HP 5500 EI & 5500 SI Switch Series

Fundamentals

Configuration Guide

Part number: 5998-1707
Software version: Release 2220
Document version: 6W100-20130810

Legal and notice information

The information contained herein is subject to change without notice.

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

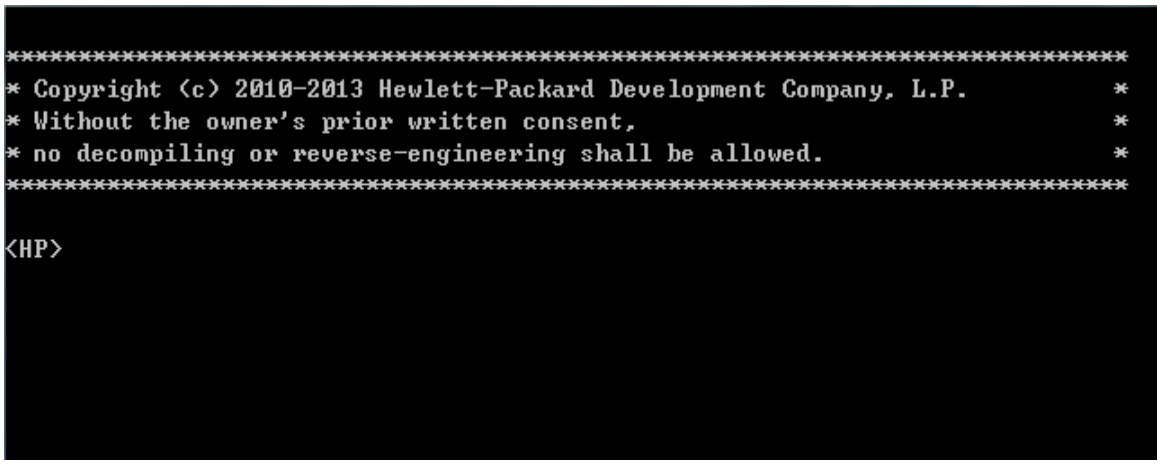
The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Contents

Using the CLI

At the command-line interface (CLI), you can enter text commands to configure, manage, and monitor your device.

Figure 1 CLI example



Logging in to the CLI

You can log in to the CLI in a variety of ways. For example, you can log in through the console port, or by using Telnet or SSH. For more information about login methods, see "Logging in to the CLI."

Command conventions

Command conventions help you understand the syntax of commands. Commands in product manuals comply with the conventions listed in Table 1.

Table 1 Command conventions

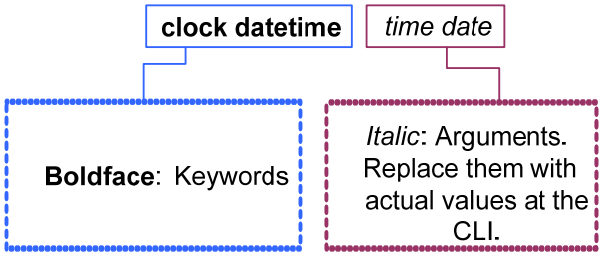
Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.

Convention	Description
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

Command keywords are case insensitive.

The following example analyzes the syntax of the **clock datetime** *time date* command according to Table 1.

Figure 2 Understanding command-line parameters



For example, to set the system time to 10:30:20, February 23, 2011, enter the following command line at the CLI and press **Enter**:

```
<Sysname> clock datetime 10:30:20 2/23/2011
```

Using the undo form of a command

Most configuration commands have an **undo** form for canceling a configuration, restoring the default, or disabling a feature. For example, the **info-center enable** command enables the information center, and the **undo info-center enable** command disables the information center.

CLI views

Commands are grouped in different views by function. To use a command, you must enter the view of the command.

CLI views are organized in a hierarchical structure, as shown in Figure 3. Each view has a unique prompt, from which you can identify where you are and what you can do. For example, the prompt `[Sysname-vlan100]` shows that you are in the view of VLAN 100 and can configure attributes for the VLAN.

You are placed in user view immediately after you are logged in to the CLI. The user view prompt is <*Device-name*>, where the *Device-name* argument defaults to **Sysname** and can be changed by using the **sysname** command. In user view, you can perform some basic operations, including display, debug, file management, FTP, Telnet, clock setting, and reboot. For more information about the **sysname** command, see *Fundamentals Command Reference*.

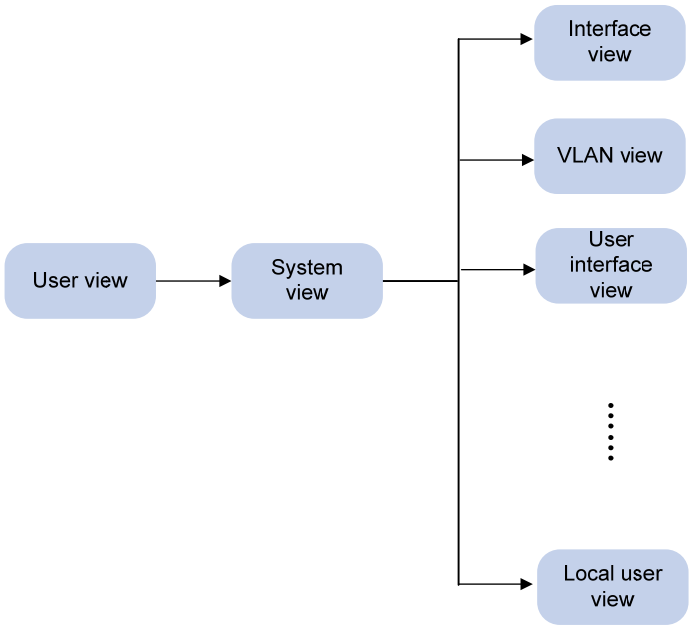
From user view, you can enter system view to configure global settings, including the daylight saving time, banners, and hotkeys. The system view prompt is [*Device-name*].

From system view, you can enter different function views. For example, you can enter interface view to configure interface parameters, enter VLAN view to add ports to the specific VLAN, enter user interface

view to configure login user attributes, or create a local user and enter local user view to configure attributes for the local user.

To display all commands available in a view, enter a question mark (?) at the view prompt.

Figure 3 CLI view hierarchy



Entering system view from user view

Task	Command
Enter system view from user view.	**system-view**

Returning to the upper-level view from any view

Task	Command
Return to the upper-level view from any view.	**quit**

Executing the **quit** command in user view terminates your connection to the device.

NOTE:

In public key code view, use the **public-key-code end** command to return to the upper-level view (public key view). In public key view, use the **peer-public-key end** command to return to system view.

Returning to user view from any other view

You can return to user view from any other view by using the **return** command, instead of using the **quit** command repeatedly. Pressing **Ctrl+Z** has the same effect.

To return to user view from any other view:

Task	Command
Return to user view.	**return**

Accessing the CLI online help

The CLI online help is context sensitive. You can enter a question mark at any point of a command to display all available options.

To access the CLI online help, use one of the following methods:

- Enter a question mark at a view prompt to display the first keywords of all commands available in the view. For example:

```
<Sysname> ?
User view commands:
  archive           Specify archive settings
  backup            Backup next startup-configuration file to TFTP server
  boot-loader       Set boot loader
  bootrom           Update/read/backup/restore bootrom
  brand             Set Original Equipment Manufacturer (BRAND) information
  cd                Change current directory
...
```

- Enter some keywords of a command and a question mark separated by a space to display available keywords and arguments.
  - Example 1: The question mark is in the place of a keyword, and the CLI displays all possible keywords with a brief description for each keyword.

```
<Sysname> terminal ?
  debugging  Send debug information to terminal
  logging    Send log information to terminal
  monitor    Send information output to current terminal
  trapping   Send trap information to terminal
```

  - Example 2: The question mark is in the place of an argument, and the CLI displays the description of the argument.

```
<Sysname> system-view
[Sysname] interface vlan-interface ?
  <1-4094>  VLAN interface
[Sysname] interface vlan-interface 1 ?
  <cr>
[Sysname] interface vlan-interface 1
```

    The string **<cr>** indicates that the command is complete, and you can press **Enter** to execute the command.

- Enter an incomplete keyword string followed by a question mark to display all keywords starting with the string. For example:

```
<Sysname> f?
  fixdisk
  format
  free
  ftp
```

```
<Sysname> display ftp?
  ftp
  ftp-server
  ftp-user
```

Entering a command

When you enter a command, you can use some keys or hotkeys to edit the command line, or use abbreviated keywords or keyword aliases.

Editing a command line

You can use the keys listed in Table 2 or the hotkeys listed in Table 3 to edit a command line.

Table 2 Keys for editing a command line

Key	Function
Common keys	If the edit buffer is not full, pressing a common key inserts the character at the position of the cursor and moves the cursor to the right.
Backspace	Deletes the character to the left of the cursor and moves the cursor back one character.
Left arrow key or **Ctrl+B**	Moves the cursor one character to the left.
Right arrow key or **Ctrl+F**	Moves the cursor one character to the right.
Tab	If you press **Tab** after entering part of a keyword, the system automatically completes the keyword: • If a unique match is found, the system substitutes the complete keyword for the incomplete one and displays what you entered in the next line. • If there is more than one match, you can press **Tab** repeatedly to choose the keyword you want to enter. • If there is no match, the system does not modify what you entered but displays it again in the next line.

Entering a STRING type value for an argument

Generally, a STRING type argument value can contain any printable character (in the ASCII code range of 32 to 126) other than the question mark (?), quotation mark ("), backward slash (\), and space. However, a specific STRING type argument might have more strict requirements. For example, the domain name is of the STRING type. Invalid characters for it include the vertical bar (|), slash (/), colon (:), asterisk (*), less-than sign (<), greater-than sign (>),and at sign (@), as well as the question mark (?), quotation mark ("), backward slash (\), and space. For more information about the specific requirements for a STRING type argument, see the relevant command reference.

```
<Sysname> system-view
[Sysname] domain ?
  STRING<1-24>  Domain name
```

Abbreviating commands

You can enter a command line quickly by entering incomplete keywords that can uniquely identify the complete command. In user view, for example, commands starting with an **s** include **startup saved-configuration** and **system-view**. To enter system view, you only need to enter **sy**. To set the configuration file to be used at the next startup, you can enter **st s**.

You can also press **Tab** to have an incomplete keyword automatically completed.

Configuring and using command keyword aliases

The command keyword alias function allows you to replace the first keyword of a non-undo command or the second keyword of an **undo** command with your preferred keyword when you execute the command. For example, if you configure **show** as the alias for the **display** keyword, you can enter **show** to execute a **display** command.

Usage guidelines

- After you successfully execute a command by using a keyword alias, the system saves the keyword, instead of its alias, to the running configuration.
- If you press **Tab** after entering part of an alias, the keyword is displayed.
- If a string you entered partially matches a keyword and an alias, the command indicated by the alias is executed. To execute the command indicated by the keyword, enter the complete keyword.
- If a string you entered exactly matches a keyword but partially matches an alias, the command indicated by the keyword is executed. To execute the command indicated by the alias, enter the complete alias.
- If you enter a string that partially matches multiple aliases, the system gives you a prompt.

Configuration procedure

To configure a command keyword alias:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the command keyword alias function.	**command-alias enable**	By default, the command keyword alias function is disabled.
3.	Configure a command keyword alias.	**command-alias mapping** *cmdkey alias*	By default, no command keyword alias is configured. You must enter the *cmdkey* and *alias* arguments in their complete form.

Configuring and using hotkeys

To facilitate CLI operation, the system defines some hotkeys and provides five configurable command hotkeys. Pressing a command hotkey equals entering a command. For system-reserved hotkeys, see Table 3.

To configure hotkeys:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure hotkeys.	**hotkey** { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** } *command*	By default: • **Ctrl+G** is assigned the **display current-configuration** command. • **Ctrl+L** is assigned the **display ip routing-table** command. • **Ctrl+O** is assigned the **undo debugging all** command. No command is assigned to **Ctrl+T** or **Ctrl+U.**
3. Display hotkeys.	**display hotkey** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Optional. Available in any view. See Table 3 for hotkeys reserved by the system.

The hotkeys in Table 3 are defined by the device. If a hotkey is also defined by the terminal software that you are using to interact with the device, the definition of the terminal software takes effect.

Table 3 Hotkeys reserved by the system

Hotkey	Function
Ctrl+A	Moves the cursor to the beginning of the line.
Ctrl+B	Moves the cursor one character to the left.
Ctrl+C	Stops the current command.
Ctrl+D	Deletes the character at the cursor.
Ctrl+E	Moves the cursor to the end of the line.
Ctrl+F	Moves the cursor one character to the right.
Ctrl+H	Deletes the character to the left of the cursor.
Ctrl+K	Aborts the connection request.
Ctrl+N	Displays the next command in the command history buffer.
Ctrl+P	Displays the previous command in the command history buffer.
Ctrl+R	Redisplays the current line.
Ctrl+V	Pastes text from the clipboard.
Ctrl+W	Deletes the word to the left of the cursor.
Ctrl+X	Deletes all characters to the left of the cursor.
Ctrl+Y	Deletes all characters to the right of the cursor.
Ctrl+Z	Returns to user view.
Ctrl+]	Terminates an incoming connection or a redirect connection.
Esc+B	Moves the cursor back one word.
Esc+D	Deletes all characters from the cursor to the end of the word.
Esc+F	Moves the cursor forward one word.

Hotkey	Function
Esc+N	Moves the cursor down one line. This hotkey is available before you press **Enter**.
Esc+P	Moves the cursor up one line. This hotkey is available before you press **Enter**.
Esc+<	Moves the cursor to the beginning of the clipboard.
Esc+>	Moves the cursor to the ending of the clipboard.

Enabling redisplaying entered-but-not-submitted commands

After you enable redisplaying entered-but-not-submitted commands:

- If you entered nothing at the command-line prompt before the system outputs system information such as logs, the system does not display the command-line prompt after the output.
- If you entered some information (except Yes or No for confirmation), the system displays a line break and then display what you have entered after the output.

To enable redisplaying entered-but-not-submitted commands:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable redisplaying entered-but-not-submitted commands.	**info-center synchronous**	By default, the feature is disabled. For more information about this command, see *Network Management and Monitoring Command Reference*.

Understanding command-line error messages

If a command line fails the syntax check, the CLI displays error messages.

Table 4 Common command-line error messages

Error message	Cause
% Unrecognized command found at '^' position.	The keyword in the marked position is invalid.
% Incomplete command found at '^' position.	One or more required keywords or arguments are missing.
% Ambiguous command found at '^' position.	The entered character sequence matches more than one command.
Too many parameters	The entered character sequence contains excessive keywords or arguments.
% Wrong parameter found at '^' position.	The argument in the marked position is invalid.

Using the command history function

The system can automatically save successfully executed commands to the command history buffer for the current user interface. You can view them and execute them again, or set the maximum number of commands that can be saved in the command history buffer.

A command is saved to the command history buffer in the exact format as it was entered. For example, if you enter an incomplete command, the command saved in the command history buffer is also incomplete; if you enter a command by using a command keyword alias, the command saved in the command history buffer also uses the alias.

If you enter a command in the same format repeatedly in succession, the system buffers the command only once. If you enter a command repeatedly in different formats, the system buffers each command format. For example, **display cu** and **display current-configuration** are buffered as two entries but successive repetitions of **display cu** create only one entry in the buffer.

By default, the command history buffer can save up to 10 commands for each user. To set the capacity of the command history buffer for the current user interface, use the **history-command max-size** command.

Viewing history commands

You can use arrow keys to access history commands in Windows 200*x* and Windows XP Terminal or Telnet. In Windows 9*x* HyperTerminal, the arrow keys are invalid, and you must use **Ctrl+P** and **Ctrl+N** instead.

To view command history, use one of the following methods:

Task	Command
Display all commands in the command history buffer.	**display history-command** [| { **begin** | **exclude** | **include** } *regular-expression*]
Display the previous history command.	Up arrow key or **Ctrl+P**
Display the next history command.	Down arrow key or **Ctrl+N**

Setting the command history buffer size for user interfaces

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter user interface view.	**user-interface** { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] }	N/A
3.	Set the maximum number of commands that can be saved in the command history buffer.	**history-command max-size** *size-value*	Optional. By default, the command history buffer can save up to 10 commands.

Controlling the CLI output

This section describes the CLI output control features that help you quickly identify the desired output.

Pausing between screens of output

If the output being displayed is more than will fit on one screen, the system automatically pauses after displaying a screen. By default, up to 24 lines can be displayed on a screen. To change the screen length, use the **screen-length** *screen-length* command. For more information about this command, see *Fundamentals Command Reference*. To control output, use keys in Table 5.

Table 5 Keys for controlling output

Keys	Function
Space	Displays the next screen.
Enter	Displays the next line.
Ctrl+C	Stops the display and cancels the command execution.
<PageUp>	Displays the previous page.
<PageDown>	Displays the next page.

To display all output at one time and refresh the screen continuously until the last screen is displayed:

Task	Command	Remarks
Disable pausing between screens of output for the current session.	**screen-length disable**	The default for a session depends on the setting of the **screen-length** command in user interface view. The default of the **screen-length** command is pausing between screens of output and displaying up to 24 lines on a screen. This command is executed in user view, and takes effect only for the current session. When you relog in to the device, the default is restored.

