Huawei devices have embedded RMON agent. The management device can obtain information including traffic volume, error packet statistics, and performance statistics of the entire network segment connected to the interfaces on the managed devices to implement network monitoring.

RMON2

RMON2 is an extension of RMON, and has the same mechanism as RMON.

RMON and RMON2 both monitor traffic on Ethernet links; however, RMON monitors traffic at only MAC layer and RMON2 monitors traffic at the upper layers above MAC layer.

RMON2 codes and decodes data packets from Layer 3 to Layer 7 of the OSI model. In RMON2, the RMON agents provide two major functions:

- Monitor traffic based on network layer protocols and addresses, including IP protocol. This enables the agent to learn its connected external LAN network segment and monitor traffic flowing to the LAN through the switch.
- Record the incoming and outgoing traffic of the specific application, such as email, FTP, and WWW because it can decode and monitor the traffic.

The RMON agent on Huawei devices can collect statistics about IP packets on the network segments connected to the managed devices, and monitors traffic flowing to these interfaces from the hosts on the network segments.

10.2.2 Principles

Before configuring RMON, understand concepts of four groups (statistics, history, alarm, and event) and Huawei-defined extended alarm group. Before configuring RMON2, understand the concepts of protocolDir and nlHost.

RMON

RMON provides packet statistics and alarm functions. The management devices use RMON to remotely monitor and manage network elements.

RMON uses statistics group and history group to provide Ethernet statistics and history statistics functions.

- Ethernet statistics (statistics group in RMON MIB): collects basic statistics on each monitored network. The system keeps on collecting traffic statistics and distribution of each type of packets on a network segment. Additionally, the system can count the number of error packets of different types, collisions, CRC error packets, undersized (or large) packets, broadcast packets, bytes received, and packets received.
- History statistics (history group in RMON MIB): periodically samples and records network statistics. The system can periodically collect statistics on each type of traffic, including bandwidth usage, number of error packets, and total number of packets.

RMON alarm functions include event definition function and alarm threshold setting function.

- Event definition (event group in RMON MIB): controls the events and notifications sent from the device and provides all events related to RMON agent. When an event occurs, the system records a log or sends a trap to the NMS.
- Alarm threshold setting (alarm group in RMON MIB): monitors the specified alarm variables (OID of an object). Based on the user-defined thresholds and sampling time, the system periodically obtains the specified alarm variables. When the alarm variables values reach or exceed the rising threshold, a rising threshold alarm event is triggered. When the alarm variables values reach or fall below the falling threshold, a falling threshold alarm event is triggered. The RMON agent records the monitored status in log or sends a trap to the NMS.

RMON standard (RFC 2819) defines multiple RMON groups. The access point supports the Huawei-defined extended alarm, statistics, history, alarm, and event groups. Details about the groups are as follows:

- Statistics group

  The statistics group keeps on collecting statistics on each type of traffic on Ethernet interfaces and records statistics results in the etherStatsTable for later retrieval. Traffic statistics include the number of network collisions, CRC error packets, undersized (or large) data packets, broadcast packets, multicast packets, received bytes, and received packets.

  After a statistics entry is created on an interface, the statistics group starts collecting statistics on the packets. The statistics are accumulated.

- History group

  The history group periodically collects network status statistics and stores them for future use.

  The history group provides two tables:

  - historyControlTable: sets control information such as the sampling interval.
  - etherHistoryTable: stores network statistics collected by the history group and provides the network administrator with history statistics such as the traffic on a network segment, error packets, broadcast packets, bandwidth usage, and collisions.

- Event group

  The defined events are used for the configuration options of alarm group and extended alarm group. When alarm conditions are met, an event is triggered. RMON event management is to add events to the specified rows in the event table, and the following options are supported:

  - **log**: only send log
  - **trap**: only send trap to the NMS
  - **log-trap**: send both log and trap
  - **none**: take no action

- Alarm group

  An alarm group presets a set of thresholds for alarm variables, which can be objects in a local MIB. Based on the user-defined alarmTable, the system periodically obtains the specified alarm variables. When the alarm variables values reach or exceed the rising threshold, a rising threshold alarm event is triggered. When the alarm variables values reach or fall below the falling threshold, the system takes actions according to the action configuration.

- Extended alarm group

  Based on RFC 2819, the extended alarm group has the following new function: set alarm object and keepalive time using expressions. This group provides the prialarmTable. Compared with the alarm table defined in RFC 2819, the extended alarm table has the following new options:

  - Extended alarm variable expression. It is the arithmetic expression composed of alarm variables OIDs (+, -, *, /, or brackets).
  - Descriptions of extended alarm entries
  - Sampling interval variables
  - Extended alarm types: Forever or Cycle. If Cycle is set, no alarm is generated and the entry is deleted after the specified cycle period expires.

Each entry has a lifetime. When an entry's status is not valid, the entry can exist for a certain period before it is deleted. The entry is deleted when the lifetime decreases to 0. **Table 10-8** shows the capacity of each table and the maximum lifetime of an entry in each table.

Table 10-8 Lifetime of entries in each table

Table	Table Size (Bytes)	Maximum Lifetime (Seconds)
etherStatsTable	100	600
historyControlTable	100	600
alarmTable	60	6000
eventTable	60	600
logTable	600	-

NOTE

Each entry in the historyControlTable corresponds to a maximum of 10 history records in the etherHistoryTable. When more than 10 records are generated, the old ones are overwritten.

No maximum lifetime is specified for the entries in logTable. Each event entry in logTable corresponds to up to 10 logs. When more than 10 logs are generated, the old ones are overwritten.

When an LPU is removed, the etherStatsTable and historyControlTable status is changed to invalid and the lifetime of entries in the etherStatsTable and historyControlTable is set to 1200 seconds. When the lifetime decreases to 0, the entry is deleted.

When an LPU is inserted, the corresponding entry status is changed to valid.

RMON2

Currently, the access point provides two RMON2 MIB groups: protocolDir and nlHost, and the RMON agent can collect statistics on IP packets. The RMON agent supports three tables: protocolDirTable, hostTable, and hostControlTable.

The hostTable uses customized indexes to invoke the protocolDirTable and hostControlTable. The hostTable does not need to be configured when you configure RMON2 traffic statistics function. After the protocolDirTable and hostControlTable are configured, the hostTable automatically collect traffic statistics.

- protocolDirTable

  Lists the protocols that the RMON agent can resolve and collect statistics on. Each protocol occupies a row. The protocols include network-layer, transport-layer, and upper-layer protocols.

- hostTable

  Collects traffic statistics on each host and analyzes incoming and outgoing data packets on interfaces based on IP addresses.

- hostControlTable

  Is classified into network-layer hostControlTable and application-layer hostControlTable. The hostControlTable defines the statistics monitoring interface and records the number of frames received by the interface but are not recorded into the nlHost table. Additionally, this table records the number of times entries are added and deleted and the maximum number of entries in nlHostTable.

Currently, the access point supports only network-layer hostControlTable, so it does not control application-layer host groups. Therefore, only IP protocols can be configured in the protocolDirTable.

10.2.3 Configuring RMON

RMON collects traffic statistics and monitors network status on the specified network segment.

Pre-configuration Tasks

Before configuring RMON, complete the following tasks:

- Configuring Ethernet interface parameters
- Configuring basic SNMP functions

Configuration Process

The RMON statistics function and RMON alarm function can be configured in any sequence. However, if the alarm variables configured in RMON alarm function are MIB variables defined in the statistics group or history group, the Ethernet statistics function or history statistics function must be configured on the monitored Ethernet interface first. Otherwise, alarm entries cannot be created.

10.2.3.1 Configuring RMON Statistics Functions

Context

RMON statistics functions include Ethernet statistics function and history statistics function, which apply to different scenarios:

- To keep on collecting traffic statistics on an Ethernet interface, configure the Ethernet statistics function. Ethernet statistics include the number of network collisions, CRC error packets, undersized (or large) data packets, broadcast packets, multicast packets, received bytes, and received packets.
- To store the statistics on the specified interface for later retrieval, configure the history statistics function. History statistics include bandwidth usage, number of error packets, and total of packets.

Procedure

- Configuring Ethernet statistics
  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface gigabitethernet *interface-number*

     The interface view is displayed.
  3. Run:
     rmon-statistics enable

RMON statistics function is enabled on an interface.

4. Run:
   rmon statistics *entry-number* [**owner** *owner-name*]

   A statistics table is created and an entry is added to the table.

- Configuring history statistics

  1. Run:
     system-view

     The system view is displayed.
  2. Run:
     interface gigabitethernet *interface-number*

     The interface view is displayed.
  3. Run:
     rmon-statistics enable

     RMON statistics function is enabled on an interface.
  4. Run:
     rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *owner-name*]

     A history control table is created and an entry is added to the table.

  NOTE

  - As recommended by the RMON specifications, each monitored interface should be configured with more than two history control entries. One entry is sampled every 30 seconds while another entry is sampled every 30 minutes.
  - The short sampling interval enables a monitor to probe the sudden changes of traffic modes, and the long sampling interval is applicable if the interface status is relatively stable.
  - Each history control table stores 10 records. When more records are generated, the old ones are overwritten.
  - To reduce the impact of RMON on system performance, the sampling interval of the history control table should be longer than 10 seconds. In addition, an interface cannot be configured with too many entries for the history control table and alarm table.
  - If the RMON statistics function is not enabled on an interface, statistics in the RMON statistics table and history table are 0.