Filtering the output from a display command

You can use one of the following methods to filter the output from a **display** command:

- Specify the **|** { **begin** | **exclude** | **include** } *regular-expression* option at the end of the command.
- When the system pauses after displaying a screen of output, enter a forward slash (/), minus sign (-), or plus sign (+) plus a regular expression to filter subsequent output. The forward slash equals the keyword **begin**, the minus sign equals the keyword **exclude**, and the plus sign equals the keyword **include**.

The following definitions apply to the **begin**, **exclude**, and **include** keywords:

- **begin**—Displays the first line that matches the specified regular expression and all lines that follow.
- **exclude**—Displays all lines that do not match the specified regular expression.
- **include**—Displays all lines that match the specified regular expression.

A regular expression is a case-sensitive string of 1 to 256 characters that supports the special characters in Table 6.

Table 6 Special characters supported in a regular expression

Character	Meaning	Remarks
^string	Starting sign. Matches a line that starts with *string*.	For example, regular expression "^user" matches a line beginning with "user", not "Auser".
string$	Ending sign. Matches a line that ends with *string*.	For example, regular expression "user$" only matches a line ending with "user", not "userA".
.	Matches any single character, such as a single character, a special character, and a blank.	For example, ".s" matches both "as" and "bs".
*	Matches the preceding character or character group zero or multiple times.	For example, "zo*" matches "z" and "zoo"; "(zo)*" matches "zo" and "zozo".
+	Matches the preceding character or character group one or multiple times	For example, "zo+" matches "zo" and "zoo", but not "z".
|	Matches the preceding or succeeding character string	For example, "def|int" only matches a character string containing "def" or "int".
_	If it is at the beginning or the end of a regular expression, it equals ^ or $. In other cases, it equals comma, space, round bracket, or curly bracket.	For example, "a_b" matches "a b" or "a(b"; "_ab" only matches a line starting with "ab"; "ab_" only matches a line ending with "ab".
-	It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means 1 to 9 (inclusive); "a-h" means a to h (inclusive).
[ ]	Matches a single character contained within the brackets.	For example, [16A] matches a string containing any character among 1, 6, and A; [1-36A] matches a string containing any character among 1, 2, 3, 6, and A (- is a hyphen). "]" can be matched as a common character only when it is put at the beginning of characters within the brackets, for example [ ]*string*]. There is no such limit on "[".
( )	A character group. It is usually used with "+" or "*".	For example, (123A) means a character group "123A"; "408(12)+" matches 40812 or 408121212. But it does not match 408.
\index	Repeats the character string specified by the index. A character string refers to the string within () before \. *index* refers to the sequence number (starting from 1 from left to right) of the character group before \. If only one character group appears before \, *index* can only be 1; if n character groups appear before *index*, *index* can be any integer from 1 to n.	For example, (*string*)\1 repeats *string*, and a matching string must contain *stringstring*. (*string1*)(*string2*)\2 repeats *string2*, and a matching string must contain *string1string2string2*. (*string1*)(*string2*)\1\2 repeats *string1* and *string2* respectively, and a matching string must contain *string1string2string1string2*.

Character	Meaning	Remarks
[^]	Matches a single character not contained within the brackets.	For example, [^16A] means to match a string containing any character except 1, 6 or A, and the matching string can also contain 1, 6 or A, but cannot contain only these three characters. For example, [^16A] matches "abc" and "m16", but not 1, 16, or 16A.
\<string	Matches a character string starting with *string*.	For example, "\<do" matches word "domain" and string "doa".
string\>	Matches a character string ending with *string*.	For example, "do\>" matches word "undo" and string "abcdo".
\bcharacter2	Matches *character1character2*. *character1* can be any character except number, letter or underline, and \b equals [^A-Za-z0-9_].	For example, "\ba" matches "-a" with "-" being *character1,* and "a" being *character2,* but it does not match "2a" or "ba".
\Bcharacter	Matches a string containing *character*, and no space is allowed before *character*.	For example, "\Bt" matches "t" in "install", but not "t" in "big top".
character1\w	Matches *character1character2*. *character2* must be a number, letter, or underline, and \w equals [A-Za-z0-9_].	For example, "v\w" matches "**vl**an" ("v" is *character1* and "l" is *character2*) and "ser**vi**ce" ("i" is *character2*).
\W	Equals \b.	For example, "\Wa" matches "-a", with "-" being *character1,* and "a" being *character2, but does not* match "2a" or "ba".
\	Escape character. If a special character listed in this table follows \, the specific meaning of the character is removed.	For example, "\\" matches a string containing "\", "\^" matches a string containing "^", and "\\b" matches a string containing "\b".

The following are several regular expression examples:

Use **| begin user-interface** in the **display current-configuration** command to match the first line of output that contains **user-interface** to the last line of output.

```
<Sysname> display current-configuration | begin user-interface
user-interface aux 0
user-interface vty 0 15
 authentication-mode none
 user privilege level 3
#
return
```

Use **| exclude Direct** in the **display ip routing-table** command to filter out direct routes and display only the non-direct routes.

```
<Sysname> display ip routing-table | exclude Direct
Routing Tables: Public

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

1.1.1.0/24          Static 60   0            192.168.0.0     Vlan1
```

Use **| include Vlan** in the **display ip routing-table** command to filter in route entries that contain **Vlan**.

```
<Sysname> display ip routing-table | include Vlan
Routing Tables: Public

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

192.168.1.0/24      Direct 0    0            192.168.1.42    Vlan999
```

Configuring user privilege and command levels

To avoid unauthorized access, the device defines the user privilege levels and command levels in Table 7. User privilege levels correspond to command levels. A user who has been logged in with a specific privilege level can use only the commands at that level or lower levels.

All commands are categorized into four levels: visit, monitor, system, and manage, and are identified from low to high, respectively by 0 through 3.

Table 7 Command levels and user privilege levels

Level	Privilege	Default set of commands
0	Visit	Includes commands for network diagnosis and commands for accessing an external device. Configuration of commands at this level cannot survive a device restart. Upon device restart, the commands at this level are restored to the default settings. Commands at this level include **ping**, **tracert**, **telnet** and **ssh2**.
1	Monitor	Includes commands for system maintenance and service fault diagnosis. Commands at this level are not saved after being configured. After the device is restarted, the commands at this level are restored to the default settings. Commands at this level include **debugging**, **terminal**, **refresh**, and **send**.
2	System	Includes service configuration commands, including routing configuration commands and commands for configuring services at different network levels. By default, commands at this level include all configuration commands except for those at manage level.
3	Manage	Includes commands that influence the basic operation of the system and commands for configuring system support modules. By default, commands at this level involve the configuration commands of file system, FTP, TFTP, Xmodem download, user management, level setting, and parameter settings within a system, which are not defined by any protocols or RFCs.

Configuring a user privilege level

If the authentication mode on a user interface is scheme, configure a user privilege level for users who access the interface by using the AAA module or directly on the user interface. For SSH users who use public-key authentication, the user privilege level configured directly on the user interface always takes effect. For other users, the user privilege level configured in the AAA module has priority over the one configured directly on the user interface.

If the authentication mode on a user interface is none or password, configure the user privilege level directly on the user interface.

For more information about user login authentication, see "Logging in to the CLI." For more information about AAA and SSH, see *Security Configuration Guide*.

Configuring a user privilege level for users by using the AAA module

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter user interface view.	**user-interface** { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] }	N/A
3. Specify the scheme authentication mode.	**authentication-mode scheme**	By default, the authentication mode for VTY users is **password**, and no authentication is needed for AUX users.
4. Return to system view.	**quit**	N/A
5. Configure the authentication mode for SSH users as **password**.	For more information, see *Security Configuration Guide*.	This task is required only for SSH users who are required to provide their usernames and passwords for authentication.
6. Configure the user privilege level by using the AAA module.	• To use local authentication: a. Use the **local-user** command to create a local user and enter local user view. b. Use the **level** keyword in the **authorization-attribute** command to configure the user privilege level. • To use remote authentication (RADIUS or HWTACACS): Configure the user privilege level on the authentication server	User either approach. For local authentication, if you do not configure the user privilege level, the user privilege level is 0. For remote authentication, if you do not configure the user privilege level, the user privilege level depends on the default configuration of the authentication server. For more information about the **local-user** and **authorization-attribute** commands, see *Security Command Reference*.

For example:

Configure the device to use local authentication for Telnet users on VTY 1 and set the user privilege level to 3.

```
<Sysname> system-view
[Sysname] user-interface vty 1
[Sysname-ui-vty1] authentication-mode scheme
[Sysname-ui-vty1] quit
[Sysname] local-user test
[Sysname-luser-test] password simple 123
[Sysname-luser-test] service-type telnet
```

When users Telnet to the device through VTY 1, they must enter username **test** and password **12345678**. After passing the authentication, the users can only use level-0 commands of level 0.

Assign commands of levels 0 through 3 to the users.

```
[Sysname-luser-test] authorization-attribute level 3
```

Configuring the user privilege level directly on a user interface

To configure the user privilege level directly on a user interface that uses the scheme authentication mode:

Step	Command	Remarks
1. Configure the authentication type for SSH users as **publickey**.	For more information, see *Security Configuration Guide*.	Required only for SSH users who use public-key authentication.
2. Enter system view.	**system-view**	N/A
3. Enter user interface view.	**user-interface** { *first-num1* [*last-num1*] | **vty** *first-num2* [*last-num2*] }	N/A
4. Enable the scheme authentication mode.	**authentication-mode scheme**	By default, the authentication mode for VTY users is **password**, and no authentication is needed for AUX users.
5. Configure the user privilege level.	**user privilege level** *level*	By default, the user privilege level for users logged in through the AUX user interface is 3, and that for users logged in through VTY user interfaces is 0.

To configure the user privilege level directly on a user interface that uses the **none** or **password** authentication mode:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter user interface view.	**user-interface** { *first-num1* [*last-num1*] | { **aux** | **vty** } *first-num2* [*last-num2*] }	N/A
3. Configure the authentication mode for any user who uses the current user interface to log in to the device.	**authentication-mode** { **none** | **password** }	Optional. By default, the authentication mode for VTY user interfaces is **password**, and no authentication is needed for AUX users.
4. Configure the privilege level of users logged in through the current user interface.	**user privilege level** *level*	Optional. By default, the user privilege level for users logged in through the AUX user interface is 3, and that for users logged in through VTY user interfaces is 0.

For example:

Display the commands a Telnet user can use by default after login.

```
<Sysname> ?
User view commands:
  display  Display current system information
  ping     Ping function
  quit     Exit from current command view
```

```
  rsh      Establish one RSH connection
  ssh2     Establish a secure shell client connection
  super    Set the current user priority level
  telnet   Establish one TELNET connection
  tftp     Open TFTP connection
  tracert  Trace route function
```

Configure the device to perform no authentication for Telnet users, and to authorize authenticated Telnet users to use level-0 and level-1 commands. (Use no authentication mode only in a secure network environment.)

```
<Sysname> system-view
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode none
[Sysname-ui-vty0-15] user privilege level 1
```

Display the commands a Telnet user can use after login. Because the user privilege level is 1, a Telnet user can use more commands now.

```
<Sysname> ?
User view commands:
  debugging      Enable system debugging functions
  dialer         Dialer disconnect
  display        Display current system information
  ping           Ping function
  quit           Exit from current command view
  refresh        Do soft reset
  reset          Reset operation
  rsh            Establish one RSH connection
  screen-length  Specify the lines displayed on one screen
  send           Send information to other user terminal interface
  ssh2           Establish a secure shell client connection
  super          Set the current user priority level
  telnet         Establish one TELNET connection
  terminal       Set the terminal line characteristics
  tftp           Open TFTP connection
  tracert        Trace route function
  undo           Cancel current setting
```

Configure the device to perform password authentication for Telnet users, and to authorize authenticated Telnet users to use the commands of privilege levels 0, 1, and 2.

```
<Sysname> system-view
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] authentication-mode password
[Sysname-ui-vty0-15] set authentication password simple 123
[Sysname-ui-vty0-15] user privilege level 2
```

After the configuration is complete, when users Telnet to the device, they must enter the password **12345678**. After passing authentication, they can use commands of levels 0, 1, and 2.

Switching the user privilege level

Users can switch to a different user privilege level without logging out and terminating the current connection. After the privilege level switching, users can continue to manage the device without relogging in, but the commands they can execute have changed. For example, with the user privilege level 3, a user can configure system parameters. After switching to user privilege level 0, the user can execute only basic commands like **ping** and **tracert** and use a few **display** commands. The switching operation is effective for the current login. After the user relogs in, the user privilege restores to the original level.

To avoid problems, HP recommends that administrators log in with a lower privilege level to view switch operating parameters, and switch to a higher level temporarily only when they must maintain the device.

When an administrator must leave for a while or ask someone else to manage the device temporarily, they can switch to a lower privilege level before they leave to restrict the operation by others.

Configuring the authentication parameters for user privilege level switching

A user can switch to a privilege level equal to or lower than the current one unconditionally and is not required to enter a password (if any).

For security, a user is required to enter a password (if any) to switch to a higher privilege level. The authentication falls into one of the following categories:

Keywords	Authentication mode	Description
local	Local password authentication only (local-only)	The device authenticates a user by using the privilege level switching password entered by the user. To use this mode, you must set the password for privilege level switching by using the **super password** command.
scheme	Remote AAA authentication through HWTACACS or RADIUS	The device sends the username and password for privilege level switching to the HWTACACS or RADIUS server for remote authentication. To use this mode, you must perform the following configuration tasks: • Configure the required HWTACACS or RADIUS schemes and configure the ISP domain to use the schemes for users. For more information, see *Security Configuration Guide*. • Add user accounts and specify the user passwords on the HWTACACS or RADIUS server.
local scheme	Local password authentication first and then remote AAA authentication	The device authenticates a user by using the local password first, and if no password for privilege level switching is set, for the user logged in to the AUX user interface, the privilege level is switched directly; for VTY users, AAA authentication is performed.
scheme local	Remote AAA authentication first and then local password authentication	AAA authentication is performed first, and if the remote HWTACACS or RADIUS server does not respond or AAA configuration on the device is invalid, the local password authentication is performed.

To configure the authentication parameters for a user privilege level:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the authentication mode for user privilege level switching.	**super authentication-mode** { **local** | **scheme** } *	Optional. By default, local-only authentication is used.
3. Configure the password for a user privilege level.	In non-FIPS mode: **super password** [**level** *user-level*] [**hash**]{ **cipher** | **simple** } *password* In FIPS mode: **super password** [**level** *user-level*] { **cipher** | **simple** } *password*	Required for local authentication. By default, a privilege level has no password. If you do not specify any user privilege level, you configure a password for privilege level 3.

If local-only authentication is used, an AUX user interface user (a user logged in through the console port) can switch to a higher privilege level even if the privilege level has not been assigned a password.

Switching to a higher user privilege level

Before you switch to a higher user privilege level, obtain the required authentication data as described in Table 8.

For scheme authentication, a privilege level switching fails after three consecutive unsuccessful password attempts. For local authentication, a privilege level switching fails after five consecutive unsuccessful password attempts.

With scheme authentication, a user who fails to provide the correct password during five consecutive attempts must wait 15 minutes before trying again. Trying again before the 15-minute period elapses restores the wait timer to 15 minutes and restarts the timer.

To switch the user privilege level, perform the following task in user view:

Task	Command	Remarks
Switch the user privilege level.	**super** [*level*]	When logging in to the device, a user has a user privilege level, which depends on user interface or authentication user level.

Table 8 Information required for user privilege level switching

User interface authentication mode	User privilege level switching authentication mode	Information required for the first authentication mode	Information required for the second authentication mode
none/password	**local**	Password configured on the device with the **super password** command for the privilege level.	N/A
	local scheme	Password configured on the device with the **super password** command for the privilege level.	Username and password configured on the AAA server for the privilege level.

User interface authentication mode	User privilege level switching authentication mode	Information required for the first authentication mode	Information required for the second authentication mode
	scheme	Username and password for the privilege level.	N/A
	scheme local	Username and password for the privilege level.	Local user privilege level switching password.
scheme	**local**	Password configured on the device with the **super password** command for the privilege level.	N/A
	local scheme	Password configured on the device with the **super password** command for the privilege level.	Password for privilege level switching that is configured on the AAA server. The system uses the username used for logging in as the privilege level switching username.
	scheme	Password for privilege level switching that is configured on the AAA server. The system uses the username used for logging in as the privilege level switching username.	N/A
	scheme local	Password for privilege level switching that is configured on the AAA server. The system uses the username used for logging in as the privilege level switching username.	Password configured on the device with the **super password** command for the privilege level.

Changing the level of a command

Every command in a view has a default command level. The default command level scheme is sufficient for the security and ease of maintenance requirements of most networks. If you want to change the level of a command, make sure the change does not result in any security risk or maintenance problem.

To change the level of a command:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Change the level of a command in a specific view.	**command-privilege level** *level* **view** *view command*	See Table 7 for the default settings.

Saving the running configuration

You can use the **save** command in any view to save all submitted and executed commands into the configuration file. Commands saved in the configuration file can survive a reboot. The **save** command does not take effect on one-time commands, including **display** and **reset** commands. One-time commands are never saved.

Displaying and maintaining CLI

Task	Command	Remarks
Display the command keyword alias configuration.	**display command-alias** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display data in the clipboard.	**display clipboard** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Login overview

This chapter describes the available CLI login methods and their configuration procedures.

Login methods at a glance

You can access the device only through the console port at the first login, locally or remotely by using a pair of modems. After you log in to the device, you can configure other login methods, including Telnet and SSH, for remote access.

Table 9 Login methods

Login method	Default setting and configuration requirements
Logging in to the CLI:	
• Logging in through the console port for the first time	By default, login through the console port is enabled, no username or password is required, and the user privilege level is 3.
• Logging in through Telnet (not supported in FIPS mode)	By default, Telnet service is disabled. To use Telnet service, complete the following configuration tasks: • Enable the Telnet server. • Assign an IP address to a Layer 3 interface and make sure the interface and the Telnet client can reach each other. • Configure the authentication mode for VTY login users (password by default). • Configure the user privilege level of VTY login users (0 by default).
• Logging in through SSH	By default, SSH service is disabled. To use SSH service, complete the following configuration tasks: • Enable the SSH function and configure SSH attributes. • Assign an IP address to a Layer 3 interface and make sure the interface and the SSH client can reach each other. • Enable scheme authentication for VTY login users. • Configure the user privilege level of VTY login users (0 by default).
• Modem dial-in through the console port	By default, modem dial-in is enabled, no username or password is required, and the user privilege level is 3.
Logging in to the Web interface	By default, Web login is disabled. To use Web service, complete the following configuration tasks: • Assign an IP address to a Layer 3 interface. • Configure a local user account for Web login, and assign a user privilege level and the Web service to the account.
Logging in through SNMP	By default, SNMP login is disabled. To use SNMP service, complete the following configuration tasks: • Assign an IP address to a Layer 3 interface, and make sure the interface and the NMS can reach each other. • Configure SNMP basic parameters.

User interfaces

The device uses user interfaces (also called "lines") to control CLI logins and monitor CLI sessions. You can configure access control settings, including authentication, user privilege, and login redirect on user interfaces. After users are logged in, their actions must be compliant with the settings on the user interfaces assigned to them.

Users are assigned different user interfaces, depending on their login methods, as shown in Table 10.

Table 10 CLI login method and user interface matrix

User interface	Login method
AUX user interface	Console port (EIA/TIA-232 DCE), locally or remotely by using modems
Virtual type terminal (VTY) user interface	Telnet or SSH

User interface assignment

The device automatically assigns user interfaces to CLI login users, depending on their login methods. Each user interface can be assigned to only one user at a time. If no user interface is available, a CLI login attempt will be rejected.

The device provides one AUX user interfaces and 16 VTY user interfaces. For a CLI login, the device always picks the lowest numbered user interface from the idle user interfaces available for the type of login.

For example, four VTY user interfaces (0 to 3) are configured, of which VTY 0 and VTY 3 are idle. When a user Telnets to the device, the device assigns VTY 0 to the user and uses the settings on VTY 0 to authenticate and manage the user.

User interface identification

A user interface can be identified by an absolute number, or the interface type and a relative number.

An absolute number uniquely identifies a user interface among all user interfaces. The user interfaces are numbered starting from 0 and incrementing by 1 and in the sequence of AUX and VTY user interfaces. You can use the **display user-interface** command without any parameters to view supported user interfaces and their absolute numbers.

A relative number uniquely identifies a user interface among all user interfaces that are the same type. The number format is *user interface type* + *number*. Except for TTY user interfaces, which are numbered starting from 1 and incrementing by 1, all the other types of user interfaces are numbered starting from 0 and incrementing by 1. For example, the first AUX user interface is AUX 0.

A relative number uniquely identifies a user interface among all user interfaces that are the same type. The number format is *user interface type* + *number*. The user interfaces are numbered starting from 0 and incrementing by 1. For example, the first AUX user interface is AUX 0, and the second AUX user interface is AUX 1.

Logging in to the CLI

By default, the first time you access the CLI you must log in through the console port, locally or remotely by using a pair of modems. At the CLI, you can configure Telnet or SSH for remote access.

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Logging in through the console port for the first time

To log in through the console port, make sure the console terminal has a terminal emulation program (for example, HyperTerminal in Windows XP). In addition, the port settings of the terminal emulation program must be the same as the default settings of the console port in Table 11.

Table 11 Default console port properties

Parameter	Default
Bits per second	9600 bps
Flow control	None
Parity	None
Stop bits	1
Data bits	8

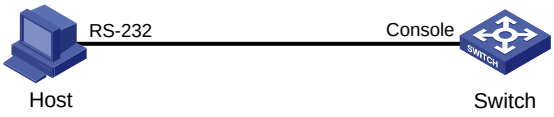
To log in through the console port from a console terminal (for example, a PC):

1. Plug the DB-9 female connector of the console cable to the serial port of the PC.
2. Plug the RJ-45 connector of the console cable to the console port of the device.

IMPORTANT:

- Identify the mark on the console port and make sure you are connecting to the correct port.
- The serial ports on PCs do not support hot swapping. If the switch has been powered on, always connect the console cable to the PC before connecting to the switch, and when you disconnect the cable, first disconnect it from the switch.

Figure 4 Connecting a terminal to the console port



3. If the PC is off, turn on the PC.
4. Launch the terminal emulation program and configure the communication properties on the PC.

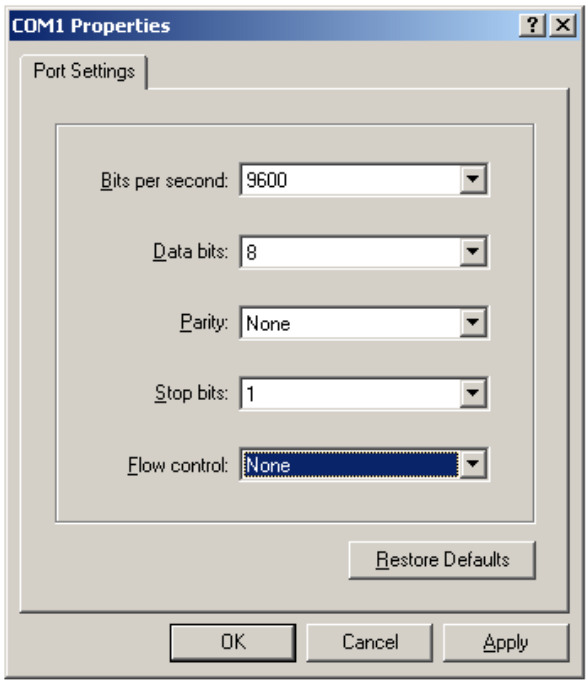
Figure 5 through Figure 7 show the configuration procedure on Windows XP HyperTerminal. On Windows Server 2003, add the HyperTerminal program first, and then log in to and manage the device as described in this document. On Windows Server 2008, Windows 7, Windows Vista, or some other operating system, obtain a third-party terminal control program first, and then follow the user guide or online help to log in to the device.

Make sure the port settings are the same as listed in Table 11.

Figure 5 Connection description

Figure 6 Specifying the serial port used to establish the connection

Figure 7 Setting the properties of the serial port



5. Power on the device and press **Enter** at the prompt.
6. At the default user view prompt <HP>, enter commands to configure the device or view the running status of the device. To get help, enter **?**.

Configuring console login control settings

The following authentication modes are available for controlling console logins:

- **None**—Requires no authentication. This mode is insecure.
- **Password**—Requires password authentication.
- **Scheme**—Uses the AAA module to provide local or remote console login authentication. You must provide a username and password for accessing the CLI. If the username or password configured on a remote server was lost, contact the server administrator for help.

By default, console login does not require authentication. Any user can log in through the console port without authentication and have user privilege level 3. To improve device security, configure the password or scheme authentication mode immediately after you log in to the device for the first time.

Table 12 Configuration required for different console login authentication modes

Authentication mode	Configuration tasks	Reference
None	Set the authentication mode to **none** for the AUX user interface.	"Configuring none authentication for console login (not supported in FIPS mode)"
Password	Enable password authentication on the AUX user interface. Set a password.	"Configuring password authentication for console login (not supported in FIPS mode)"

Authentication mode	Configuration tasks	Reference
Scheme	Enable scheme authentication on the AUX user interface. Configure local or remote authentication settings. To configure local authentication: 1. Configure a local user and specify the password. 2. Configure the device to use local authentication. To configure remote authentication: 1. Configure the RADIUS or HWTACACS scheme on the device. 2. Configure the username and password on the AAA server. 3. Configure the device to use the scheme for user authentication.	"Configuring scheme authentication for console login"

Configuring none authentication for console login (not supported in FIPS mode)

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter AUX user interface view.	**user-interface aux** *first-number* [*last-number*]	N/A
3. Enable the none authentication mode.	**authentication-mode none**	By default, you can log in to the device through the console port without authentication and have user privilege level 3.
4. Configure common settings for console login.	See "Configuring common console login settings (optional)."	Optional.

The next time you attempt to log in through the console port, you do not need to provide any username or password.

Configuring password authentication for console login (not supported in FIPS mode)

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter AUX user interface view.	**user-interface aux** *first-number* [*last-number*]	N/A

Step		Command	Remarks
3.	Enable password authentication.	**authentication-mode password**	By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login.
4.	Set a password.	**set authentication password** [**hash**] { **cipher** | **simple** } *password*	By default, no password is set.
5.	Configure common settings for console login.	See "Configuring common console login settings (optional)."	Optional.

The next time you attempt to log in through the console port, you must provide the configured login password.

Configuring scheme authentication for console login

Follow these guidelines when you configure scheme authentication for console login:

- To make the command authorization or command accounting function take effect, apply an HWTACACS scheme to the intended ISP domain. This scheme must specify the IP address of the authorization server and other authorization parameters.
- If the local authentication scheme is used, use the **authorization-attribute level** *level* command in local user view to set the user privilege level on the device.
- If a RADIUS or HWTACACS authentication scheme is used, set the user privilege level on the RADIUS or HWTACACS server.
- If password aging is enabled, make sure passwords for legal users are within the validity period.

To configure scheme authentication for console login:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enter AUX user interface view.	**user-interface aux** *first-number* [*last-number*]	N/A
3.	Enable scheme authentication.	**authentication-mode scheme**	Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme. By default, console log users are not authenticated in non-FIPS mode and **scheme** authentication is used in FIPS mode.

Step	Command	Remarks
4. Enable command authorization.	**command authorization**	Optional. By default, command authorization is disabled. The commands available for a user only depend on the user privilege level. If command authorization is enabled, a command is available only if the user has the commensurate user privilege level and is authorized to use the command by the AAA scheme.
5. Enable command accounting.	**command accounting**	Optional. By default, command accounting is disabled. The accounting server does not record the commands executed by users. Command accounting allows the HWTACACS server to record all commands executed by users, regardless of command execution results. This function helps control and monitor user behaviors on the device. If command accounting is enabled and command authorization is not enabled, every executed command is recorded on the HWTACACS server. If both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.
6. Exit to system view.	**quit**	N/A
7. Apply an AAA authentication scheme to the intended domain.	a. Enter ISP domain view: **domain** *domain-name* b. Apply an AAA scheme to the domain: **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] } c. Exit to system view: **quit**	Optional. By default, local authentication is used. For local authentication, configure local user accounts. For RADIUS or HWTACACS authentication, configure the RADIUS or HWTACACS scheme on the device and configure authentication settings (including the username and password) on the server. For more information about AAA configuration, see *Security Configuration Guide*.
8. Create a local user and enter local user view.	**local-user** *user-name*	By default, no local user exists.

Step	Command	Remarks
9. Set an authentication password for the local user.	• In non-FIPS mode: **password** [[**hash**] { **cipher** | **simple** } *password*] • In FIPS mode: **password**	By default, no password is set. In FIPS mode, you can set the password only in interactive mode.
10. Specifies a command level of the local user.	**authorization-attribute level** *level*	Optional. By default, the command level is 0.
11. Specify terminal service for the local user.	**service-type terminal**	By default, no service type is specified.
12. Configure common settings for console login.	See "Configuring common console login settings (optional)."	Optional.

The next time you attempt to log in through the console port, you must provide the configured login username and password.

Configuring common console login settings (optional)

Some common settings configured for an AUX user interface take effect immediately and can interrupt the console login session. To save you the trouble of repeated re-logins, use a login method different from console login to log in to the device before you change console login settings.

After the configuration is complete, change the terminal settings on the configuration terminal and make sure they are the same as the settings on the device.

To configure common settings for an AUX user interface:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable copyright information display.	**copyright-info enable**	By default, copyright information display is enabled.
3. Enter AUX user interface view.	**user-interface aux** *first-number* [*last-number*]	N/A
4. Configure the baud rate.	**speed** *speed-value*	By default, the transmission rate is 9600 bps.
5. Configure the parity check mode.	**parity** { **even** | **none** | **odd** }	The default setting is **none**, namely, no parity check.
6. Configure the number of stop bits.	**stopbits** { **1** | **1.5** | **2** }	The default is 1. Stop bits indicate the end of a character. The more the stop bits, the slower the transmission.

Step	Command	Remarks
7. Configure the number of data bits in a character.	**databits** { **7** | **8** }	By default, the number of data bits in each character is 8. The setting depends on the character coding type. For example, you can set it to 7 if standard ASCII characters are to be sent, and set it to 8 if extended ASCII characters are to be sent.
8. Define a shortcut key for enabling a terminal session.	**activation-key** *character*	By default, press **Enter** to enable a terminal session.
9. Define a shortcut key for terminating tasks.	**escape-key** { **default** | *character* }	By default, press **Ctrl+C** to terminate a task.
10. Configure the flow control mode.	**flow-control** { **hardware** | **none** | **software** }	By default, the flow control mode is **none**. The device supports only the **none** mode.
11. Specify the terminal display.	**terminal type** { **ansi** | **vt100** }	By default, the terminal display type is ANSI. The device supports two terminal display types: ANSI and VT100. HP recommends setting the display type to VT100 for both the device and the client. If the device and the client use different display types or both use the ANSI display type, when the total number of characters of a command line exceeds 80, the screen display on the terminal might be abnormal. For example, the cursor might be displayed at a wrong place.
12. Configure the user privilege level for login users.	**user privilege level** *level*	By default, the default command level is 3 for AUX user interfaces. This command is not supported in FIPS mode.
13. Set the maximum number of lines to be displayed on a screen.	**screen-length** *screen-length*	By default, a screen displays 24 lines at most. A value of 0 disables pausing between screens of output.
14. Set the size of command history buffer.	**history-command max-size** *value*	By default, the buffer saves 10 history commands at most.

Step	Command	Remarks
15. Set the idle-timeout timer.	**idle-timeout** *minutes* [*seconds*]	The default idle-timeout is 10 minutes. The system automatically terminates the user's connection if there is no information interaction between the device and the user within the idle-timeout time. Setting idle-timeout to 0 disables the timer.

Logging in through Telnet (not supported in FIPS mode)

You can Telnet to the device through a VTY user interface for remote management.

Figure 8 Telnet login

Use the PC as a Telnet client to Telnet to other devices, as shown in Figure 8.

Table 13 shows the Telnet server and client configuration required for a successful Telnet login.

Table 13 Telnet server and Telnet client configuration requirements

Object	Requirements
Telnet server	Assign an IP address to a Layer 3 interface, and make sure the Telnet server and client can reach each other. Configure the authentication mode and other settings. Enable Telnet server.
Telnet client	Run the Telnet client program. Obtain the IP address of the Layer 3 interface on the server.

To control Telnet access to the device working as a Telnet server, configure authentication and user privilege for Telnet users.

By default, password authentication applies to Telnet login, but no login password is configured. To allow Telnet access to the device after you enable the Telnet server, you must configure a password.

The following are authentication modes available for controlling Telnet logins:

- **None**—Requires no authentication and is insecure.
- **Password**—Requires a password for accessing the CLI. If your password was lost, log in to the device through the console port and change the password.
- **Scheme**—Uses the AAA module to provide local or remote authentication. You must provide a username and password for accessing the CLI. If the password configured in the local user database was lost, log in to the device through the console port and change the password. If the

username or password configured on a remote server was lost, contact the server administrator for help.