----End

10.2.3.2 Configuring RMON Alarm Functions

Context

RMON alarm functions include event definition function and alarm threshold setting function.

To monitor the system running status, configure the alarm threshold setting function. When an error occurs in the system, the related event is triggered. The event definition function can determine whether to log the event or send a trap to the NMS.

NOTE

If the alarm variables configured in RMON alarm function are MIB variables defined in the statistics group or history group, the Ethernet statistics function or history statistics function must be configured on the monitored Ethernet interface first.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure event definition function.

Run the **rmon event** *entry-number* [**description** *string*] { **log** | **trap** *object* | **log-trap** *object* | **none** } [**owner** *owner-name*] command to create an event table and add an entry to the table.

Step 3 Configure alarm threshold function.

(Optional) Run the **snmp-agent trap enable feature-name rmon** [**trap-name** { **fallingalarm** | **risingalarm** | **rmon_pri_fallingalarm** | **rmon_pri_risingalarm** }] command to enable the alarm function for the RMON module.

By default, all alarms for the RMON module are enabled. If only one or some event alarms need to be enabled, run the **snmp-agent trap enable feature-name rmon trap-name** command.

1. Run the **rmon alarm** *entry-number alarm-OID sampling-time* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *owner-name*] command to create an alarm table and add an entry to the table.
2. Run the **rmon prialarm** *entry-number prialarm-formula description-string sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **cycle** *entry-period* | **forever** } [**owner** *owner-name*] command to create an extended alarm table and add an entry to the table.

   If the events (*event-entry1, event-entry2*) corresponding to alarm rising threshold and falling threshold are not configured in the event table, no alarm will be generated even if the alarm conditions are met. In this situation, the alarm record status is undercreation, but not valid.

   After either of the events is configured, the alarm will be generated when the alarm conditions are met and the alarm status is valid. If an incorrect alarm variable is created, for example, an inexistent OID is specified, the alarm is in the undercreation state and no alarm is generated.

----End

10.2.3.3 Checking the Configuration

Prerequisites

The RMON configurations are complete.

Procedure

- Run the **display rmon alarm** [*entry-number*] command to view RMON alarm configurations.

- Run the **display rmon event** [*entry-number*] command to view RMON event configurations.
- Run the **display rmon eventlog** [*entry-number*] command to view details about RMON event logs.
- Run the **display rmon history** [**gigabitethernet** *interface-number*] command to view RMON history sampling records.
- Run the **display rmon prialarm** [*entry-number*] command to view RMON extended alarm configurations.
- Run the **display rmon statistics** [**gigabitethernet** *interface-number*] command to view RMON Ethernet statistics.
- Run the **display snmp-agent trap feature-name rmon all** command to view the status of all traps about the RMON module.

----End

10.2.4 Configuring RMON2

RMON2 collects statistics on IP packets on the specified interface.

Pre-configuration Tasks

Before configuring RMON2, complete the following task:

- Configuring Ethernet interface parameters

10.2.4.1 Configuring RMON2 Statistics Function

Context

RMON2 collects statistics about traffic on a specified interface, including the source and destination hosts of traffic and traffic passing the interface from each host on the network.

Currently, RMON2 on the access point can collect statistics on IP packets on the specified interfaces.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
rmon2 hlhostcontroltable index ctrl-index [ datasource interface interface-type interface-number ] [ maxentry maxentry-value ] [ owner owner-name ] [ status { active | inactive } ]
```

A host control table is created and an entry is added to the table.

If the host control table contains too many entries, system performance is degraded. The default settings of host control table are recommended. By default, a host control table contains a maximum of 50 entries.

When creating an entry, specify the **datasource interface** parameter to identify the interface, which specifies the subnet. The parameter value, namely, the interface index, is the data source defining the entry. In the command, the data source is represented by interface type and number. Only one entry can be created for each interface in the host control table.

The parameter **status** in the **display rmon2 hlhostcontroltable** command output matches the hlhostcontrolstatus value, which indicates the entry status.

- When the hlhostcontrolstatus value is set to **inactive**, all related entries in the host table are deleted automatically.
- When the hlhostcontrolstatus value is set to **active**, you cannot change the hlhostcontroldatasource and hlhostcontrolnlmaxdesiredentries values.
- If an interface that corresponds to the hlhostcontroldatasource in an entry is deleted, the entry is deleted at the same time.

Step 3 Run:

```
rmon2 protocoldirtable protocoldirid protocol-id parameter parameter-value [ descr
description-string ] [ host { notsupported | supportedon | supportedoff } ]
[ owner owner-name ] [ status { active | inactive } ]
```

A protocol directory table is created and an entry is added to the table.

RMON2 supports only statistics on IP packets on an Ethernet interface. A protocol occupies an entry, so there is only one entry in the table.

When running the **rmon2 protocoldirtable** command, you must set the description and protocols supported by the host. That is, the **descr** and **host** parameters are mandatory.

The parameter **status** in the **display rmon2 protocoldirtable** command output matches the protocolDirStatus value, which indicates the entry status.

- When the **status** parameter is set to **active**, the **descr** value cannot be modified. The value of **host** (corresponding to the protocolDirHostConfig value, indicating the protocol directory host configuration) can be modified. This parameter indicates whether to monitor the network-layer host table of the protocol.
  - If the **host** value is set to **notsupported**, the **host** value cannot be modified.
  - If the **host** value is not **notsupported**, the value can be switched between **supportedon** and **supportedoff**.
  - When the **host** value is changed from **supportedon** to **supportedoff**, the corresponding entry in the host control table is deleted.
- When the status is **inactive**, all related entries in the host table are deleted.

----End

10.2.4.2 Checking the Configuration

Procedure

- Run the **display rmon2 protocoldirtable** command to view information about the protocol directory table.
- Run the **display rmon2 hlhostcontroltable** [**index** *ctrl-index*] command to view information about the host control table.

- Run the **display rmon2 nlhosttable** [**hostcontrolindex** *ctrl-index*] [**hostaddress** *ip-address*] command to view information about the host table.

----End

10.2.5 References

The following table lists the references.

Table 10-9 References

Document	Description	Remarks
RFC2021	Remote Network Monitoring Management Information Base Version 2 using SMIv2	-
RFC2819	Remote Network Monitoring Management Information Base	-
RFC2895	Remote Network Monitoring MIB Protocol Identifier Reference	-
RFC3577	Introduction to the Remote Monitoring (RMON) Family of MIB Modules	-

10.3 Mirroring Configuration

Packet mirroring copies packets to a specified destination so that you can analyze packets to monitor the network and rectify faults.

NOTE

The terms mirrored port, port mirroring, traffic mirroring, and mirroing in this manual are mentioned only to describe the product's function of communication error or failure detection, and do not involve collection or processing of any personal information or communication data of users.

10.3.1 Overview

This section describes the definition and purpose of mirroring.

Definition

Packet mirroring copies the packets on a mirrored port (source port) to an observing port (destination port).

Purpose

During network maintenance, you may need to obtain and analyze packets in some conditions. For example, if you detect suspected attack packets, you need to obtain and analyze the packets without affecting packet forwarding.

Packet mirroring copies packets on a mirrored port to an observing port without affecting packet forwarding. You can analyze packets copied to the observing port by a monitoring device to monitor the network and rectify faults.

10.3.2 Principles

This section describes the mirroring implementation principles.

Concepts

- Mirrored port

  All the packets passing through a mirrored port are copied to a local or remote observing port.
- Local observing port

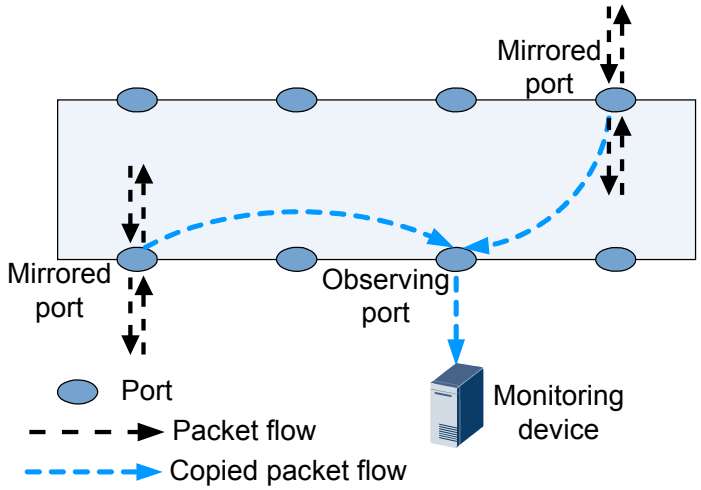
  In local packet mirroring, a local observing port is connected to a monitoring device and is used to export the packets copied from a mirrored port.
- Remote observing server

  In remote packet mirroring, a remote observing server defines the mirrored ports and IP address of the remote monitoring device so that mirrored packets can be copied to the monitoring device.

Port Mirroring

A packet passing through a mirrored port is copied and then sent to a specified monitoring device for analysis and monitoring, as shown in **Figure 10-8**.

Figure 10-8 Networking diagram of port mirroring



Port mirroring can be performed on the packets in the following directions:

- Inbound: mirrors the packets that are received by the port.
- Outbound: mirrors the packets that are sent by the port.
- Bidirectional: mirrors the packets that are sent and received by the port.

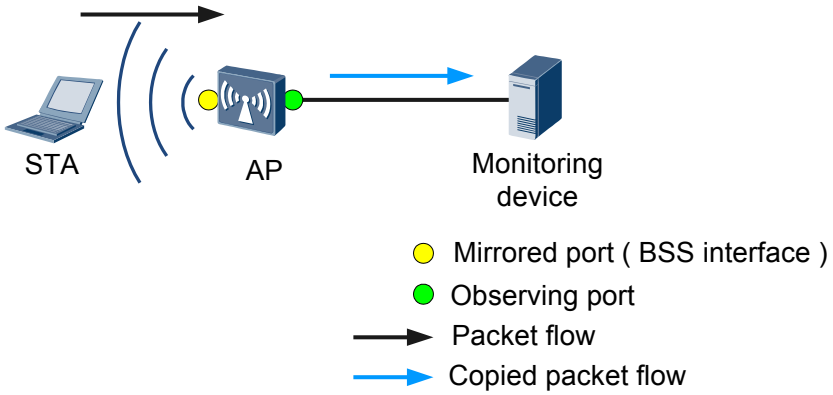
NOTE

If the mirrored port and observing port are added to the same port isolation group in Layer 2 isolation mode, the inbound traffic on the mirrored port is isolated and cannot reach the observing port; however, the outbound traffic on the mirrored port is not isolated and is still mirrored to the observing port.

Port mirroring is classified into local port mirroring and remote port mirroring.

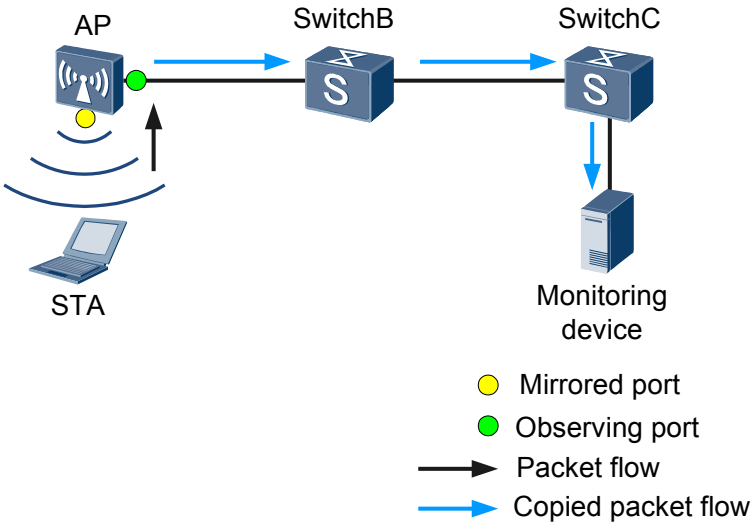
- In local port mirroring, the monitoring and monitored devices are connected to the same device, as shown in **Figure 10-9**.

Figure 10-9 Networking diagram of local mirroring



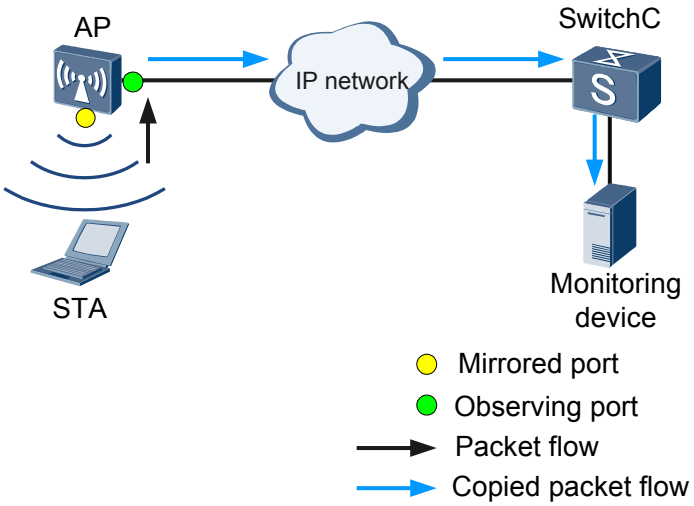
- In remote mirroring, the monitoring and monitored devices are connected through a Layer 2 network or Layer 3 network.
  - In Layer 2 remote port mirroring, packets passing through a mirrored port are tagged a VLAN ID, broadcast in the remote mirroring VLAN through the observing port, and forwarded to the monitoring device, as shown in **Figure 10-10**.

Figure 10-10 Networking diagram of Layer 2 remote port mirroring



  - In Layer 3 remote port mirroring, packets passing through a mirrored port sent to the monitoring device through the Layer 3 IP network, as shown in **Figure 10-11**.

Figure 10-11 Networking diagram of Layer 3 remote port mirroring



10.3.3 Configuring Mirroring

This section describes the procedures for configuring mirroring.

10.3.3.1 Configuring Local Port Mirroring

After local port mirroring is configured, packets passing through mirrored ports are copied to a local monitoring device for analysis and monitoring.

Pre-configuration Tasks

Before configuring local port mirroring, complete the following task:

- Ensuring that the link layer protocol status of ports is Up.

10.3.3.1.1 Configuring a Local Observing Port

Context

In local mirroring, the monitoring device is directly connected to the observing port.

Do not configure other functions on an observing port; otherwise, the mirroring function is affected.

- If other service packets are transmitted on the observing port besides the mirrored packets, the packet sources cannot be identified.
- If congestion occurs on the observing port, mirrored packets may be discarded because of their low priorities.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
observe-port interface interface-type interface-number
```

A local observing port is configured.

NOTE

The observing port must be a Layer 2 physical interface.

----End

10.3.3.1.2 Configuring a Local Mirrored Port

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface wlan-bss wlan-bss-number
```

A WLAN-BSS interface is created.

Step 3 Run:

```
mirror to observe-port { both | inbound | outbound }
```

A local mirrored port is configured.

----End

10.3.3.1.3 Checking the Configuration

Procedure

- Run the **display observe-port** command to check the observing port.
- Run the **display mirror-port** command to check the port mirroring configuration.

----End

10.3.3.2 Configuring Remote Port Mirroring

After remote port mirroring is configured, packets passing through mirrored ports are copied to a remote monitoring device for analysis and monitoring.

Pre-configuration Tasks

Before configuring remote port mirroring, complete the following tasks:

- Ensuring that the observing port can communicate with the monitoring device on a Layer 2 or Layer 3 network

10.3.3.2.1 Configuring a Remote Observing Port or Remote Observing Server

Context

In remote mirroring, the observing device and monitored device are connected over a Layer 2 or 3 network. Therefore, remote mirroring can be classified into Layer 2 remote mirroring and Layer 3 remote mirroring.

- Layer 2 remote mirroring: The device encapsulates mirrored packets into VLAN packets so that the mirrored packets can be transmitted to the remote monitoring device over a Layer 2 network.
- Layer 3 remote mirroring: The device encapsulates mirrored packets into GRE packets so that the mirrored packets can be transmitted to the remote monitoring device over a Layer 3 network.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Configure an observing port for Layer 2 remote mirroring or an observing server for Layer 3 remote mirroring based on the site requirement.

- Run:
  observe-port interface *interface-type interface-number* **vlan** *vlan-id*

  The observing port for Layer 2 remote mirroring is configured, and the remote mirroring VLAN is specified.

  NOTE

  The observing port must be a Layer 2 physical interface.

- Run:
  observe-server destination-ip *destination-ip-address* **source-ip** *source-ip-address* [**dscp** *dscp-value*]

  The observing server for Layer 3 remote mirroring is configured.

  NOTE

  - The *destination-ip-address* parameter indicates the IP address of the observing device, and the *source-ip-address* parameter indicates the IP address of the mirrored port.

----End

10.3.3.2.2 Configuring a Remote Mirrored Port

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface wlan-bss wlan-bss-number
```

A WLAN-BSS interface is created.

Step 3 Run:

```
mirror to observe-server{ both | inbound | outbound }
```

A remote mirrored port is configured.

----End

10.3.3.2.3 Checking the Configuration

Procedure

- Run the **display observe-server** command to check the observing server.
- Run the **display mirror-port** command to check the port mirroring configuration.

----End

10.3.4 Configuration Examples

This section provides several configuration examples of packet mirroring, including network requirements, configuration roadmap, and configuration procedures.

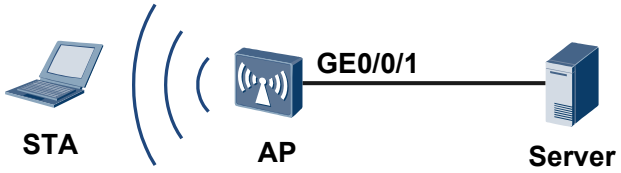
10.3.4.1 Example for Configuring Local Port Mirroring

Networking Requirements

As shown in **Figure 10-12**, the AP that uses WLAN-BSS1 provides WLAN services for wireless users, and the AP's GE0/0/1 is directly connected to the server. The WLAN services have been configured on the AP.

The server functioning as a monitoring device is required to monitor the packets sent by the AP.