Table 14 Configuration required for different Telnet login authentication modes

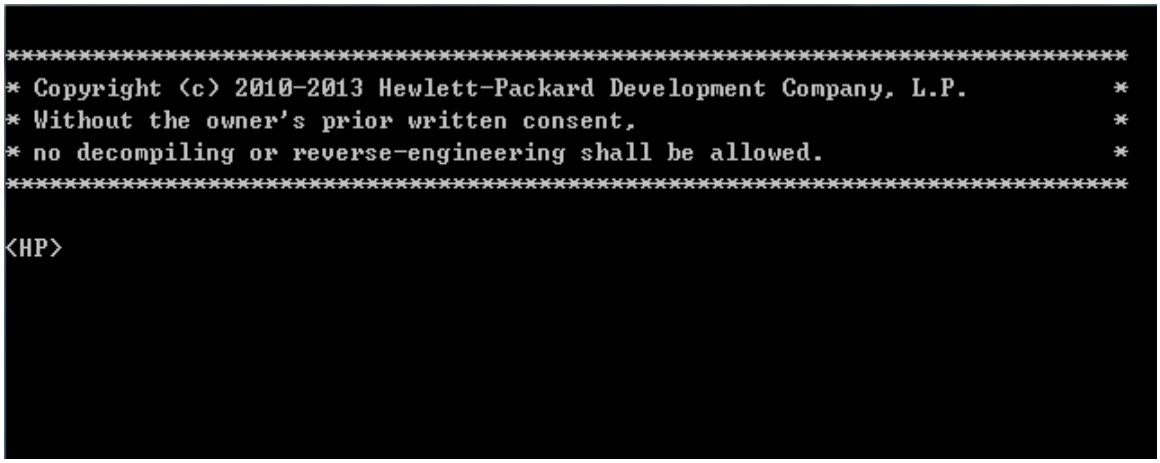
Authentication mode	Configuration tasks	Reference
None	Set the authentication mode to **none** for the VTY user interface.	"Configuring none authentication for Telnet login"
Password	Enable password authentication on the VTY user interface. Set a password.	"Configuring password authentication for Telnet login"
AAA	Enable scheme authentication on the VTY user interface. Configure local or remote authentication settings. To configure local authentication: 1. Configure a local user and specify the password. 2. Configure the device to use local authentication. To configure remote authentication: 1. Configure the RADIUS or HWTACACS scheme on the device. 2. Configure the username and password on the AAA server. 3. Configure the device to use the scheme for user authentication.	"Configuring scheme authentication for Telnet login"

Configuring none authentication for Telnet login

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable Telnet server.	**telnet server enable**	By default, the Telnet server is disabled.
3.	Enter one or multiple VTY user interface views.	**user-interface vty** *first-number* [*last-number*]	N/A
4.	Enable the none authentication mode.	**authentication-mode none**	By default, authentication mode for VTY user interfaces is **password**.
5.	Configure the command level for login users on the current user interfaces.	**user privilege level** *level*	By default, the default command level is 0 for VTY user interfaces.
6.	Configure common settings for the VTY user interfaces.	See "Configuring common settings for VTY user interfaces (optional)."	Optional.

The next time you attempt to Telnet to the device, you do not need to provide any username or password, as shown in Figure 9. If the maximum number of login users has been reached, your login attempt fails and the message "All user interfaces are used, please try later!" appears.

Figure 9 Telneting to the device without authentication



Configuring password authentication for Telnet login

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable Telnet.	**telnet server enable**	By default, the Telnet service is disabled.
3.	Enter one or multiple VTY user interface views.	**user-interface vty** *first-number* [*last-number*]	N/A
4.	Enable password authentication.	**authentication-mode password**	By default, password authentication is enabled for VTY user interfaces.
5.	Set a password.	**set authentication password** [**hash**] { **cipher** | **simple** } *password*	By default, no password is set.
6.	Configure the user privilege level for login users.	**user privilege level** *level*	The default level is 0.
7.	Configure common settings for VTY user interfaces.	See "Configuring common settings for VTY user interfaces (optional)."	Optional.

The next time you attempt to Telnet to the device, you must provide the configured login password, as shown in Figure 10. If the maximum number of login users has been reached, your login attempt fails and the message "All user interfaces are used, please try later!" appears.

Figure 10 Password authentication interface for Telnet login

Configuring scheme authentication for Telnet login

Follow these guidelines when you configure scheme authentication for Telnet login:

- To make the command authorization or command accounting function take effect, apply an HWTACACS scheme to the intended ISP domain. This scheme must specify the IP address of the authorization server and other authorization parameters.
- If the local authentication scheme is used, use the **authorization-attribute level** *level* command in local user view to set the user privilege level on the device.
- If a RADIUS or HWTACACS authentication scheme is used, set the user privilege level on the RADIUS or HWTACACS server.
- If password aging is enabled, make sure passwords for legal users are within the validity period.

To configure scheme authentication for Telnet login:

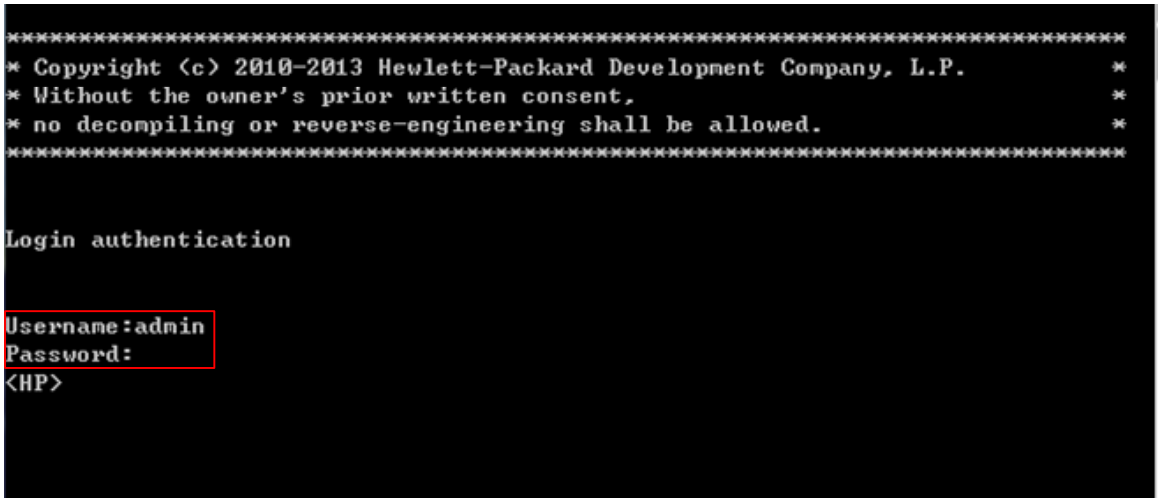
Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable Telnet.	**telnet server enable**	By default, the Telnet service is disabled.
3.	Enter one or multiple VTY user interface views.	**user-interface vty** *first-number* [*last-number*]	N/A
4.	Enable scheme authentication.	**authentication-mode scheme**	Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme. By default, local authentication is adopted.

Step	Command	Remarks
5. Enable command authorization.	**command authorization**	Optional. By default, command authorization is disabled. The commands available for a user only depend on the user privilege level. If command authorization is enabled, a command is available only if the user has the commensurate user privilege level and is authorized to use the command by the AAA scheme.
6. Enable command accounting.	**command accounting**	Optional. By default, command accounting is disabled. The accounting server does not record the commands executed by users. Command accounting allows the HWTACACS server to record all executed commands that are supported by the device, regardless of the command execution result. This function helps control and monitor user behaviors on the device. If command accounting is enabled and command authorization is not enabled, every executed command is recorded on the HWTACACS server. If both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.
7. Exit to system view.	**quit**	N/A
8. Apply an AAA authentication scheme to the intended domain.	a. Enter ISP domain view: **domain** *domain-name* b. Apply an AAA scheme to the domain: **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] } c. Exit to system view: **quit**	Optional. By default, local authentication is used. For local authentication, configure local user accounts. For RADIUS or HWTACACS authentication, configure the RADIUS or HWTACACS scheme on the device and configure authentication settings (including the username and password) on the server. For more information about AAA configuration, see *Security Configuration Guide*.

Step	Command	Remarks
9. Create a local user and enter local user view.	**local-user** *user-name*	By default, no local user exists.
10. Set a password.	**password** [[**hash**] { **cipher** | **simple** } *password*]	By default, no password is set.
11. Specify the command level of the local user.	**authorization-attribute level** *level*	Optional. By default, the command level is 0.
12. Specify Telnet service for the local user.	**service-type telnet**	By default, no service type is specified.
13. Exit to system view.	**quit**	N/A
14. Configure common settings for VTY user interfaces.	See "Configuring common settings for VTY user interfaces (optional)."	Optional.

The next time you attempt to Telnet to the CLI, you must provide the configured login username and password, as shown in Figure 11. If you are required to pass a second authentication, you must also provide the correct password to access the CLI. If the maximum number of login users has been reached, your login attempt fails and the message "All user interfaces are used, please try later!" appears.

Figure 11 Scheme authentication interface for Telnet login



Configuring common settings for VTY user interfaces (optional)

You might be unable to access the CLI through a VTY user interface after configuring the **auto-execute command** command on it. Before you configure the command and save the configuration, make sure you can access the CLI through a different user interface.

To configure common settings for VTY user interfaces:

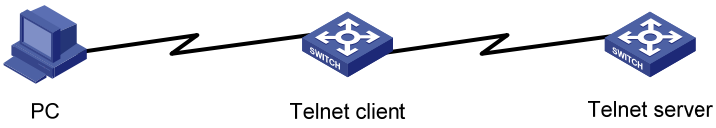
Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable copyright information display.	**copyright-info enable**	By default, copyright information display is enabled.

Step	Command	Remarks
3. Enter one or multiple VTY user interface views.	**user-interface vty** *first-number* [*last-number*]	N/A
4. Enable the terminal service.	**shell**	Optional. By default, terminal service is enabled.
5. Enable the user interfaces to support Telnet, SSH, or both of them.	**protocol inbound** { **all** | **ssh** | **telnet** }	Optional. By default, both Telnet and SSH are supported. The configuration takes effect the next time you log in.
6. Define a shortcut key for terminating tasks.	**escape-key** { **default** | character }	Optional. By default, press **Ctrl+C** to terminate a task.
7. Configure the type of terminal display.	**terminal type** { **ansi** | **vt100** }	Optional. By default, the terminal display type is ANSI.
8. Set the maximum number of lines to be displayed on a screen.	**screen-length** *screen-length*	Optional. By default, a screen displays 24 lines. A value of 0 disables the function.
9. Set the size of command history buffer.	**history-command max-size** *value*	Optional. By default, the buffer saves 10 history commands.
10. Set the idle-timeout timer.	**idle-timeout** *minutes* [*seconds*]	Optional. The default idle-timeout is 10 minutes for all user interfaces. The system automatically terminates the user's connection if there is no information interaction between the device and the user within the timeout time. Setting idle-timeout to 0 disables the timer.
11. Specify a command to be automatically executed when a user logs in to the user interfaces.	**auto-execute command** *command*	Optional. By default, no automatically executed command is specified. The command auto-execute function is typically used for redirecting a Telnet user to a specific host. After executing the specified command and performing the incurred task, the system automatically disconnect the Telnet session.

Using the device to log in to a Telnet server

You can use the device as a Telnet client to log in to a Telnet server. If the server is located in a different subnet than the device, make sure the two devices have routes to reach each other.

Figure 12 Telnetting from the device to a Telnet server



To use the device to log in to a Telnet server:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Specify a source IPv4 address or source interface for outgoing Telnet packets.	**telnet client source** { **interface** *interface-type interface-number* | **ip** *ip-address* }	Optional. By default, no source IPv4 address or source interface is specified. The IP address of the outbound interface is used as the source IPv4 address.
3.	Exit to user view.	**quit**	N/A
4.	Use the device to log in to a Telnet server.	• Log in to an IPv4 Telnet server: **telnet** *remote-host* [*service-port*] [[**vpn-instance** *vpn-instance-name*] | [**source** { **interface** *interface-type interface-number* | **ip** *ip-address* }]] • Log in to an IPv6 Telnet server: **telnet ipv6** *remote-host* [**-i** *interface-type interface-number*] [*port-number*] [**vpn-instance** *vpn-instance-name*]	Use either command. The **vpn-instance** *vpn-instance-name* option is only available on the HP 5500 EI switches.

Setting the DSCP value for IP to use for outgoing Telnet packets

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the DSCP value for IP to use for outgoing Telnet packets.	• On a Telnet client running IPv4: **telnet client dscp** *dscp-value* • On a Telnet client running IPv6: **telnet client ipv6 dscp** *dscp-value* • On a Telnet server running IPv4: **telnet server dscp** *dscp-value* • On a Telnet server running IPv6: **telnet server ipv6 dscp** *dscp-value*	The default is as follows: • 16 for a Telnet client running IPv4. • 0 for a Telnet client running IPv6. • 48 for a Telnet server running IPv4. • 0 for a Telnet server running IPv6.

Logging in through SSH

SSH offers a secure approach to remote login. By providing encryption and strong authentication, it protects devices against attacks such as IP spoofing and plaintext password interception. You can log in to the device working as an SSH server for remote management, as shown in Figure 13. You can also use the device as an SSH client to log in to an SSH server.

Figure 13 SSH login diagram

Table 15 shows the SSH server and client configuration required for a successful SSH login.

Table 15 SSH server and client requirements

Device role	Requirements
SSH server	Assign an IP address to a Layer 3 interface, and make sure the interface and the client can reach each other. Configure the authentication mode and other settings.
SSH client	If the host is operating as an SSH client, run the SSH client program on the host. Obtain the IP address of the Layer 3 interface on the server.

To control SSH access to the device working as an SSH server, configure authentication and user privilege level for SSH users.

By default, password authentication is adopted for SSH login, but no login password is configured. To allow SSH access to the device after you enable the SSH server, you must configure a password.

Configuring the SSH server on the device

Follow these guidelines when you configure the SSH server:

- To make the command authorization or command accounting function take effect, apply an HWTACACS scheme to the intended ISP domain. This scheme must specify the IP address of the authorization server and other authorization parameters.
- If the local authentication scheme is used, use the **authorization-attribute level** *level* command in local user view to set the user privilege level on the device.
- If a RADIUS or HWTACACS authentication scheme is used, set the user privilege level on the RADIUS or HWTACACS server.

The SSH client authentication method is password in this configuration procedure. For more information about SSH and publickey authentication, see *Security Configuration Guide*.

To configure the SSH server on the device:

Step	Command	Remarks
3. Enter system view.	**system-view**	N/A

Step		Command	Remarks
4.	Create local key pairs.	**public-key local create** { **dsa** | **rsa** }	By default, no local key pairs are created.
5.	Enable SSH server.	**ssh server enable**	By default, SSH server is disabled.
6.	Enter one or more VTY user interface views.	**user-interface vty** *first-number* [*last-number*]	N/A
7.	Enable scheme authentication.	**authentication-mode scheme**	By default, password authentication is enabled on VTY user interfaces in non-FIPS mode and **scheme** authentication is used in FIPS mode.
8.	Enable the user interfaces to support Telnet, SSH, or both of them.	In non-FIPS mode: **protocol inbound** { **all** | **ssh** | **telnet** }	Optional. By default, both protocols are supported in non-FIPS mode and SSH is used in FIPS mode.
		In FIPS mode: **protocol inbound { all | ssh }**	
9.	Enable command authorization.	**command authorization**	Optional. By default, command authorization is disabled. The commands available for a user only depend on the user privilege level. If command authorization is enabled, a command is available only if the user has the commensurate user privilege level and is authorized to use the command by the AAA scheme.

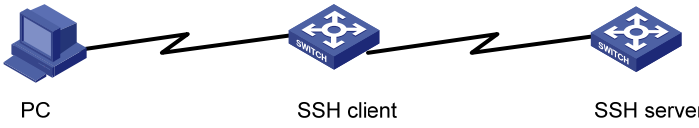
Step	Command	Remarks
10. Enable command accounting.	**command accounting**	Optional. By default, command accounting is disabled. The accounting server does not record the commands executed by users. Command accounting allows the HWTACACS server to record all executed commands that are supported by the device, regardless of the command execution result. This function helps control and monitor user behaviors on the device. If command accounting is enabled and command authorization is not enabled, every executed command is recorded on the HWTACACS server. If both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.
11. Exit to system view.	**quit**	N/A
12. Apply an AAA authentication scheme to the intended domain.	a. Enter the ISP domain view: **domain** *domain-name* b. Apply the specified AAA scheme to the domain: **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] } c. Exit to system view: **quit**	Optional. For local authentication, configure local user accounts. For RADIUS or HWTACACS authentication, configure the RADIUS or HWTACACS scheme on the device and configure authentication settings (including the username and password) on the server. For more information about AAA configuration, see *Security Configuration Guide*.
11. Create a local user and enter local user view.	**local-user** *user-name*	By default, no local user exists.
12. Set a password for the local user.	• In non-FIPS mode: **password** [[**hash**] { **cipher** | **simple** } *password*] • In FIPS mode: **password**	By default, no password is set. In FIPS mode, you can set the password only in interactive mode.
13. Specify the command level of the user.	**authorization-attribute level** *level*	Optional. By default, the command level is 0.
14. Specify SSH service for the user.	**service-type ssh**	By default, no service type is specified.
15. Exit to system view.	**quit**	N/A

Step	Command	Remarks
16. Create an SSH user, and specify the authentication mode for the SSH user.	**ssh user** *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }	N/A
17. Configure common settings for VTY user interfaces.	See "Configuring common settings for VTY user interfaces (optional)."	Optional.

Using the device as an SSH client to log in to the SSH server

You can use the device as an SSH client to log in to an SSH server. If the server is located in a different subnet than the device, make sure the two devices have routes to reach each other.