Figure 10-12 Networking diagram of local port mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the AP's GE0/0/1 as a local observing port to enable the connected server to receive the mirrored packets.
2. Configure the AP's WLAN-BSS1 that provides WLAN services as a mirrored port to monitor the packets on WLAN-BSS1.

Procedure

Step 1 Configure an observing interface.

Configure GE0/0/1 as a local observing port on the AP.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] observe-port interface gigabitethernet 0/0/1
```

Step 2 Configure a mirrored port.

Configure WLAN-BSS1 as a mirrored port on the AP to monitor the packets sent by STA.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] mirror to observe-port inbound
[AP-Wlan-Bss1] quit
[AP] quit
```

Step 3 Verify the configuration.

Check the configuration of the observing port.

```
<AP> display observe-port
  ------------------------------------------------------------------
  Index    : 1
  Interface: GigabitEthernet0/0/1
  Used     : 1
------------------------------------------------------------------
```

Check the configuration of the mirrored port.

```
<AP> display mirror-port
  ------------------------------------------------------------------------------
    Mirror-port              Direction  Observe-dest
  ------------------------------------------------------------------------------
  1 Wlan-Bss1                Inbound    GigabitEthernet0/0/1
  ------------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 101
#
dhcp enable
#
 observe-port interface GigabitEthernet0/0/1
#
interface Vlanif101
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 mirror to observe-port inbound
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
```

```
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/1
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

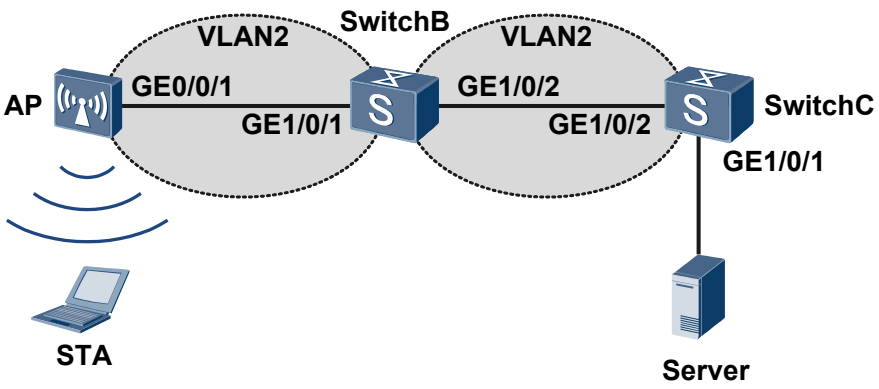
10.3.4.2 Example for Configuring Layer 2 Remote Port Mirroring

Networking Requirements

As shown in **Figure 10-13**, the AP provides WLAN servers for wireless users and uses WLAN-BSS1 as the BSS interface. The server connects to GE1/0/1 on SwitchC and the AP connects to SwitchC through GE0/0/1 in a Layer 2 network. The WLAN services have been configured on the AP.

The server functioning as a monitoring device is required to remotely monitor the packets sent by the AP.

Figure 10-13 Networking diagram of Layer 2 remote port mirroring



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure interfaces to ensure that the devices can communicate on Layer 2.
2. Configure GE0/0/1 of the AP as a remote observing port to send mirroring packets passing through the Layer 2 network to the monitoring device.
3. Configure the AP's WLAN-BSS1 that provides WLAN services as a mirrored port to monitor the packets on WLAN-BSS1.

Procedure

Step 1 Configure interfaces to ensure that the devices can communicate on Layer 2.

Configure the AP.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan 2
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 2
[AP-GigabitEthernet0/0/1] quit
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 2
[AP-Wlan-Bss1] port hybrid untagged vlan 2
[AP-Wlan-Bss1] quit
```

Configure SwitchB.

```
<Quidway> system-view
[Quidway] sysname SwitchB
[SwitchB] vlan 2
[SwitchB-vlan2] quit
[SwitchB] interface gigabitethernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-type trunk
[SwitchB-GigabitEthernet1/0/1] port trunk allow-pass vlan 2
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface gigabitethernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-type trunk
[SwitchB-GigabitEthernet1/0/2] port trunk allow-pass vlan 2
[SwitchB-GigabitEthernet1/0/2] quit
```

Configure SwitchC.

```
<Quidway> system-view
[Quidway] sysname SwitchC
[SwitchC] vlan 2
[SwitchC-vlan2] quit
[SwitchC] interface gigabitethernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-type access
[SwitchC-GigabitEthernet1/0/1] port default vlan 2
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface gigabitethernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-type trunk
[SwitchC-GigabitEthernet1/0/2] port trunk allow-pass vlan 2
[SwitchC-GigabitEthernet1/0/2] quit
```

Step 2 Configure a remote observing port.

Configure GE0/0/1 as a remote observing port on the AP.

```
[AP] observe-port interface gigabitethernet 0/0/1 vlan 2
```

Step 3 Configure a mirrored port.

Configure WLAN-BSS1 as a mirrored port on the AP.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] mirror to observe-port inbound
[AP-Wlan-Bss1] quit
[AP] quit
```

Step 4 Verify the configuration.

Check the configuration of the observing port.

```
<AP> display observe-port
  ------------------------------------------------------------------------------
  Index    : 1
  Interface: GigabitEthernet0/0/1
  Used     : 1
  ------------------------------------------------------------------------------
```

Check the configuration of the mirrored port.

```
<AP> display mirror-port
  ------------------------------------------------------------------------------
    Mirror-port              Direction  Observe-dest
  ------------------------------------------------------------------------------
  1 Wlan-Bss1                Inbound    GigabitEthernet0/0/1
  ------------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 2
#
dhcp enable
#
 observe-port interface GigabitEthernet0/0/1 vlan 2
#
interface Vlanif2
 ip address 192.168.11.1 255.255.255.0
 dhcp select interface
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface Wlan-Bss1
 port hybrid pvid vlan 2
 port hybrid untagged vlan 2
 mirror to observe-port inbound
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/1
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

- Configuration file of SwitchB

```
#
sysname SwitchB
#
vlan batch 2
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface GigabitEthernet1/0/2
```

```
 port link-type trunk
 port trunk allow-pass vlan 2
#
return
```

- Configuration file of SwitchC

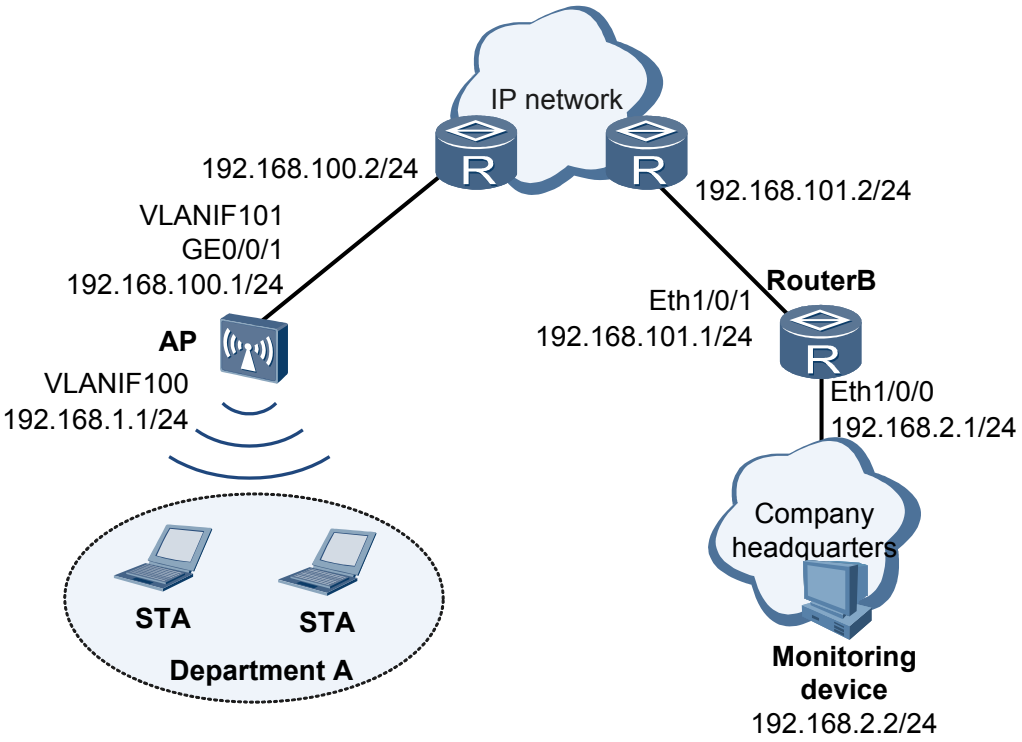
```
#
sysname SwitchC
#
vlan batch 2
#
interface GigabitEthernet1/0/1
 port link-type access
 port default vlan 2
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 2
#
return
```

10.3.4.3 Example for Configuring a Remote Mirroring Server

Networking Requirements

As shown in **Figure 10-14**, the AP uses WLAN-BSS1 to provide WLAN services for a company's department A, and the monitoring device is deployed at the company headquarters. The WLAN services have been configured on the AP. To improve information security, the headquarters requires that all packets sent through the wireless network of department A should be monitored.

Figure 10-14 Networking diagram of configuring a remote mirroring server



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure a static route to ensure that there are reachable routes between the AP and monitoring server.
2. Configure remote port mirroring to send the packets mirrored on the mirrored port to the monitoring device through the Layer 3 IP network.

Procedure

Step 1 Configure IP addresses for interfaces.

Add the Layer 2 physical interface and BSS interface of the AP to a VLAN and configure an IP address for the VLANIF interface.

```
<Huawei> system-view
[Huawei] sysname AP
[AP] vlan batch 100 to 101
[AP] interface gigabitethernet 0/0/1
[AP-GigabitEthernet0/0/1] port link-type trunk
[AP-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
[AP-GigabitEthernet0/0/1] quit
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] port hybrid pvid vlan 100
[AP-Wlan-Bss1] port hybrid untagged vlan 100
[AP-Wlan-Bss1] quit
[AP] interface vlanif 101
[AP-Vlanif101] ip address 192.168.100.1 24
[AP-Vlanif101] quit
[AP] interface vlanif 100
[AP-Vlanif100] ip address 192.168.1.1 24
[AP-Vlanif100] quit
```

Assign IP addresses to all interfaces of RouterB.

```
<Huawei> system-view
[Huawei] sysname RouterB
[RouterB] interface ethernet 1/0/0
[RouterB-Ethernet1/0/0] ip address 192.168.2.1 24
[RouterB-Ethernet1/0/0] quit
[RouterB] interface ethernet 1/0/1
[RouterB-Ethernet1/0/1] ip address 192.168.101.1 24
[RouterB-Ethernet1/0/1] quit
```

Configure the default route for the AP.

```
[AP] ip route-static 0.0.0.0 0.0.0.0 192.168.100.2
```

Configure the default route for RouterB.

```
[RouterB] ip route-static 0.0.0.0 0.0.0.0 192.168.101.2
```

Step 2 Configure a remote observing server.

Configure a remote observing server on the AP.

```
[AP] observe-server destination-ip 192.168.2.2 source-ip 192.168.1.1
```

Step 3 Configure a mirrored port.

Configure WLAN-BSS1 as a mirrored port on the AP to monitor the packets sent by the department.

```
[AP] interface wlan-bss 1
[AP-Wlan-Bss1] mirror to observe-server inbound
[AP-Wlan-Bss1] quit
[AP] quit
```

Step 4 Verify the configuration.

Check the configuration of the observing server.

```
<AP> display observe-server
  ------------------------------------------------------------------------
  Index          : 1
  destination-ip : 192.168.2.2
  source-ip      : 192.168.1.1
  dscp           : 0
  Used           : 1
  ------------------------------------------------------------------------
```

Check the configuration of the mirrored port.

```
<AP> display mirror-port
  ------------------------------------------------------------------------------
    Mirror-port           Direction  Observe-dest
  ------------------------------------------------------------------------------
  1 Wlan-Bss1             Inbound    DIP:192.168.2.2 SIP:192.168.1.1 DSCP:0
  ------------------------------------------------------------------------------
```

----End

Configuration Files

- Configuration file of the AP

```
#
 sysname AP
#
vlan batch 100 to 101
#
dhcp enable
#
 observe-sever destination-ip 192.168.2.2 source-ip 192.168.1.1
#
interface Vlanif100
 ip address 192.168.1.1 255.255.255.0
#
interface Vlanif101
 ip address 192.168.100.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface Wlan-Bss1
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 mirror to observe-server inbound
#
ip route-static 0.0.0.0 0.0.0.0 192.168.100.2
#
wlan
 wmm-profile name wmm id 1
 traffic-profile name traffic id 1
 security-profile name security id 1
 service-set name test id 1
  Wlan-Bss 1
  ssid test
  traffic-profile id 1
  security-profile id 1
```

```
 radio-profile name radio id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/1
 radio-profile id 1
 service-set id 1 wlan 1
#
return
```

- Configuration file of RouterB

```
#
 sysname RouterB
#
interface Ethernet1/0/0
 ip address 192.168.2.1 255.255.255.0
#
interface Ethernet1/0/1
 ip address 192.168.101.1 255.255.255.0
#
ip route-static 0.0.0.0 0.0.0.0 192.168.101.2
#
return
```

10.4 LLDP Configuration

The Link Layer Discovery Protocol (LLDP) allows you to obtain details about the network topology, changes in the topology, and detect incorrect configurations on the network.

10.4.1 LLDP Overview

This section describes the definition and purpose of LLDP.

Definition

The Link Layer Discovery Protocol (LLDP) is a standard Layer 2 topology discovery protocol defined in IEEE 802.1ab. LLDP collects local device information including the management IP address, device ID, and port ID and advertises the information to neighbors. Neighbors save the received information in their management information bases (MIBs). The network management system (NMS) can use data in MIBs to query the link status.

Purpose

An NMS must be capable of managing multiple network devices with diverse functions and complex configurations. Most NMSs can detect Layer 3 network topologies, but they cannot detect detailed Layer 2 topologies or detect configuration conflicts. A standard protocol is required to exchange Layer 2 information between network devices.

The LLDP protocol provides a standard link-layer discovery method. Layer 2 information obtained from LLDP allows the NMS to detect the topology of neighboring devices, and display paths between clients, switches, routers, application servers, and network servers. The NMS can also detect configuration conflicts between network devices and identify causes of network failures. Enterprise users can use an NMS to monitor the link status on devices running LLDP and quickly locate network faults.

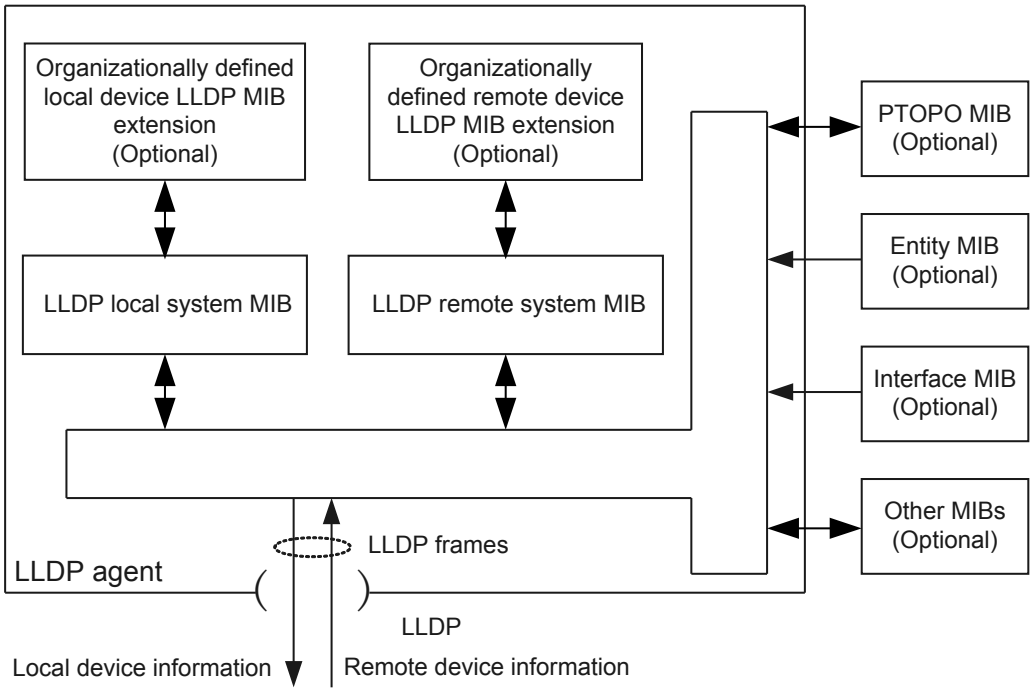
10.4.2 Principles

This section describes the implementation of LLDP.

10.4.2.1 LLDP Implementation

LLDP collects and sends local device information to remote devices, and the local device saves information received from remote devices to standard MIBs. **Figure 10-15** shows how LLDP is implemented.

Figure 10-15 LLDP block diagram



LLDP is implemented as follows:

1. The LLDP module uses an LLDP agent to interact with the Physical Topology MIB, Entity MIB, Interfaces MIB, and other MIBs to update the LLDP local system MIB and LLDP local organizationally defined extended MIB.
2. The LLDP agent encapsulates local device information in LLDP frames and sends the LLDP frames to remote devices.
3. After receiving LLDP frames from remote devices, the LLDP agent updates the LLDP remote system MIB and LLDP remote organizationally defined extended MIB.
4. By exchanging LLDP frames with remote devices, the local device can obtain information about remote devices, including remote interfaces connected to the local device and MAC addresses of remote devices.

The LLDP local system MIB stores local device information, including the device ID, port ID, system name, system description, port description, and management address.

The LLDP remote system MIB stores neighbor information, including the device ID, port ID, system name, system description, port description, and management address of each neighbor.

An LLDP agent performs the following tasks:

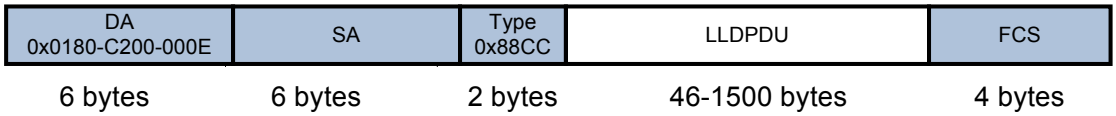
- Maintains the LLDP local system MIB and LLDP remote system MIB.