Figure 14 Logging in to an SSH server from the device



To use the device as an SSH client to log in to an SSH server, perform the following tasks in user view:

Task	Command	Remarks
Log in to an IPv4 SSH server.	**ssh2** *server*	The *server* argument represents the IPv4 address or host name of the server.
Log in to an IPv6 SSH server.	**ssh2 ipv6** *server*	The *server* argument represents the IPv6 address or host name of the server.

To work with the SSH server, you might need to configure the SSH client. For information about configuring the SSH client, see *Security Configuration Guide*.

Modem dial-in through the console port

You can use a pair of modems to remotely connect to a device through its console port over the PSTN when the IP network connection is broken. To do so, make sure the dial-in connection, the device, and the modems are correctly set up.

By default, you can log in to the device through modems without authentication, and have user privilege level 3. To improve device security, configure AUX login authentication.

The following are authentication modes available for modem dial-in through the console port:

- **None**—Requires no authentication and is insecure.
- **Password**—Requires a password for accessing the CLI. If your password was lost, log in to the device through the console port and change the password.
- **Scheme**—Uses the AAA module to provide local or remote authentication. If your password was lost, log in to the device through the console port and change the password. If the username or password configured on a remote server was lost, contact the server administrator for help.

Table 16 Configuration required for different modem login authentication modes

Authentication mode	Configuration task	Reference
None	Set the authentication mode to **none** for the AUX user interface.	"Configuring none authentication for modem dial-in (not supported in FIPS mode)"
Password	Enable password authentication on the AUX user interface. Set a password.	"Configuring password authentication for modem dial-in (not supported in FIPS mode)"
Scheme	Enable scheme authentication on the AUX user interface. Configure local or remote authentication settings. To configure local authentication: 1. Configure a local user and specify the password. 2. Configure the device to use local authentication. To configure remote authentication: 1. Configure the RADIUS or HWTACACS scheme on the device. 2. Configure the username and password on the AAA server. 3. Configure the device to use the scheme for user authentication.	"Configuring scheme authentication for modem dial-in"

Setting up the configuration environment

Set up a configuration environment as shown in Figure 15:

1. Connect the serial port of the PC to a modem and the console port of the device to a modem.
2. Connect each modem to the PSTN through a telephone cable.
3. Obtain the telephone number of the modem connected to the device.

Figure 15 Connecting the PC to the device through modems

4. Perform the following configurations on the modem directly connected to the device:
   - **AT&F**—Restores the factory default.
   - **ATS0=1**—Configures auto-answer on first ring.
   - **AT&D**—Ignores data Terminal Ready signals.
   - **AT&K0**—Disables local flow control.
   - **AT&R1**—Ignores Data Flow Control signals.
   - **AT&S0**—Forces **DSR** to remain on.

- **ATEQ1&W**—Disables the modem from returning command responses and execution results.

To verify your configuration, enter AT&V to display the configuration results.

NOTE:

The configuration commands and output vary by modem. For more information, see the modem user guide.

5. To avoid data loss, verify that the speed of the console port is lower than the transmission rate of the modem, and the default parity check, stop bits, and data bits settings are used.
6. Launch the terminal emulation program and create a connection by using the telephone number of the modem connected to the device.

   Figure 16 to Figure 18 shows the configuration procedure in Windows XP HyperTerminal.

Figure 16 Creating a connection

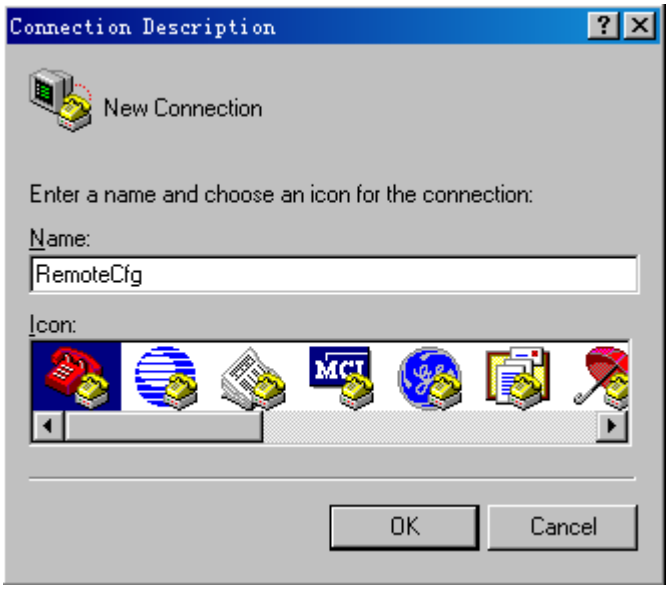
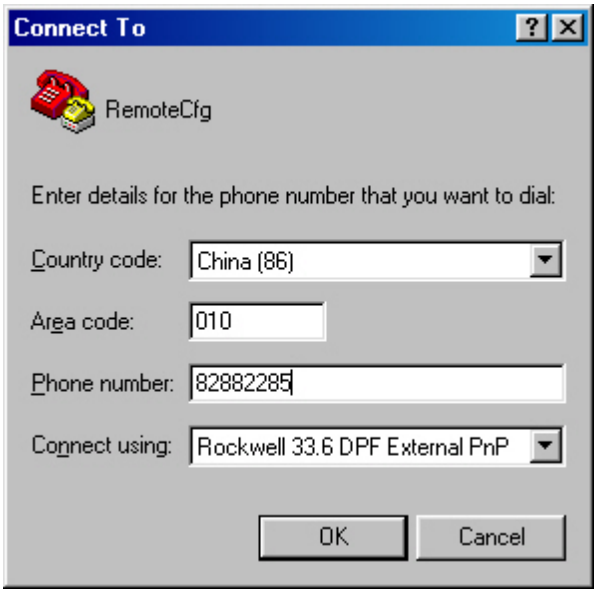


Figure 17 Configuring the dialing parameters

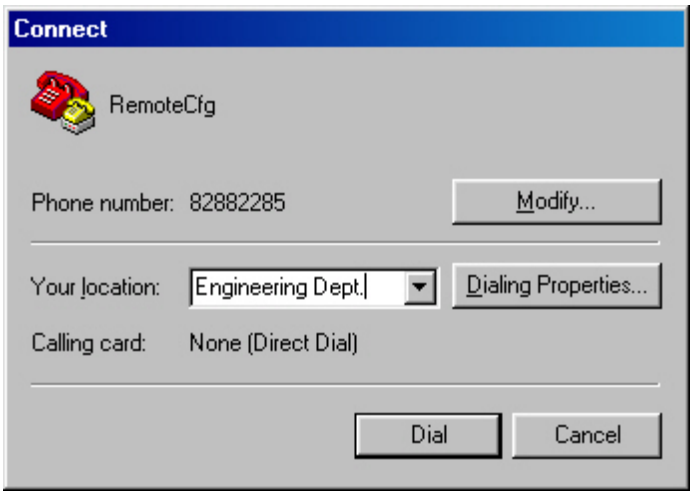


NOTE:

On Windows Server 2003, you must add the HyperTerminal program first, and then log in to and manage the device as described in this document. On Windows Server 2008, Windows 7, Windows Vista, or some other operating system, obtain a third-party terminal control program first, and follow the user guide or online help of that program to log in to the device.

7. Dial the telephone number to establish a connection to the device.

Figure 18 Dialing the number



8. Press **Enter** as prompted.
9. At the default user view prompt <HP>, enter commands to configure the device or view the running status of the device. To get help, enter **?**.

To disconnect the PC from the device, execute the **ATH** command in the HyperTerminal. If the command cannot be entered, type AT+ + + and then press **Enter**. When the word "**OK**" appears, execute the **ATH** command. The connection is terminated if "**OK**" is displayed. You can also terminal the connection by clicking  in the HyperTerminal window.

IMPORTANT:

Do not directly close the HyperTerminal. Doing so can cause some modems to stay in use, and your subsequent dial-in attempts will always fail.

Configuring none authentication for modem dial-in (not supported in FIPS mode)

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter one or more AUX user interface views.	**user-interface aux** *first-number* [*last-number*]	N/A
3. Enable the none authentication mode.	**authentication-mode none**	By default, modem users can dial in to the device without authentication.

Step	Command	Remarks
4. Configure common settings for the AUX user interfaces.	See "Configuring common settings for modem dial-in (optional)."	Optional.

The next time you attempt to dial in to the device, you do not need to provide any username or password.

Configuring password authentication for modem dial-in (not supported in FIPS mode)

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter one or more AUX user interface views.	**user-interface aux** *first-number* [*last-number*]	N/A
3. Enable password authentication.	**authentication-mode password**	By default, no authentication is performed for modem dial-in users.
4. Set a password.	**set authentication password** [**hash**] { **cipher** | **simple** } *password*	By default, no password is set.
5. Configure common settings for the AUX user interfaces.	For more information, see "Configuring common settings for modem dial-in (optional)."	Optional.

The next time you attempt to dial in to the device, you must provide the configured login password.

Configuring scheme authentication for modem dial-in

Follow these guidelines when you configure scheme authentication for AUX login:

- To make the command authorization or command accounting function take effect, apply an HWTACACS scheme to the intended ISP domain. This scheme must specify the IP address of the authorization server and other authorization parameters.
- If the local authentication scheme is used, use the **authorization-attribute level** *level* command in local user view to set the user privilege level on the device.
- If a RADIUS or HWTACACS authentication scheme is used, set the user privilege level on the RADIUS or HWTACACS server.
- If password aging is enabled, make sure passwords for legal users are within the validity period.

To configure scheme authentication for modem dial-in users:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enter AUX user interface view.	**user-interface aux** *first-number* [*last-number*]	N/A

Step	Command	Remarks
3. Enable scheme authentication.	**authentication-mode scheme**	Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme. By default, no authentication is performed for modem dial-in users in non-FIPS mode and **scheme** authentication is used in FIPS mode.
4. Enable command authorization.	**command authorization**	Optional. By default, command authorization is disabled. The commands available for a user only depend on the user privilege level. If command authorization is enabled, a command is available only if the user has the commensurate user privilege level and is authorized to use the command by the AAA scheme.
5. Enable command accounting.	**command accounting**	Optional. By default, command accounting is disabled. The accounting server does not record the commands executed by users. Command accounting allows the HWTACACS server to record all executed commands that are supported by the device, regardless of the command execution result. This function helps control and monitor user behaviors on the device. If command accounting is enabled and command authorization is not enabled, every executed command is recorded on the HWTACACS server. If both command accounting and command authorization are enabled, only the authorized and executed commands are recorded on the HWTACACS server.
6. Exit to system view.	**quit**	N/A
7. Apply an AAA authentication scheme to the intended domain.	a. Enter the ISP domain view: **domain** *domain-name* b. Apply the specified AAA scheme to the domain: **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] } c. Exit to system view: **quit**	Optional. By default, local authentication is used. For local authentication, configure local user accounts. For RADIUS or HWTACACS authentication, configure the RADIUS or HWTACACS scheme on the device and configure authentication settings (including the username and password) on the server. For more information about AAA configuration, see *Security Configuration Guide*.

Step	Command	Remarks
8. Create a local user and enter local user view.	**local-user** *user-name*	By default, no local user exists.
9. Set a password for the local user.	• In non-FIPS mode: **password** [[**hash**] { **cipher** | **simple** } *password*] • In FIPS mode: **password**	By default, no password is set. In FIPS mode, you can set the password only in interactive mode.
10. Specify the command level of the local user.	**authorization-attribute level** *level*	Optional. By default, the command level is 0.
11. Specify terminal service for the local user.	**service-type terminal**	By default, no service type is specified.
12. Configure common settings for the AUX user interfaces.	See "Configuring common settings for modem dial-in (optional)."	Optional.

The next time you attempt to dial in to the device, you must provide the configured username and password.

Configuring common settings for modem dial-in (optional)

CAUTION:

To avoid packet loss, make sure the speed of the console port is lower than the transmission rate of the modem.

Some common settings configured for an AUX user interface take effect immediately and can interrupt the login session. To save you the trouble of repeated re-logins, use a login method different from AUX login to log in to the device before you change AUX user interface settings.

After the configuration is complete, change the terminal settings on the configuration terminal and make sure they are the same as the settings on the device.

To configure common AUX user interface settings for modem dial-in accesses:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable copyright information display.	**copyright-info enable**	By default, copyright information display is enabled.
3. Enter one or more AUX user interface views.	**user-interface aux** *first-number* [*last-number*]	N/A
4. Configure the baud rate.	**speed** *speed-value*	By default, the baud rate is 9600 bps.
5. Configure the parity check mode.	**parity** { **even** | **none** | **odd** }	The default setting is **none**, namely, no parity check.

Step	Command	Remarks
6. Configure the number of stop bits.	**stopbits** { **1** | **1.5** | **2** }	The default is 1. Stop bits indicate the end of a character. The more the bits, the slower the transmission.
7. Configure the number of data bits in each character.	**databits** { **7** | **8** }	By default, the number of data bits in each character is 8. The setting depends on the character coding type. For example, you can set it to 7 if standard ASCII characters are to be sent, and set it to 8 if extended ASCII characters are to be sent.
8. Define a shortcut key for starting a session.	**activation-key** *character*	By default, press **Enter** to start a session.
9. Define a shortcut key for terminating tasks.	**escape-key** { **default** | character }	By default, press **Ctrl+C** to terminate a task.
10. Configure the flow control mode.	**flow-control** { **hardware** | **none** | **software** }	By default , the flow control mode is **none**. The device supports only the **none** mode.
11. Specify the terminal display type.	**terminal type** { **ansi** | **vt100** }	By default, the terminal display type is ANSI. The device supports two terminal display types: ANSI and VT100. HP recommends setting the display type to VT100 for both the device and the client. If the device and the client use different display types or both use the ANSI display type, when the total number of characters of a command line exceeds 80, the screen display on the terminal might be abnormal. For example, the cursor might be displayed at a wrong place.
12. Configure the user privilege level for login users.	**user privilege level** *level*	3 by default. This command is not supported in FIPS mode.
13. Set the maximum number of lines to be displayed on a screen.	**screen-length** *screen-length*	By default, a screen displays 24 lines at most. A value of 0 disables the function.
14. Set the size of the command history buffer.	**history-command max-size** *value*	By default, the buffer saves 10 history commands at most.

Step	Command	Remarks
15. Set the idle-timeout timer.	**idle-timeout** *minutes* [*seconds*]	The default idle-timeout is 10 minutes. The system automatically terminates the user's connection if there is no information interaction between the device and the user within the idle-timeout time. Setting idle-timeout to 0 disables the timer.

Displaying and maintaining CLI login

Task	Command	Remarks
Display information about the user interfaces that are being used.	**display users** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display information about all user interfaces the device supports.	**display users all** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display user interface information.	**display user-interface** [*num1* | { **aux** | **vty** } *num2*] [**summary**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Display the configuration of the device when it serves as a Telnet client.	**display telnet client configuration** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view.
Release a user interface.	**free user-interface** { *num1* | { **aux** | **vty** } *num2* }	Available in user view. Multiple users can log in to the system to simultaneously configure the device. You can execute the command to release the connections established on the specified user interfaces. You cannot use this command to release the connection you are using.
Lock the current user interface.	**lock**	Available in user view. By default, the system does not lock a user interface automatically. This command is not supported in FIPS mode.
Send messages to the specified user interfaces.	**send** { **all** | *num1* | { **aux** | **vty** } *num2* }	Available in user view.

Logging in to the Web interface

The device provides a built-in Web server for you to configure the device through a Web browser. Web login is by default disabled.

To enable Web login, log in via the console port, and perform the following configuration tasks:

- Enable HTTP or HTTPS service.
- Configure the IP address of a Layer 3 interface, and make sure the interface and the configuration terminal can reach each other.
- Configure a local user account for Web login.

The device supports HTTP 1.0 and HTTPS for transferring webpage data across the Internet.

HTTPS uses SSL to encrypt data between the client and the server for data integrity and security, and is more secure than HTTP. You can define a certificate attribute-based access control policy to allow only legal clients to access the device.

HTTP login and HTTPS login are separate login methods. To use HTTPS login, you do not need to configure HTTP login.

Table 17 shows the basic Web login configuration requirements.

Table 17 Basic web login configuration requirements

Object	Requirements
Device	Configure an IP address for a Layer 3 interface. Configuring routes to make sure the interface and the PC can reach each other. Perform either or both of the following tasks: • Configuring HTTP login • Configuring HTTPS login
PC	Install a Web browser. Obtain the IP address of the device's Layer 3 interface.

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Web login is not supported in FIPS mode.

Configuring HTTP login

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A

Step	Command	Remarks
2. Enable the HTTP service.	**ip http enable**	• When the device starts up with empty configuration, the software initial settings are used, and HTTP service is enabled. • When the device starts up with the default configuration file, the software default settings are used, and HTTP service is disabled. For more information about the initial settings and default configuration file, see *Fundamentals Configuration Guide*.
3. Configure the HTTP service port number.	**ip http port** *port-number*	Optional. The default HTTP service port is 80. If you execute the command multiple times, the last one takes effect.
4. Associate the HTTP service with an ACL.	**ip http acl** *acl-number*	Optional. By default, the HTTP service is not associated with any ACL. Associating the HTTP service with an ACL enables the device to allow only clients permitted by the ACL to access the device.
5. Create a local user and enter local user view.	**local-user** *user-name*	By default, no local user is configured.
6. Configure a password for the local user.	In non-FIPS mode: **password** [[**hash**] { **cipher** | **simple** } *password*] In FIPS mode: **password**	By default, no password is configured for the local user.
7. Specify the command level of the local user.	**authorization-attribute level** *level*	No command level is configured for the local user.
8. Specify the Telnet service type for the local user.	**service-type web**	By default, no service type is configured for the local user.
9. Exit to system view.	**quit**	N/A
10. Set the DSCP value for IP to use for HTTP packets.	• For IPv4: **ip http dscp** *dscp-value* • For IPv6: **ipv6 http dscp** *dscp-value*	Optional. The default is as follows: • 16 for IPv4. • 0 for IPv6.
11. Create a VLAN interface and enter its view.	**interface vlan-interface** *vlan-interface-id*	If the VLAN interface already exists, the command enters its view.

Step	Command	Remarks
12. Assign an IP address and subnet mask to the interface.	**ip address** *ip-address* { *mask* | *mask-length* }	By default, no IP address is assigned to the interface.

NOTE:

When the device transitions from FIPS mode to non-FIPS mode, it automatically enables the HTTP service. If you want the HTTP service to be disabled, execute the **undo ip http enable** command.

Configuring HTTPS login

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Associate the HTTPS service with an SSL server policy.	**ip https ssl-server-policy** *policy-name*	By default, the HTTPS service is not associated with any SSL server policy, and the device uses a self-signed certificate for authentication. If you disable the HTTPS service, the system automatically de-associates the HTTPS service from the SSL service policy. Before re-enabling the HTTPS service, associate the HTTPS service with an SSL server policy first. If the HTTPS service has been enabled, any changes to the SSL server policy associated with the HTTP service that is enabled do not take effect.
3. Enable the HTTPS service.	**ip https enable**	By default, HTTPS is disabled. Enabling the HTTPS service triggers an SSL handshake negotiation process. During the process, if the local certificate of the device exists, the SSL negotiation succeeds, and the HTTPS service can be started properly. If no local certificate exists, a certificate application process will be triggered by the SSL negotiation. Because the application process takes much time, the SSL negotiation often fails and the HTTPS service cannot be started normally. In that case, execute the **ip https enable** command multiple times to start the HTTPS service.

Step	Command	Remarks
4. Associate the HTTPS service with a certificate attribute-based access control policy.	**ip https certificate access-control-policy** *policy-name*	Optional. By default, the HTTPS service is not associated with any certificate-based attribute access control policy. Associating the HTTPS service with a certificate-based attribute access control policy enables the device to control the access rights of clients. You must configure the **client-verify enable** command in the associated SSL server policy. If not, no clients can log in to the device. The associated SSL server policy must contain at least one **permit** rule. Otherwise, no clients can log in to the device. For more information about certificate attribute-based access control policies, see *Security Configuration Guide*.
5. Specify the HTTPS service port number.	**ip https port** *port-number*	Optional. The default HTTPS service port is 443.
6. Associate the HTTPS service with an ACL.	**ip https acl** *acl-number*	By default, the HTTPS service is not associated with any ACL. Associating the HTTPS service with an ACL enables the device to allow only clients permitted by the ACL to access the device.
7. Create a local user and enter local user view.	**local-user** *user-name*	By default, no local user is configured.
8. Configure a password for the local user.	• In non-FIPS mode: **password** [[**hash**] { **cipher** | **simple** } *password*] • In FIPS mode: **password**	By default, no password is configured for the local user.
9. Specify the command level of the local user.	**authorization-attribute level** *level*	By default, no command level is configured for the local user.
10. Specify the Web service type for the local user.	**service-type web**	By default, no service type is configured for the local user.
11. Exit to system view.	**quit**	N/A
12. Create a VLAN interface and enter its view.	**interface vlan-interface** *vlan-interface-id*	If the VLAN interface already exists, the command enters its view. You could replace this VLAN interface with any other Layer 3 interface as appropriate.
13. Assign an IP address and subnet mask to the interface.	**ip address** *ip-address* { *mask* | *mask-length* }	By default, no IP address is assigned to the interface.

For more information about SSL and PKI, see *Security Configuration Guide*.

Displaying and maintaining Web login

Task	Command	Remarks
Display information about Web users.	**display web users** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display HTTP state information.	**display ip http** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display HTTPS state information.	**display ip https** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

HTTP login configuration example

Network requirements

As shown in Figure 19, configure the device to allow the PC to log in over the IP network by using HTTP.

Figure 19 Network diagram

Configuration procedure

1. Configure the device:

   # Create VLAN 999, and add GigabitEthernet 1/0/1 (the interface connected to the PC) to VLAN 999.

   ```
   <Sysname> system-view
   [Sysname] vlan 999
   [Sysname-vlan999] port GigabitEthernet 1/0/1
   [Sysname-vlan999] quit
   ```

   # Assign the IP address 192.168.0.58 and the subnet mask 255.255.255.0 to VLAN-interface 999.

   ```
   [Sysname] interface vlan-interface 999
   [Sysname-VLAN-interface999] ip address 192.168.0.58 255.255.255.0
   [Sysname-VLAN-interface999] quit
   ```

   # Create a local user named **admin**, and set the password to **admin** for the user. Specify the Web service type for the local user, and set the command level to 3 for this user.

   ```
   [Sysname] local-user admin
   [Sysname-luser-admin] service-type web
   [Sysname-luser-admin] authorization-attribute level 3
   ```

```
[Sysname-luser-admin] password simple admin
```

2. Verify the configuration:

   # On the PC, run the Web browser. Enter the IP address of the device in the address bar. The Web login page appears, as shown in Figure 20.

Figure 20 Web login page

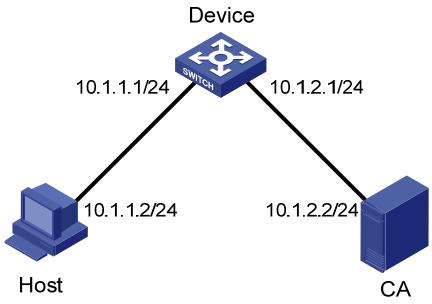
   # Enter the user name, password, verify code, select **English**, and click **Login**. The homepage appears. After login, you can configure device settings through the Web interface.

HTTPS login configuration example

Network requirements

As shown in Figure 21, to prevent unauthorized users from accessing the device, configure the device as the HTTPS server and the host as the HTTPS client, and request a certificate for each of them.

Figure 21 Network diagram



Configuration procedure

This example assumes that the CA is named **new-ca**, runs Windows Server, and is installed with the SCEP add-on. This example also assumes the device, host, and CA can reach one other.

1. Configure the device (HTTPS server):

   # Configure a PKI entity, configure the common name of the entity as **http-server1**, and the FQDN of the entity as **ssl.security.com**.

   ```
   <Device> system-view
   [Device] pki entity en
   [Device-pki-entity-en] common-name http-server1
   [Device-pki-entity-en] fqdn ssl.security.com
   [Device-pki-entity-en] quit
   ```

   # Create a PKI domain, specify the trusted CA as **new-ca**, the URL of the server for certificate request as **http://10.1.2.2/certsrv/mscep/mscep.dll**, authority for certificate request as **RA**, and the entity for certificate request as **en**.

   ```
   [Device] pki domain 1
   [Device-pki-domain-1] ca identifier new-ca
   [Device-pki-domain-1] certificate request url
   http://10.1.2.2/certsrv/mscep/mscep.dll
   [Device-pki-domain-1] certificate request from ra
   [Device-pki-domain-1] certificate request entity en
   [Device-pki-domain-1] quit
   ```

   # Create RSA local key pairs.

   ```
   [Device] public-key loc  al create rsa
   ```

   # Retrieve the CA certificate from the certificate issuing server.

   ```
   [Device] pki retrieval-certificate ca domain 1
   ```

   # Request a local certificate from a CA through SCEP for the device.

   ```
   [Device] pki request-certificate domain 1
   ```

   # Create an SSL server policy **myssl**, specify PKI domain 1 for the SSL server policy, and enable certificate-based SSL client authentication.

   ```
   [Device] ssl server-policy myssl
   [Device-ssl-server-policy-myssl] pki-domain 1
   [Device-ssl-server-policy-myssl] client-verify enable
   [Device-ssl-server-policy-myssl] quit
   ```

   # Create a certificate attribute group **mygroup1**, and configure a certificate attribute rule, specifying that the distinguished name in the subject name includes the string of new-ca.

   ```
   [Device] pki certificate attribute-group mygroup1
   [Device-pki-cert-attribute-group-mygroup1] attribute 1 issuer-name dn ctn new-ca
   [Device-pki-cert-attribute-group-mygroup1] quit
   ```

   # Create a certificate attribute-based access control policy **myacp**. Configure a certificate attribute-based access control rule, specifying that a certificate is considered valid when it matches an attribute rule in certificate attribute group **myacp**.

   ```
   [Device] pki certificate access-control-policy myacp
   [Device-pki-cert-acp-myacp] rule 1 permit mygroup1
   [Device-pki-cert-acp-myacp] quit
   ```

   # Associate the HTTPS service with SSL server policy **myssl**.

   ```
   [Device] ip https ssl-server-policy myssl
   ```

Associate the HTTPS service with certificate attribute-based access control policy **myacp**.

```
[Device] ip https certificate access-control-policy myacp
```

Enable the HTTPS service.

```
[Device] ip https enable
```

Create a local user named **usera**, set the password to **123**, specify the Web service type, and specify the user privilege level 3. A level-3 user can perform all operations supported by the device.

```
[Device] local-user usera
[Device-luser-usera] password simple 123
[Device-luser-usera] service-type web
[Device-luser-usera] authorization-attribute level 3
```

2. Configure the host (HTTPS client):

   On the host, run the IE browser, and then enter **http://10.1.2.2/certsrv** in the address bar and request a certificate for the host as prompted.

3. Verify the configuration:

   Enter **https://10.1.1.1** in the address bar, and select the certificate issued by **new-ca**. When the Web login page of the device appears, enter the username **usera** and password **123** to log in to the Web management page.

For more information about PKI configuration commands, SSL configuration commands, and the **public-key local create rsa** command, see *Security Command Reference*.

Logging in through SNMP

You can use an NMS to access the device MIB and perform GET and SET operations to manage and monitor the device. The device supports SNMPv1, SNMPv2c, and SNMPv3, and can work with various network management software products, including IMC. For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

By default, SNMP access is disabled. To enable SNMP access, log in to the device via any other method.

Configuring SNMP login

Connect the PC (the NMS) and the device to the network, making sure they can reach each other, as shown in Figure 22.

Figure 22 Network diagram

IMPORTANT:

This document describes only the basic SNMP configuration procedures on the device. To make SNMP work correctly, make sure the SNMP settings (including the SNMP version) on the NMS are consistent with those on the device.

Prerequisites

- Assign an IP address to a Layer 3 interface on the device.
- Configure routes to make sure the NMS and the Layer 3 interface can reach each other.

Configuring SNMPv3 settings

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the SNMP agent.	**snmp-agent**	Optional. By default, the SNMP agent is disabled. You can enable SNMP agent with this command or any command that begins with **snmp-agent**.

Step	Command	Remarks
3. Configure an SNMP group and specify its access right.	**snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	By default, no SNMP group is configured.
4. Add a user to the SNMP group.	**snmp-agent usm-user v3** *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	N/A

Configuring SNMPv1 or SNMPv2c settings

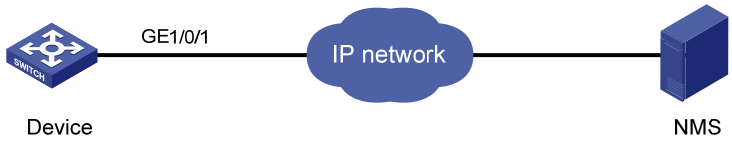
Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable the SNMP agent.	**snmp-agent**	Optional. By default, the SNMP agent is disabled. You can enable SNMP agent with this command or any command that begins with **snmp-agent**.
3. Create or update MIB view information.	**snmp-agent mib-view** { **excluded** | **included** } *view-name oid-tree* [**mask** *mask-value*]	Optional. By default, the MIB view name is ViewDefault and OID is 1.
4. Configure SNMP NMS access right.	• (Approach 1) Specify the SNMP NMS access right directly by configuring an SNMP community: **snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] * • (Approach 2) Configure an SNMP group and add a user to the SNMP group: a. **snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] * b. **snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	Use either approach. The direct configuration approach is for SNMPv1 or SNMPv2c. The community name configured on the NMS should be consistent with the username configured on the agent. The indirect configuration approach is for SNMPv3.

NMS login example

Network requirements

Configure the device and the NMS so you can remotely manage the device through SNMPv3.

Figure 23 Network diagram



Configuration procedure

1. Configure the device:

   # Assign an IP address to the device. Make sure the device and the NMS can reach each other. (Details not shown.)

   # Enter system view.

   ```
   <Sysname> system-view
   ```

   # Enable the SNMP agent.

   ```
   [Sysname] snmp-agent
   ```

   # Configure an SNMP group.

   ```
   [Sysname] snmp-agent group v3 managev3group
   ```

   # Add a user to the SNMP group.

   ```
   [Sysname] snmp-agent usm-user v3 managev3user managev3group
   ```

2. Configure the NMS.

   Details are not shown. For more information, see the NMS manual.

   Make sure the NMS has the same SNMP settings. Otherwise, the device cannot be discovered or managed by the NMS.

Controlling user logins

To harden device security, use ACLs to prevent unauthorized logins. For more information about ACLs, see *ACL and QoS Configuration Guide*.

Controlling Telnet logins (not supported in FIPS mode)

Use a basic ACL (2000 to 2999) to filter Telnet traffic by source IP address. Use an advanced ACL (3000 to 3999) to filter Telnet traffic by source and/or destination IP address. Use an Ethernet frame header ACL (4000 to 4999) to filter Telnet traffic by source MAC address.

To access the device, a Telnet user must match a permit statement in the ACL applied to the user interface.

Configuring source IP-based Telnet login control

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a basic ACL and enter its view, or enter the view of an existing basic ACL.	**acl** [**ipv6**] **number** *acl-number* [**match-order** { **config** | **auto** }]	By default, no basic ACL exists.
3.	Configure an ACL rule.	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name* | **fragment** | **logging**]*	By default, a basic ACL does not contain any rule.
4.	Exit the basic ACL view.	**quit**	N/A
5.	Enter user interface view.	**user-interface** [*type*] *first-number* [*last-number*]	N/A
6.	Use the ACL to control user logins by source IP address.	**acl** [**ipv6**] *acl-number* { **inbound** | **outbound** }	• **inbound**: Filters incoming packets. • **outbound**: Filters outgoing packets.

Configuring source/destination IP-based Telnet login control

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create an advanced ACL and enter its view, or enter the view of an existing advanced ACL.	**acl** [**ipv6**] **number** *acl-number* [**match-order** { **config** | **auto** }]	By default, no advanced ACL exists.

Step		Command	Remarks
3.	Configure an ACL rule.	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	N/A
4.	Exit advanced ACL view.	**quit**	N/A
5.	Enter user interface view.	**user-interface** [*type*] *first-number* [*last-number*]	N/A
6.	Use the ACL to control user logins by source and destination IP addresses.	**acl** [**ipv6**] *acl-number* { **inbound** | **outbound** }	• **inbound**: Filters incoming packets. • **outbound**: Filters outgoing packets.

Configuring source MAC-based Telnet login control

Ethernet frame header ACLs apply to Telnet traffic only if the Telnet client and server are located in the same subnet.

To configure source MAC-based Telnet login control:

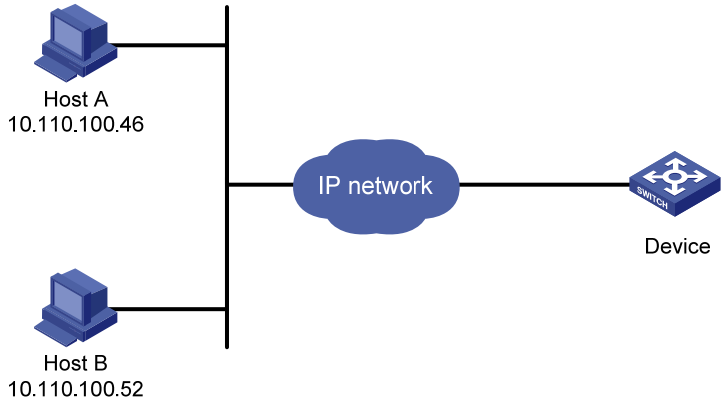
Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create an Ethernet frame header ACL and enter its view.	**acl number** *acl-number* [**match-order** { **config** | **auto** }]	By default, no Ethernet frame header ACL exists.
3.	Configure an ACL rule.	**rule** [*rule-id*] { **permit** | **deny** } *rule-string*	N/A
4.	Exit Ethernet frame header ACL view.	**quit**	N/A
5.	Enter user interface view.	**user-interface** [*type*] *first-number* [*last-number*]	N/A
6.	Use the ACL to control user logins by source MAC address.	**acl** *acl-number* **inbound**	**inbound**: Filters incoming packets.