- Obtains and sends LLDP local system MIB information to remote devices when the local device status changes. An LLDP agent also obtains and sends LLDP local system MIB information to remote devices at periodic intervals if the local device status does not change.
- Identifies and processes received LLDP frames.
- Sends LLDP traps to the NMS when information in the LLDP local system MIB or LLDP remote system MIB changes.

10.4.2.2 LLDP Frame Format

An LLDP frame is an Ethernet frame encapsulated with an LLDP data unit (LLDPDU). **Figure 10-16** shows the LLDP frame format.

Figure 10-16 LLDP frame format



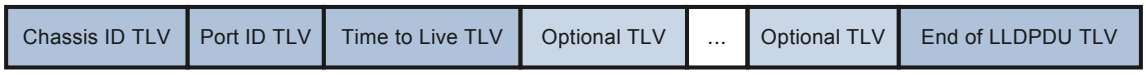
An LLDP frame contains the following fields:

- DA: destination MAC address, a fixed multicast MAC address 0x0180-C200-000E.
- SA: source MAC address, the MAC address of the sender
- Type: packet type, 0x88CC in LLDP frames.
- LLDPDU: LLDP data unit, body of an LLDP frame.
- FCS: frame check sequence.

LLDPDU

An LLDPDU contains local device information and is encapsulated in an LLDP frame. Each LLDPDU consists of several information elements known as TLVs that each includes Type, Length, and Value fields. The local device encapsulates its local information in TLVs, constructs an LLDPDU with several TLVs, and encapsulates the LLDPDU in the data field of an LLDP frame. **Figure 10-17** shows the LLDPDU structure.

Figure 10-17 LLDPDU structure



As shown in **Figure 10-17**, an LLDPDU has four mandatory TLVs: Chassis ID TLV, Port ID TLV, Time to Live TLV, and End of LLDPDU TLV. Other TLVs are optional, and a device can determine whether to encapsulate them in an LLDPDU.

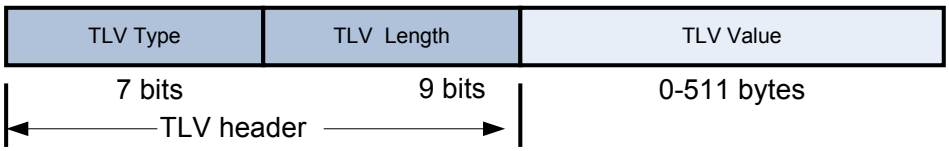
When LLDP is disabled on an interface or an interface is shut down, the interface sends a shutdown LLDPDU to the neighbors. In the shutdown LLDPDU, the value of the Time to Live TLV is 0. A shutdown LLDPDU contains no optional TLVs.

TLV Structure

An LLDPDU is formed by TLVs, and each TLV is an information element.

Figure 10-18 shows the structure of a TLV.

Figure 10-18 TLV structure



A TLV contains the following fields:

- TLV Type (7 bits): type of a TLV. Each TLV type has a unique value. For example, the value of End of LLDPDU TLV is 0, and the value of Chassis ID TLV is 1.
- TLV Length (9 bits): size of a TLV.
- TLV Value (0-511 bytes): The first bit indicates the sub-type of a TLV, and the other bits are the TLV content.

TLV Type

LLDPDUs can encapsulate basic TLVs, TLVs defined by IEEE 802.1 working groups, TLVs defined by IEEE 802.3 working groups, and Media Endpoint Discovery (MED) TLVs. Basic TLVs are used for basic device management. The TLVs defined by IEEE 802.1 and IEEE 802.3 working groups, and MED TLVs defined by other organizations are used for enhanced device management functions. A device determines whether to encapsulate organizationally specific TLVs.

- Basic TLVs

  Four basic TLVs are mandatory in LLDP implementation and must be encapsulated in an LLDPDU.

  Table 10-10 Basic TLVs

TLV	Description	Mandatory
Chassis ID TLV	Bridge MAC address of the device sending an LLDPDU.	Yes

TLV	Description	Mandatory
Port ID TLV	Port from which an LLDPDU is sent. ● If an LLDPDU does not contain any MED TLVs, the Port ID TLV identifies the port name. ● If an LLDPDU contains a MED TLV, the Port ID TLV identifies the port MAC address. If the port has no MAC address, the Port ID TLV identifies the bridge MAC address.	Yes
Time To Live TLV	Time to live (TTL) of the local device information stored on the neighbor device.	Yes
End of LLDPDU TLV	End of an LLDPDU.	Yes
Port Description TLV	Character string that describes the port sending an LLDPDU.	No
System Name TLV	System name.	No
System Description TLV	Character string that describes the system.	No
System Capabilities TLV	Main functions of the system and the functions that have been enabled.	No
Management Address TLV	Address used by the NMS to identify and manage the local device. Management IP addresses uniquely identify network devices, facilitating layout of the network topology and network management.	No

- TLVs defined by the IEEE 802.1 working group

Table 10-11 TLVs defined by the IEEE 802.1 working group

TLV	Description
Port VLAN ID TLV	VLAN ID of a port.
Port And Protocol VLAN ID TLV	Protocol VLAN ID of a port.
VLAN Name TLV	Name of the VLAN on a port.
Protocol Identity TLV	Protocol types that a port supports.

- TLVs defined by the IEEE 802.3 working group

Table 10-12 TLVs defined by the IEEE 802.3 working group

TLV	Description
Link Aggregation TLV	Whether a port supports link aggregation and has link aggregation enabled.
MAC/PHY Configuration/ Status TLV	Rate and duplex mode of a port, whether the port supports auto-negotiation, and whether auto-negotiation is enabled on the port.
Maximum Frame Size TLV	Maximum frame length that a port supports. The value is the maximum transmission unit (MTU) of the port.
Power Via MDI TLV	Power capabilities of a port, for example, whether a port supports PoE and whether a port supplies or demands power.

10.4.2.3 Transmission and Reception Mechanisms

LLDP frame transmission

After LLDP is enabled on a device, the device periodically sends LLDP frames to neighbors. When the local configuration changes, the device sends LLDP frames to notify neighbors of the changes. To reduce the number of LLDP frames sent when the local information changes frequently, the device waits for a period before sending the next LLDP frame.

LLDP frame reception

An LLDP-capable device checks the validity of received LLDP frames and the TLVs in those frames. When determining that an LLDP frame and its TLVs are valid, the local device saves neighbor information and sets the aging time of neighbor information on the local device to the TTL value carried in the received LLDPDU. If the TTL value carried in the received LLDPDU is 0, the neighbor information ages out immediately.

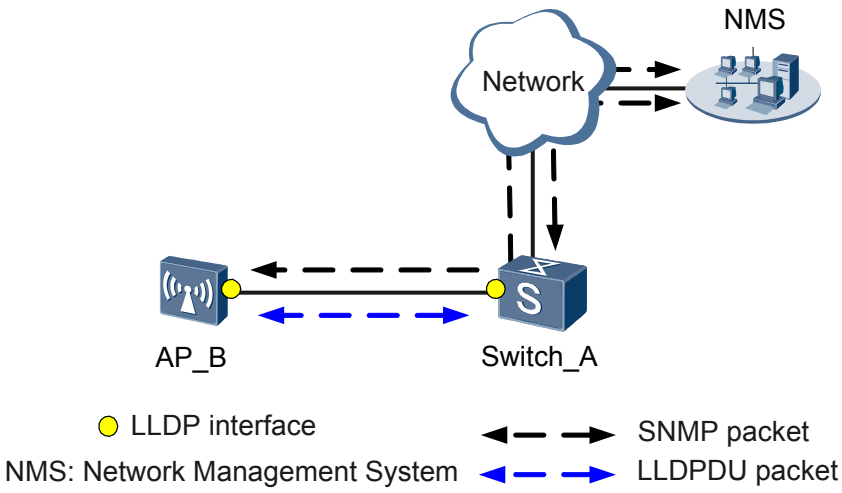
10.4.2.4 LLDP Networking

LLDP has the following networking modes:

- Single-neighbor networking

  In this networking, interfaces between two devices are directly connected, and each interface has only one neighbor. As shown in **Figure 10-19**, Switch_A is directly connected to AP_B. Each interface on Switch_A and AP_B has only one neighbor.

Figure 10-19 Single-neighbor networking



10.4.3 Default Configuration

This section describes the default LLDP configuration.

Table 10-13 describes the default LLDP configuration.

Table 10-13 Default LLDP configuration

Parameter	Default Setting
LLDP	Disabled globally
Interval between sending LLDP packets	30 seconds
Delay in sending LLDP packets	2 seconds
Hold time multiplier of device information on neighbors	4
Delay in initializing interfaces	2 seconds
Delay in sending a notification after neighbor information changes	5 seconds
Type of the type-length-values (TLVs) that an interface can send	All types of TLVs except the Location Identification TLV
Standard with which the 802.3 Power via MDI TLV sent by the interface complies	802.1 ab

10.4.4 Configuring the LLDP

10.4.4.1 Configuring Basic LLDP Functions

When LLDP is configured on devices, the NMS can obtain detailed information such as the network topology, device interface status, and management address.

Pre-configuration Tasks

Before configuring LLDP, ensure that the local device and NMS are reachable to each other, and configure the Simple Network Management Protocol (SNMP).