Telnet login control configuration example

Network requirements

As shown in Figure 24, configure an ACL on the device to permit only incoming Telnet packets sourced from Host A and Host B.

Figure 24 Network diagram



Configuration procedure

Configure basic ACL 2000, and configure rule 1 to permit packets sourced from Host B, and rule 2 to permit packets sourced from Host A.

```
<Sysname> system-view
[Sysname] acl number 2000 match-order config
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-basic-2000] quit
```

Reference ACL 2000 in user interface view to allow Telnet users from Host A and Host B to access the Device.

```
[Sysname] user-interface vty 0 15
[Sysname-ui-vty0-15] acl 2000 inbound
```

Configuring source IP-based SNMP login control

Use a basic ACL (2000 to 2999) to control SNMP logins by source IP address. To access the requested MIB view, an NMS must use a source IP address permitted by the ACL.

Configuration procedure

To configure source IP-based SNMP login control:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a basic ACL and enter its view, or enter the view of an existing basic ACL.	**acl** [**ipv6**] **number** *acl-number* [**name** *name*] [**match-order** { **config** | **auto** }]	By default, no basic ACL exists.
3.	Create an ACL rule.	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name* | **fragment** | **logging**]*	N/A
4.	Exit the basic ACL view.	**quit**	N/A

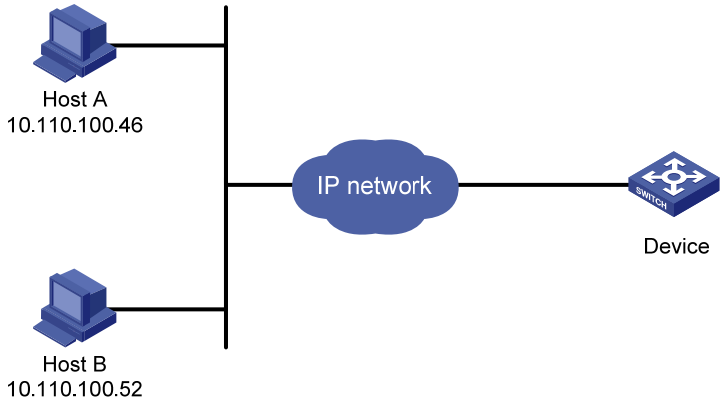
Step	Command	Remarks
5. Apply the ACL to an SNMP community, group or user.	• SNMPv1/v2c community: **snmp-agent community** { **read** | **write** } *community-name* [**mib-view** *view-name*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] * • SNMPv1/v2c group: **snmp-agent group** { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] * • SNMPv3 group: **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] * • SNMPv1/v2c user: **snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] * • SNMPv3 user: **snmp-agent usm-user v3** *user-name group-name* [[**cipher**] **authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **3des** | **aes128** | **des56** } *priv-password*]] [**acl** *acl-number* | **acl ipv6** *ipv6-acl-number*] *	For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

SNMP login control configuration example

Network requirements

As shown in Figure 25, configure the device to allow only NMS users from Host A and Host B to access.

Figure 25 Network diagram



Configuration procedure

Create ACL 2000, and configure rule 1 to permit packets sourced from Host B, and rule 2 to permit packets sourced from Host A.

```
<Sysname> system-view
[Sysname] acl number 2000 match-order config
[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0
[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0
[Sysname-acl-basic-2000] quit
```

Associate the ACL with the SNMP community and the SNMP group.

```
[Sysname] snmp-agent community read aaa acl 2000
[Sysname] snmp-agent group v2c groupa acl 2000
[Sysname] snmp-agent usm-user v2c usera groupa acl 2000
```

Configuring Web login control (not supported in FIPS mode)

Use a basic ACL (2000 to 2999) to filter HTTP traffic by source IP address for Web login control. To access the device, a Web user must use an IP address permitted by the ACL.

You can also log off suspicious Web users who have been logged in.

Configuring source IP-based Web login control

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a basic ACL and enter its view, or enter the view of an existing basic ACL.	**acl** [**ipv6**] **number** *acl-number* [**match-order** { **config** | **auto** }]	By default, no basic ACL exists.
3.	Create rules for this ACL.	**rule** [*rule-id*] { **permit** | **deny** } [**source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name* | **fragment** | **logging**]*	N/A
4.	Exit the basic ACL view.	**quit**	N/A
5.	Associate the HTTP or HTTPS service with the ACL.	• **ip http acl** *acl-number* • **ip https acl** *acl-number*	HTTP and HTTPS are independent of each other. Configure one or both of the commands as required.

Logging off online Web users

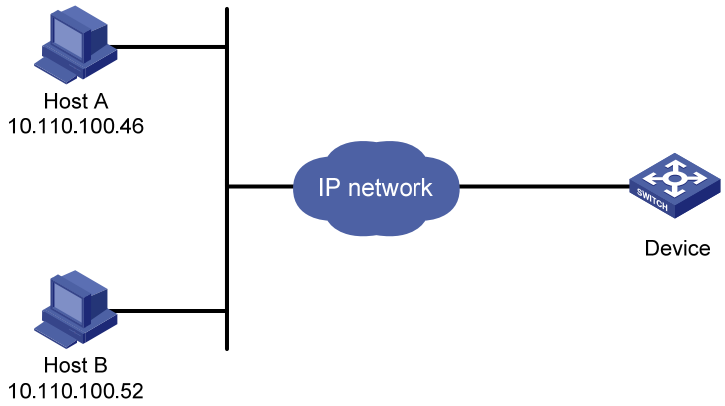
Task	Command	Remarks
Log off online Web users.	**free web-users** { **all** | **user-id** *user-id* | **user-name** *user-name* }	Available in user interface view

Web login control configuration example

Network requirements

As shown in Figure 26, configure the device to allow only Web users from Host B to access.

Figure 26 Network diagram



Configuration procedure

Create ACL 2000, and configure rule 1 to permit packets sourced from Host B.

```
<Sysname> system-view
[Sysname] acl number 2030 match-order config
[Sysname-acl-basic-2030] rule 1 permit source 10.110.100.52 0
```

Associate the ACL with the HTTP service so only Web users from Host B are allowed to access the device.

```
[Sysname] ip http acl 2030
```

Configuring FTP

File Transfer Protocol (FTP) is an application layer protocol based on the client/server model. It is used to transfer files from one host to another over a TCP/IP network.

FTP server uses TCP port 20 to transfer data and TCP port 21 to transfer control commands. For more information about FTP, see RFC 959.

FTP supports the following transfer modes:

- **Binary mode**—Used to transfer image files, such as **.app** and **.bin** files.
- **ASCII mode**—Used to transfer text files, such as **.txt**, **.bat**, and **.cfg** files.

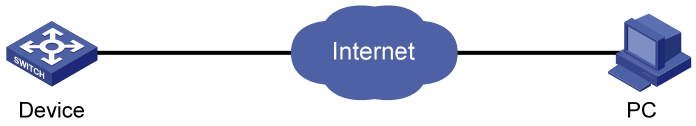
FTP can operate in either of the following modes:

- **Active mode (PORT)**—The FTP server initiates the TCP connection. This mode is not suitable when the FTP client is behind a firewall, for example, when the FTP client resides in a private network.
- **Passive mode (PASV)**—The FTP client initiates the TCP connection. This mode is not suitable when the server does not allow the client to use a random unprivileged port greater than 1024.

The FTP operation mode varies depending on the FTP client program.

The device can act as the FTP client or FTP server:

Figure 27 FTP application scenario



FIPS compliance

FTP is not supported in FIPS mode.

Using the device as an FTP client

To connect to an FTP server or enter FTP client view, make sure the following requirements are met:

- You have level-3 (Manage) user privileges on the device. In FTP client view, whether a directory or file management command can be successfully executed depends on the authorization set on the FTP server.
- The device and the FTP server can reach each other.
- You have a user account (including the username, password, and authorization) on the FTP server. If the FTP server supports anonymous FTP, you can directly access the FTP server without a username and password.

Establishing an FTP connection

To access an FTP server, use the **ftp** command in user view or use the **open** command in FTP client view to establish a connection to the FTP server.

You can use the **ftp client source** command to specify a source IP address or source interface for the FTP packets sent by the device. If a source interface (typically a loopback interface) is specified, its primary IP address is used as the source IP address for the FTP packets sent by the device. The source interface setting and the source IP address setting overwrite each other.

The **ftp client source** command setting applies to all FTP sessions. When you set up an FTP session by using the **ftp** or **ftp ipv6** command, you can also specify a different source IP address for the FTP session.

IMPORTANT:

To avoid FTP connection failures, when you specify a source interface for FTP packets, make sure the interface has been assigned a primary IP address.

To establish an IPv4 FTP connection:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Specify a source IP address for outgoing FTP packets.	**ftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	Optional. By default, the primary IP address of the output interface is used as the source IP address.
3. Return to user view.	**quit**	N/A
4. Log in to the FTP server.	• (Approach 1) Log in to the FTP server in user view: **ftp** [*server-address* [*service-port*]] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]] • (Approach 2) Log in to the FTP server in FTP client view: a. **ftp** b. **open** server-address [service-port]	Use either approach. Only 5500 EI switches support the **vpn-instance** *vpn-instance-name* option.

To establish an IPv6 FTP connection, perform one of the following tasks:

Task	Command	Remarks
Log in to the FTP server from user view.	**ftp ipv6** [*server-address* [*service-port*]] [**vpn-instance** *vpn-instance-name*] [**source ipv6** *source-ipv6-address*] [**-i** *interface-type interface-number*]]	Only HP 5500 EI switches support the **vpn-instance** *vpn-instance-name* option.
Log in to the FTP server from FTP client view.	1. **ftp ipv6** 2. **open ipv6** *server-address* [*service-port*] [**-i** *interface-type interface-number*]	

Setting the DSCP value for IP to use for outgoing FTP packets

You can set the DSCP value for IPv4 or IPv6 to use for outgoing FTP packets on an FTP client, so outgoing FTP packets are forwarded based on their priorities on transit devices.

To set the DSCP value for IP to use for outgoing FTP packets:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Set the DSCP value for IP to use for outgoing FTP packets.	• For IPv4: **ftp client dscp** *dscp-value* • For IPv6: **ftp client ipv6 dscp** *dscp-value*	The default is 0, whether the FTP client is running IPv4 or IPv6.

Managing directories on the FTP server

After the device establishes a connection to an FTP server, you can create or delete folders in the authorized directory on the FTP server.

To manage the directories on the FTP server:

Task	Command
Display detailed information about files and directories under the current directory on the FTP server.	**dir** [*remotefile* [*localfile*]]
Query a directory or file on the FTP server.	**ls** [*remotefile* [*localfile*]]
Change the working directory on the FTP server.	**cd** { *directory* | **..** | **/** }
Return to the upper level directory on the FTP server.	**cdup**
Display the current directory on the FTP server.	**pwd**
Create a directory on the FTP server.	**mkdir** *directory*
Remove the specified working directory on the FTP server.	**rmdir** *directory*

Working with the files on the FTP server

After you log in to the server, you can upload a file to or download a file from the authorized directory by following these steps:

1. Use the **dir** or **ls** command to display the directory and the location of the file on the FTP server.
2. Delete unused files to get more free storage space.
3. Set the file transfer mode. FTP transmits files in two modes: ASCII and binary. Use ASCII mode to transfer text files. Use binary mode to transfer image files.
4. Use the **lcd** command to display the local working directory of the FTP client. You can upload the file or save the downloaded file in this directory.
5. Upload or download the file.

To work with the files on the FTP server:

Task	Command	Remarks
Display detailed information about a directory or file on the FTP server.	**dir** [*remotefile* [*localfile*]]	The **ls** command displays the name of a directory or file only, while the **dir** command displays detailed information such as the file size and creation time.
Query a directory or file on the FTP server.	**ls** [*remotefile* [*localfile*]]	The **ls** command displays the name of a directory or file only, while the **dir** command displays detailed information such as the file size and creation time.
Delete the specified file on the FTP server permanently.	**delete** *remotefile*	N/A
Set the file transfer mode to ASCII.	**ascii**	By default, ASCII mode is used.
Set the file transfer mode to binary.	**binary**	By default, ASCII mode is used.
Set the FTP operation mode to passive.	**passive**	By default, passive mode is used
Display the local working directory of the FTP client.	**lcd**	N/A
Upload a file to the FTP server.	**put** *localfile* [*remotefile*]	N/A
Download a file from the FTP server.	**get** *remotefile* [*localfile*]	N/A

Switching to another user account

After you log in to the FTP server with one user account, you can switch to another user account to get a different privilege without reestablishing the FTP connection. You must correctly enter the new username and password. A wrong username or password can cause the FTP connection to disconnect.

To switch to another user account:

Task	Command
Change the username after FTP login.	**user** *username* [*password*]

Maintaining and troubleshooting the FTP connection

Task	Command	Remarks
Display the help information of FTP-related commands on the FTP server.	**remotehelp** [*protocol-command*]	N/A
Enable displaying detailed prompt information received from the server.	**verbose**	Enabled by default.
Enable FTP related debugging when the device acts as the FTP client.	**debugging**	Disabled by default.

Terminating the FTP connection

To terminate an FTP connection, perform one of the following tasks:

Task	Command	Remarks
Terminate the FTP connection without exiting FTP client view.	• **disconnect** • **close**	Use either command in FTP client view.
Terminate the FTP connection and return to user view.	• **bye** • **quit**	Use either command in FTP client view.

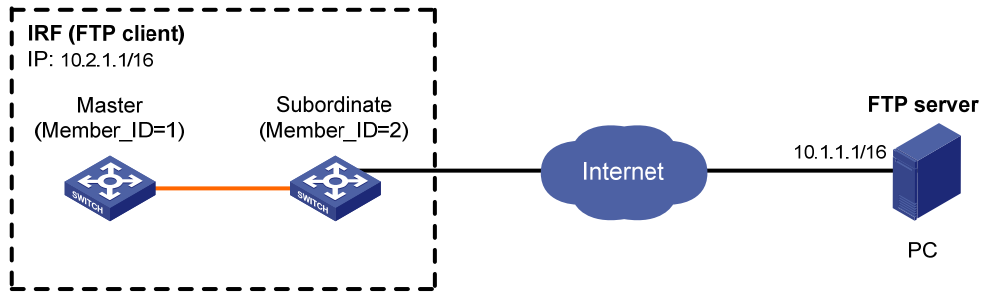
FTP client configuration example

Network requirements

As shown in Figure 28, the IRF fabric that comprises two member devices acts as the FTP client and the PC acts as the FTP server. The IRF fabric and the PC can reach each other. An account with the username **abc** and password **abc** is already configured on the FTP server.

Log in to the FTP server from the FTP client, download the file **newest.bin** from the FTP server to the FTP client, and upload the configuration file **config.cfg** from the FTP client to the FTP server for backup.

Figure 28 Network diagram



Note: The orange line represents an IRF link.

Configuration procedure

Examine the storage medium of the device for insufficiency or impairment. If no sufficient free space is available, use the **delete/unreserved** *file-url* command to delete unused files. (Details not shown.)

Log in to the server at 10.1.1.1 through FTP.

```
<Sysname> ftp 10.1.1.1
Trying 10.1.1.1 ...
Connected to 10.1.1.1.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(10.1.1.1:(none)):abc
331 Give me your password, please
Password:
230 Logged in successfully
```

Set the file transfer mode to binary.

```
[ftp] binary
200 Type set to I.
```

Download the system software image file **newest.bin** from the PC to the IRF fabric:

- Download the file **newest.bin** from the PC to the Flash root directory of the master device.

  ```
  [ftp] get newest.bin
  ```

- Download the file **newest.bin** from the PC to the Flash root directory of the subordinate device (with member ID of 2).

  ```
  [ftp] get newest.bin slot2#flash:/newest.bin
  ```

Set the transfer mode to ASCII and upload the configuration file **config.cfg** from the IRF fabric to the PC for backup.

```
[ftp] ascii
[ftp] put config.cfg back-config.cfg
227 Entering Passive Mode (10,1,1,1,4,2).
125 ASCII mode data connection already open, transfer starting for /config.cfg.
226 Transfer complete.
FTP: 3494 byte(s) sent in 5.646 second(s), 618.00 byte(s)/sec.
[ftp] bye
221 Server closing.
```

Specify **newest.bin** as the main system software image file for the next startup of all member devices.

```
<Sysname> boot-loader file newest.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot 1!
  The specified file will be used as the main boot file at the next reboot on slot 2!
```

IMPORTANT:

The system software image file used for the next startup must be saved in the Flash root directory. You can copy or move a file to the Flash root directory.

Reboot the device, and the system software image file is updated at the system reboot.

```
<Sysname> reboot
```

Using the device as an FTP server

If the device is operating as an FTP server, make sure the following requirements are met to ensure successful FTP operations:

- The device and the FTP server can reach each other.
- Configure a user account (including the username, password, and authorization) on the device or a remote authentication server for an FTP user. This task is required because the device does not support anonymous FTP for security reasons. By default, authenticated users can access the root directory of the device.
- The FTP user provides the correct username and password.