10.4.4.1.1 Enabling LLDP

Context

The LLDP function enables a device to send LLDP packets with local system status information to neighbors and parse LLDP packets received from neighbors. The NMS obtains Layer 2 connection status from the device to analyze the network topology.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
lldp enable
```

LLDP is enabled globally.

By default, LLDP is disabled globally.

----End

10.4.4.1.2 (Optional) Disabling LLDP on an Interface

Context

LLDP can be enabled in the system view and the interface view.

- When LLDP is enabled in the system view, LLDP is enabled on all interfaces.
- When LLDP is disabled in the system view, LLDP is disabled on all interfaces.
- An interface can send and receive LLDP packets only after LLDP is enabled in both the system view and the interface view.
- After LLDP is disabled globally, the commands for enabling and disabling LLDP on an interface do not take effect.
- If LLDP needs to be disabled on some interfaces, enable LLDP globally first, and run the **undo lldp enable** command on these interfaces. To re-enable LLDP on these interfaces, run the **lldp enable** command in the views of these interfaces.

NOTE

- Only physical interfaces support LLDP. Logical interfaces such as the VLANIF interfaces do not support LLDP.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run:

```
undo lldp enable
```

LLDP is disabled on the interface.

----End

10.4.4.1.3 (Optional) Configuring an LLDP Management IP Address

Context

The management address of a device is carried in the Management Address TLV field of the LLDP packet. The NMS uses management addresses to identify and manage devices.

If no management address is configured or the configured management address is invalid, the system sets an IP address in the address list as the management address. The system selects the IP address in the following sequence: loopback interface address, and VLANIF interface address. Among the IP addresses of the same type, the system selects the smallest one. If the system does not find a management IP address, the bridge MAC address is used as the management address.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
lldp management-address ip-address
```

The LLDP management address is configured.

The value of *ip-address* must be a valid unicast IP address existing on the device.

----End

10.4.4.1.4 (Optional) Configuring LLDP Time Parameters

Context

Interval between sending LLDP packets

When the LLDP status of the device keeps unchanged, the device sends LLDP packets to the neighbors at a certain interval.

Consider the value of *delay* when adjusting the value of *interval* because it is restricted by the value of *delay*.

- The value of *interval* ranges from 5 to 32768. Increasing the value of *interval* is not restricted by the value of *delay*.
- The value of *interval* must be equal to or greater than four times the value of *delay*. Therefore, if you want to set *interval* to be smaller than four times the value of *delay*, first reduce the *delay* value to be equal to or smaller than a quarter of the new *interval* value, and then reduce the *interval* value.

Delay in sending LLDP packets

There is a delay before the device sends an LLDP packet to the neighbor when the device status changes frequently.

Consider the value of *interval* when adjusting the value of *delay* because it is restricted by the value of *interval*.

- The value of *delay* ranges from 1 to 8192. Decreasing the value of *delay* is not restricted by the value of *interval*.
- The value of *delay* must be smaller than or equal to a quarter of *interval*. Therefore, if you want to set *delay* to be greater than a quarter of *interval*, first increase the *interval* value to four times the new *delay* value, and then increase the *delay* value.

Hold time multiplier of device information on neighbors

The hold time multiplier is used to calculate the Time to Live (TTL), which determines how long information about a device can be saved on the neighbors. You can specify the hold time of device information on the neighbors. After receiving an LLDP packet, a neighbor updates the aging time of the device information from the sender based on the TTL.

The storage time calculation formula is: TTL = Min (65535, (*interval* x *hold*)).

- TTL is the hold time of device information. It is the smaller value between 65535 and (*interval* x *hold*).
- *interval* indicates the interval at which the device sends LLDP packets to neighbors.
- *hold* indicates the hold time multiplier of device information on neighbors. The value ranges from 2 to 10.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
lldp message-transmission interval interval
```

The interval between sending LLDP packets is set.

The default interval between sending LLDP packets is 30 seconds.

Step 3 Run:

```
lldp message-transmission delay delay
```

The delay in sending LLDP packets is set.

The default delay in sending LLDP packets is 2 seconds.

Step 4 Run:

```
lldp message-transmission hold-multiplier hold
```

The hold time multiplier of device information stored on neighbors is set.

The default hold time multiplier is 4.

----End

10.4.4.1.5 (Optional) Configuring the Delay in Initializing Interfaces

Context

The delay in initializing interfaces is the delay before LLDP is re-enabled on an interface. The delay suppresses the topology flapping caused by the frequent LLDP status changes.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
lldp restart-delay delay
```

The delay in initializing interfaces is set.

The default delay is 2 seconds.

----End

10.4.4.1.6 (Optional) Configuring the Type of TLVs that an Interface Can Send

Context

LLDPDUs can encapsulate basic TLVs, TLVs defined by IEEE 802.1 working groups, TLVs defined by IEEE 802.3 working groups.

NOTE

- When the supported TLVs are basic TLVs, TLVs in the IEEE 802.1 format, and TLVs in the IEEE 802.3 format, the **lldp tlv-enable** command with the **all** parameter advertises all TLVs.

  If the **all** parameter is not specified, only one type of TLV can be sent. To send multiple types of TLVs, run this command multiple times.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
interface interface-type interface-number
```

The interface view is displayed.

Step 3 Run the following commands to set the type of TLVs to be advertised on the interface:

- Run:
  ```
  lldp tlv-enable basic-tlv { all | management-address | port-description | system-capability | system-description | system-name }
  ```
  The interface is configured to advertise basic TLVs.
- Run:
  ```
  lldp tlv-enable dot1-tlv { all | port-vlan-id | protocol-vlan-id [ vlan-id ] | vlan-name [ vlan-id ] | protocol-identity }
  ```
  The interface is configured to advertise TLVs defined by the IEEE 802.1 working group.
- Run:
  ```
  lldp tlv-enable dot3-tlv { all | link-aggregation | mac-physic | max-frame-size | power }
  ```
  The interface is configured to advertise the TLVs advertised by the IEEE 802.3 working group.

By default, an interface advertises all types of TLVs except the Location Identification TLV.

Step 4 Run:

```
lldp dot3-tlv power { 802.1ab | 802.3at }
```

The standard with which the 802.3 Power via MDI TLV sent by the interface complies is set.

By default, the 802.3 Power via MDI TLV conforms to 802.1 ab.

NOTE

Before selecting a format of the 802.3 Power via MDI TLV, you must know the TLV format supported by the neighbors. The TLV format on the local device must be also supported by the neighbors.

----End

10.4.4.1.7 Checking the Configuration

Procedure

- Run the **display lldp local** [**interface** *interface-type interface-number*] command to view LLDP local information on a specified interface or all interfaces.
- Run the **display lldp neighbor** [**interface** *interface-type interface-number*] command to view neighbor information in the system or on an interface.
- Run the **display lldp neighbor brief** command to view brief information about neighbors.

- Run the **display lldp tlv-config** [**interface** *interface-type interface-number*] command to view TLV types supported by the entire system or an interface.

----End

10.4.4.2 Configuring the LLDP Alarm Function

This section describes how to configure the LLDP alarm function on a network device, so that the device can send alarms to the NMS when information about neighbors changes.

Pre-configuration Tasks

Before configuring the LLDP alarm function, complete the following task:

- Configuring reachable routes between devices and the NMS, and SNMP parameters

10.4.4.2.1 Setting the Delay in Sending Traps About Neighbor Information Changes

Context

There is a delay before the device sends LLDP traps about neighbor information changes to the NMS. When neighbor information changes frequently, extend the delay to prevent the device from sending traps to the NMS too frequently. This suppresses the topology flapping.

The configured delay applies only to the trap, which reports changes in neighbor information, including the number of added neighbors, number of deleted neighbors, number of neighbors that are aged out, and number of neighbors of which the information is deleted.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
lldp trap-interval interval
```

The delay in sending neighbor change traps to the NMS is set.

The default delay in sending neighbor change traps to the NMS is 5 seconds.

----End

10.4.4.2.2 Enabling the LLDP Trap Function

Context

After the LLDP trap function is enabled, the device sends traps to the NMS in one of the following cases:

- The LLDP function is enabled or disabled globally.
- The local management address changes.

- Neighbor information changes. No trap is generated if the management address of a neighbor changes.

NOTE

- The LLDP trap function applies to all interfaces. The LLDP trap function takes effect no matter whether LLDP is enabled globally.
- If the network topology is unstable, disable the LLDP trap function to prevent frequent trap sending.
- To set the interval between sending neighbor change traps to the NMS, run the **lldp trap-interval** commands. If neighbor information changes frequently, extend the interval to reduce the number of traps. In this way, network topology flapping is suppressed.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
snmp-agent trap enable feature-name lldptrap [ trap-name { hwlldpdisabled | hwlldpenabled | hwlldplocmanipaddrchange | lldpremtableschange } ]
```

The LLDP trap function is enabled.

By default, the LLDP trap function is enabled.

----End

10.4.4.2.3 Checking the Configuration

Procedure

- Run the **display snmp-agent trap feature-name lldptrap all** command to view status of all traps on the LLDP module.
- Run the **display lldp local** [**interface** *interface-type interface-number*] command to view LLDP status in the system or on an interface.

----End

10.4.5 Maintenance LLDP

This section describes how to clear LLDP statistics and monitor LLDP status.

10.4.5.1 Clearing LLDP Statistics

Context

NOTICE

Statistics cannot be restored after being cleared. Therefore, exercise caution when you run the following commands.

Procedure

- Run the **reset lldp statistics** [**interface** *interface-type interface-number*] command in the user view to clear LLDP packet statistics in the system or on an interface.
- Run the **lldp clear neighbor** [**interface** *interface-type interface-number*] command in the user view to clear neighbor information in the system or on an interface.

----End

10.4.5.2 Monitoring LLDP Status

Context

In routine maintenance, you can run the following commands in any view to check the LLDP status.

Procedure

- Run the **display lldp statistics** [**interface** *interface-type interface-number*] command to view statistics about sent and received LLDP packets in the system or on an interface.

----End

10.4.6 References

This section lists references of LLDP.

The following table lists the references for this document.

Document	Description	Remarks
IEEE 802.1ab	IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity Discovery	-
IEEE 802.3at	802.3at Data Terminal Equipment(DTE) Power via the Media Dependent Interface(MDI) Enhancements	-

10.5 Packet Capture Configuration

This section describes the concept and configuration of the packet capture function.

NOTE

Based on your requirements to detect failures in telecom transmission, this feature may collect or store some communication information about specific customers. Huawei cannot offer services to collect or store this information unilaterally. Before enabling the function, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.

10.5.1 Packet Capture Overview

The packet capture function captures packets matching the specified rules. This function improves network maintenance efficiency and reduces maintenance costs.

As Internet develops, devices on a network transmit various services, and network administrators often need to capture packets on devices to locate faults. The packet capturing function allows devices to capture received packets for fault location. This function simplifies the configurations of packet analysis device and network monitoring device.

After the packet capturing function is enabled, the devices capture the packets matching certain conditions. The maintenance personnel can run commands to view information about captured packets or save the captured packets to the local storage media as *.cap files. The saved files can be downloaded for fault analysis. This function greatly improves maintenance efficiency and reduces maintenance costs.

10.5.2 Configuring the Device to Capture Packets

If the device fails to forward traffic correctly, configure the packet capture function to capture service packets for analysis. This allows the device to process invalid packets in time, ensuring that network data can be transmitted correctly.

Context

You can configure ACL rules to capture packets matching a specified ACL.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
capture-packet interface interface-type interface-number [ acl acl-number ]
destination { terminal | file file-name } * [ car cir car-value | time-out time |
packet-num number | packet-len length ] *
```

The device is configured to capture packets.

NOTE

- The packet capture configuration is not saved in the configuration file, and becomes invalid when packet capture is complete.
- The device can capture only upstream packets and cannot capture downstream packets.
- Before using the **capture-packet** command again, wait until the last command execution is complete.
- The system limits the rate of captured packets. If the rate of packets exceeds the limit, some packets may be discarded.
- You can set the timeout period specified by *time* and the number of packets to be captured specified by *number* for a capture instance. If the timeout period expires or the specified number of packets are captured, the system stops capturing packets.
- You can set packet capture parameters based on the number of packets on the interface. If a large number of packets are forwarded on an interface, set the *time* parameter to a small value and the *number* parameter to a large value. If a small number of packets are forwarded on an interface, set the *time* parameter to a large value and the *number* parameter to a small value.

----End

10.6 Service Diagnosis Configuration

The service diagnosis function monitors user status changes and protocol processing during user access and exports the monitored information to a terminal or server. Maintenance personnel can refer to and analyze the monitored information to locate user access faults.

10.6.1 Service Diagnosis Overview

Service diagnosis is a method for debugging and checking services and is used by maintenance personnel to locate faults occurred during the user access process.

Service diagnosis allows maintenance personnel to create a diagnosis object using command lines. When a user matching attributes of the diagnosis object gets online, the access point automatically creates a diagnosis instance for the user based on the diagnosis object and monitors and exports instance information including status changes and protocol processing during user access.

A diagnosis object is a database of users with some same attributes. For example, all users on an interface card can be defined as a diagnosis object. A diagnosis instance is created based on a diagnosis object and maps a user.

A diagnosis object has one or multiple of the following attributes:

- Interface number
- VLAN ID
- Access mode
- User name
- IP address
- MAC address

Multiple users may get online or offline simultaneously and debugging information about a specified user cannot be displayed. Therefore, it is difficult to locate faults during user access based on debugging information on existing networks. Maintenance personnel need to capture information about services of a specified user.

The service diagnosis function of the access point meets this requirement.

Currently, the access point supports diagnosis for Dynamic Host Configuration Protocol (DHCP), Network Admission Control (NAC), and Authentication, Authorization and Accounting (AAA) services. The access point diagnoses and exports complete key information about exchanges between modules during user access. This helps maintenance personnel know about service implementation and locate and rectify service faults based on the information. Table 10-14 describes key information about exchanges between modules during service diagnosis.

Table 10-14 Key information about exchanges between modules during service diagnosis

Service		Key Exchange Information
DHCP	DHCP server	IP address allocation, release, and lease.
	DHCP relay agent	IP address request, release, and lease between the DHCP client and server.
	DHCP snooping	IP address request, release, lease, and adding or deleting of dynamic DHCP snooping binding entries.
AAA		User access, authentication, authorization, and accounting. **NOTE** Service diagnosis supports only common AAA users.
NAC		User access, authentication, authorization, and accounting.

10.6.2 Configuring Service Diagnosis

When locating faults of DHCP, NAC, or AAA service during user access, maintenance personnel can create diagnosis objects to diagnose services and locate the faults.

Context

NOTICE

Service diagnosis affects system performance. Therefore, enable service diagnosis only when fault locating is required. After locating faults, immediately run the **undo trace enable** command to disable service diagnosis.

Users with different services have different attributes. Create diagnosis objects for different services based on different attributes.

- DHCP service: based on the MAC address.
- NAC and AAA services: based on the MAC address, IP address, user name, user VLAN ID, access mode, or interface number.

NOTE

The configurations of the **trace enable** and **trace syslog source** commands are not recorded in the configuration file. After the device restarts, run these commands again to make service diagnosis take effect.

Procedure

Step 1 Run:

```
system-view
```

The system view is displayed.

Step 2 Run:

```
trace enable [ brief ]
```

Service diagnosis is enabled.

By default, service diagnosis is disabled.

- The **trace enable brief** command configures the device to output brief service diagnosis information.
- The **trace enable** command configures the device to output detailed service diagnosis information.

Step 3 Run:

```
trace object { mac-address mac-address | ip-address ip-address | interface interface-type interface-number | user-vlan user-vlan-id | user-name user-name | access-mode { dot1x | mac-authen | portal | wlan } } * [ output { command-line | file file-name | syslog-server syslog-server-ip } ]
```

A diagnosis object is created.

By default, no diagnosis object is created. If you do not specify the direction at which information is exported, the default direction is the CLI.

NOTE

It is recommended that you export the diagnosis information to a specified file.

The diagnosis output file cannot exceeds 1 MB. The excessive diagnosis information is not recorded.

Step 4 (Optional) Run:

```
save trace information
```

Diagnosis information in the device buffer is saved as a file.

When you specify the device to export diagnosis information as a file, to view real-time diagnosis information, save diagnosis information in the buffer area as a file.

Step 5 (Optional) Run:

```
trace syslog source interface-type interface-number
```

An interface is configured for exporting diagnosis information to a log server.

By default, no interface is specified to export diagnosis information to a log server.

When you specify the device to export diagnosis information to a log server, configure an interface for exporting diagnosis information to the log server.

Step 6 (Optional) Run:

```
undo trace enable
```

The service diagnosis function is disabled.

NOTICE

Service diagnosis affects system performance. Therefore, enable service diagnosis only when fault locating is required. After locating faults, immediately run the **undo trace enable** command to disable service diagnosis.

----End

Checking the Configuration

- Run the **display trace information** command to view information about service diagnosis.
- Run the **display trace instance** [*instance-start-id* [*instance-end-id*] | **mac-address** *mac-address* | **ip-address** *ip-address* | **interface** *interface-type interface-number* | **cid** *cid*] command to view diagnosis instances on the device.
- Run the **display trace object** [*service-object-id*] command to view the configuration about a diagnosis object.

10.6.3 Maintaining Service Diagnosis

This section describes how to clear all diagnosis instances on a device.

Context

After service diagnosis is enabled and a diagnosis object is created on a device, the device creates a diagnosis instance when a user matching the attributes of the diagnosis object gets online. If the device diagnoses services of multiple users, it creates a diagnosis instance for each user, which occupies a large amount of system resources. Therefore, the device automatically deletes diagnosis instances when corresponding users get offline. The service diagnosis module may fail to detect that some users are offline because these users got offline abnormally. The diagnosis instances created for these users are not deleted and occupy system resources. The device provides an aging mechanism for service diagnosisg. When the aging time is reached, the device automatically deletes diagnosis instances to reclaim resources.

In addition to the preceding two methods you can run the **reset trace instance** command to clear all the diagnosis instances on the device.

NOTICE

After all the diagnosis instances are cleared using the **reset trace instance** command, properly running diagnosis instances are also deleted. Exercise caution when you run the **reset trace instance** command.

Procedure

- Run the **reset trace instance** command to clear all diagnosis instances on the device.

----End