NOTE:

When you use the Internet Explorer browser to log in to the device operating as an FTP server, some FTP functions are not available. This is because multiple connections are required during the login process but the device supports only one connection at a time.

Configuring basic parameters

The FTP server uses one of the following modes to update a file when you upload the file (using the **put** command) to the FTP server:

- **Fast mode**—The FTP server starts writing data to the Flash after a file is transferred to the memory. This prevents the existing file on the FTP server from being corrupted in the event that anomaly, such as a power failure, occurs during a file transfer.
- **Normal mode**—The FTP server writes data to the Flash while receiving data. This means that any anomaly, such as a power failure, during file transfer might result in file corruption on the FTP server. This mode, however, consumes less memory space than the fast mode.

To configure basic parameters for the FTP server:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable the FTP server.	**ftp server enable**	By default, the FTP server is disabled.
3.	Set the DSCP value for IPv4 to use for outgoing FTP packets.	**ftp server dscp** *dscp-value*	Optional. The default is 0.
4.	Use an ACL to control FTP access.	**ftp server acl** *acl-number*	Optional. By default, no ACL is used for access control.
5.	Configure the idle-timeout timer.	**ftp timeout** *minutes*	Optional. The default idle-timeout timer is 30 minutes. If no data is transferred within the idle-timeout time, the connection is terminated.
6.	Set the file update mode for the FTP server.	**ftp update** { **fast** | **normal** }	Optional. By default, normal update is used.
7.	Return to user view.	**quit**	N/A
8.	Release the FTP connection established by a specific user.	**free ftp user** *username*	Optional.

Configuring authentication and authorization

Perform this task on the FTP server to authenticate FTP clients and specify the directories that authenticated clients can access.

The following authentication modes are available:

- **Local authentication**—The device looks up the client's username and password in the local user account database. If a match is found, authentication succeeds.
- **Remote authentication**—The device sends the client's username and password to a remote authentication server for authentication. If this approach is used, the user account is configured on the remote authentication server rather than the device.

To assign an FTP user write access (including upload, delete, and create) to the device, assign level-3 (Manage) user privileges to the user. For read-only access to the file system, any user privilege level is OK.

For more information, see *Security Configuration Guide*.

To configure authentication and authorization for the FTP server:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a local user account and enter its view.	**local-user** *user-name*	By default, no local user account authorized with the FTP service exists, and the system does not support FTP anonymous user access.
3.	Set a password for the user account.	**password** [[**hash**] { **cipher** | **simple** } *password*]	N/A
4.	Assign FTP service to the user account	**service-type ftp**	By default, no service type is specified. If the FTP service is specified, the root directory of the device is by default used.
5.	Configure authorization attributes.	**authorization-attribute** { **acl** *acl-number* | **callback-number** *callback-number* | **idle-cut** *minute* | **level** *level* | **user-profile** *profile-name* | **user-role** { **guest** | **guest-manager** | **security-audit** } | **vlan** *vlan-id* | **work-directory** *directory-name* } *	Optional. By default, the FTP users can access the root directory of the device, and the user level is 0. You can change the default configuration by using this command.

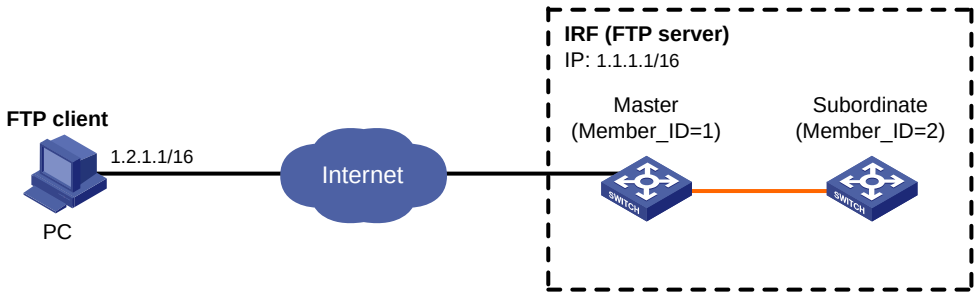
For more information about the **local-user**, **password**, **service-type ftp**, and **authorization-attribute** commands, see *Security Command Reference*.

FTP server configuration example

Network requirements

Create a local user account with username **abc** and password **abc** and enable FTP server on the IRF fabric in Figure 29. Use the user account to log in to the FTP server from the FTP client, upload the file **newest.bin** from the FTP client to the FTP server, and download the configuration file **config.cfg** from the FTP server to the FTP client for backup.

Figure 29 Network diagram



Note: The orange line represents an IRF link.

Configuration procedure

1. Configure the FTP server:

   # Examine the storage medium of the device for insufficiency or impairment. If no sufficient free space is available, use the **delete/unreserved** *file-url* command to delete unused files. (Details not shown.)

   # Create a local user account **abc**, set its password to **abc** and the user privilege level to level 3 (the manage level), specify the Flash root directory of the master device as the authorized directory, and specify the service type as FTP.

   ```
   <Sysname> system-view
   [Sysname] local-user abc
   [Sysname-luser-abc] password simple abc
   [Sysname-luser-abc] authorization-attribute level 3
   [Sysname-luser-abc] authorization-attribute work-directory flash:/
   [Sysname-luser-abc] service-type ftp
   [Sysname-luser-abc] quit
   ```

   To access the Flash root directory of the subordinate device (with the member ID 2), replace **flash:/** in the command **authorization-attribute work-directory flash:/** with **slot2#flash:/**.

   # Enable the FTP server.

   ```
   [Sysname] ftp server enable
   [Sysname] quit
   ```

2. Perform FTP operations from the FTP client:

   # Log in to the FTP server at 1.1.1.1 by using the username **abc** and password **abc**.

   ```
   c:\> ftp 1.1.1.1
   Connected to 1.1.1.1.
   220 FTP service ready.
   User(1.1.1.1:(none)):abc
   331 Password required for abc.
   Password:
   230 User logged in.
   ```

   # Download the configuration file **config.cfg** from the FTP server to the PC for backup.

   ```
   ftp> get config.cfg back-config.cfg
   ```

   # Upload the file **newest.bin** to the Flash root directory of the master.

   ```
   ftp> put newest.bin
   200 Port command okay.
   150 Opening ASCII mode data connection for /newest.bin.
   226 Transfer complete.
   ftp> bye
   221 Server closing.

   c:\>
   ```

   This FTP procedure also applies to upgrading configuration files.

   After you finish upgrading the Boot ROM image through FTP, execute the **bootrom update** command to upgrade Boot ROM.

3. Upgrade the FTP server:

   # Copy the system software image file **newest.bin** to the Flash root directory of the subordinate device (with the member ID 2).

```
<Sysname> copy newest.bin slot2#flash:/
```

Specify **newest.bin** as the main system software image file for the next startup of all member devices.

```
<Sysname> boot-loader file newest.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot on slot
1!
  The specified file will be used as the main boot file at the next reboot on slot
2!
```

IMPORTANT:

The system software image file used for the next startup and the startup configuration file must be saved in the Flash root directory. You can copy or move a file to the Flash root directory.

Reboot the IRF fabric and the system software image file is updated at the system reboot.

```
<Sysname> reboot
```

Displaying and maintaining FTP

Task	Command	Remarks
Display the source IP address configuration of the FTP client.	**display ftp client configuration** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the FTP server configuration.	**display ftp-server** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display online FTP user information.	**display ftp-user** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Configuring TFTP

Trivial File Transfer Protocol (TFTP) is a simplified version of FTP for file transfer over secure reliable networks. TFTP uses UDP port 69 for connection establishment and data transmission. In contrast to TCP-based FTP, TFTP requires no authentication or complex message exchanges, and is easier to deploy.

TFTP supports the following transfer modes:

- **Binary mode**—Used to transfer image files, such as **.app** and **.bin .btm** files.
- **ASCII mode**—Used to transfer text files, such as **.txt**, **.bat**, and **.cfg** files.

The device can operate only as a TFTP client (see Figure 30) to upload or download files.

Figure 30 TFTP application scenario

FIPS compliance

TFTP is not supported in FIPS mode.

Prerequisites

Run a TFTP server program on the file host and set a TFTP working directory.

Configure IP addresses and routes to make sure the device and the TFTP server can reach each other.

Using the device as a TFTP client

The device provides the following modes for downloading a new file from a TFTP server:

- **Normal download**—The new file is written directly to Flash and overwrites the old file that has the same name as it. If file download is interrupted, both old and new files are lost.
- **Secure download**—The new file is downloaded to memory and will not be written to Flash until the whole file is obtained. A download failure does not affect the old file that has the same name as the old file.

To avoid undesired file loss, use the secure download mode. If you use the normal download mode because of insufficient memory, assign the new file a file name unique in Flash.

You can use the **tftp client source** command to specify a source IP address or source interface for the TFTP packets sent by the device. If a source interface (typically, a loopback interface) is specified, its primary IP address is used as the source IP address for the TFTP packets. The source interface setting and the source IP address setting overwrite each other.

The **tftp client source** command setting applies to all TFTP sessions. When you set up a TFTP session with the **tftp** command, you can also specify a different source IP address for the TFTP session.

IMPORTANT:

To avoid TFTP connection failures, when you specify a source interface for TFTP packets, make sure the interface has a primary IP address.

To configure the TFTP client:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Use an ACL to control the client's access to TFTP servers.	**tftp-server** [**ipv6**] **acl** *acl-number*	Optional. By default, no ACL is used for access control.
3.	Specify a source IP address for outgoing TFTP packets.	**tftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }	Optional. By default, the primary IP address of the output interface is used as the source IP address.
4.	Set the DSCP value for IP to use for outgoing TFTP packets.	• For IPv4: **tftp client dscp** *dscp-value* • For IPv6: **tftp client ipv6 dscp** *dscp-value*	Optional. The default is 0, whether the TFTP client is running IPv4 or IPv6.
5.	Return to user view.	**quit**	N/A
6.	Download or upload a file.	• For IPv4: **tftp** *server-address* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }] • For IPv6: **tftp ipv6** *tftp-ipv6-server* [**-i** *interface-type interface-number*] { **get** | **put** } *source-filename* [*destination-filename*] [**vpn-instance** *vpn-instance-name*]	Optional. Only HP 5500 EI switches support the **vpn-instance** *vpn-instance-name* option.

Displaying and maintaining the TFTP client

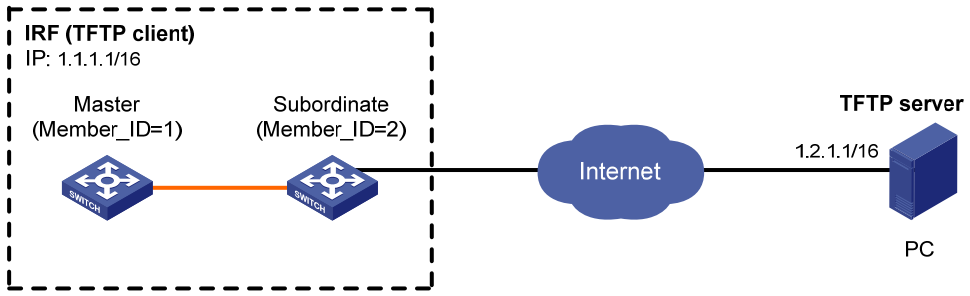
Task	Command	Remarks
Display the source IP address configuration of the TFTP client.	**display tftp client configuration** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

TFTP client configuration example

Network requirements

Configure the PC in Figure 31 as a TFTP server, and use TFTP to download the system software image file **newest.bin** from the TFTP server to the client and upload the configuration file **config.cfg** from the TFTP client to the server for backup.

Figure 31 Network diagram



Note: The orange line represents an IRF link.

Configuration procedure

This configuration procedure assumes that the PC and the IRF fabric can reach each other.

1. Configure the PC (TFTP server):
   - Enable the TFTP server. (Details not shown.)
   - Configure a TFTP working directory. (Details not shown.)
2. Configure the IRF fabric (TFTP client):

   # Examine the storage medium of the device for insufficiency or impairment. If no sufficient free space is available, use the **delete/unreserved** *file-url* command to delete unused files. (Details not shown.)

   # Download system software image file **newest.bin** from the PC to the master and subordinate devices:

   - Download system software image file **newest.bin** from the PC to the root directory of the Flash on the master.

     ```
     <Sysname> tftp 1.2.1.1 get newest.bin
     ```

   - Download system software image file **newest.bin** from the PC to the root directory of the Flash on a subordinate device (with the member ID 2).

     ```
     <Sysname> tftp 1.2.1.1 get newest.bin slot2#flash:/newest.bin
     ```

   # Upload a configuration file **config.cfg** to the TFTP server.

   ```
   <Sysname> tftp 1.2.1.1 put config.cfg configback.cfg
   ```

   # Specify **newest.bin** as the main system software image file for the next startup for all member devices.

   ```
   <Sysname> boot-loader file newest.bin slot all main
     This command will set the boot file of the specified board. Continue? [Y/N]:y
     The specified file will be used as the main boot file at the next reboot on slot
   1!
     The specified file will be used as the main boot file at the next reboot on slot
   2!
   ```

IMPORTANT:

The system software image file used for the next startup must be saved in the Flash root directory. You can copy or move a file to the Flash root directory.

Reboot the IRF fabric and the software is upgraded.

```
<Sysname> reboot
```

Managing the file system

This chapter describes how to manage the device's file system, including the storage media, directories and files.

Storage medium naming rules

A storage medium is named based on the following rules:

- If a storage medium is the only storage medium of its type on the device, it is named by its type. For example, if the device has only one Flash, the name of the Flash is **flash**.
- If multiple storage media of the same type exist on the device, the physical device name of a storage medium is composed of the storage medium type and the sequence number of the storage medium. A sequence number is an English letter such as a, b, or c.
- If a storage medium is partitioned, the name of a partition is composed of the physical device name and the partition number. The sequence numbers of partitions are numbers such as 0, 1 and 2.

File name formats

When you specify a file, enter the file name in one of the formats shown in Table 18.

Table 18 File name formats

Format	Description	Length	Example
file-name	Specifies a file in the current working directory.	1 to 91 characters	a.cfg indicates a file named **a.cfg** in the current working directory. This working directory might be on the master device or a subordinate device.
path/file-name	Specifies a file in a specific folder in the current working directory. The *path* argument represents the path to the file. If the file is in a single-level folder, specify the folder name for the argument. If the file is in a nested folder, separate each folder name by a forward slash (/).	1 to 135 characters	test/a.cfg indicates a file named **a.cfg** in the **test** folder in the current working directory.

Format	Description	Length	Example
drive:/[path]/file-name	Specifies a file in a specific storage medium on the device. The *drive* argument represents the storage medium name. The storage medium on the master is typically flash. The storage medium on a subordinate device is typically slotX#flash, where X represents the member ID of the subordinate device, for example, slot2#flash. To view the correspondence between a device and its member ID, use the **display irf** command.	1 to 135 characters	flash:/test/a.cfg indicates a file named **a.cfg** in the **test** folder in the root directory of the Flash memory on the master. To access the file **a.cfg** in the root directory of the Flash on the subordinate device with member ID 2, enter **slot2#flash:/a.cfg** for the file name.

Managing files

CAUTION:

To avoid file system corruption, do not plug or unplug storage media or perform active/standby switchover while the system is processing a file operation.

You can display directory or file information; display file contents; rename, copy, move, remove, restore, and delete files.

The copy operation enables you to create a file. You can also create a file by performing the download operation or using the **save** command.

Displaying file information

Perform this task in user view.

Task	Command
Display file or directory information.	**dir** [**/all**] [*file-url* | **/all-filesystems**]

Displaying file contents

Perform this task in user view.

Task	Command	Remarks
Display the contents of a file.	**more** *file-url*	Only text files can be displayed.

Renaming a file

Perform this task in user view.

Task	Command
Rename a file.	**rename** *fileurl-source fileurl-dest*

Copying a file

Perform this task in user view.

Task	Command
Copy a file.	**copy** *fileurl-source fileurl-dest*

Moving a file

Perform this task in user view.

Task	Command
Move a file.	**move** *fileurl-source fileurl-dest*

Deleting/restoring a file

You can delete a file permanently or just move it to the recycle bin. A file moved to the recycle bin can be restored, but a file permanently deleted cannot.

A file in the recycle bin occupies storage space. To release the occupied space, execute the **reset recycle-bin** command in the directory that holds the file. To save storage space, periodically empty the recycle bin with the **reset recycle-bin** command.

Perform the following tasks in user view:

Task	Command
Delete a file by moving it to the recycle bin.	**delete** *file-url*
Restore a file from the recycle bin.	**undelete** *file-url*
Delete a file permanently.	**delete /unreserved** *file-url*

Emptying the recycle bin

Step	Command	Remarks
1. Enter the original working directory of the file to be deleted in user view.	**cd** { *directory* | **..** | **/** }	Skip this step if the original directory of the file to be deleted is the current working directory.
2. Empty the recycle bin.	**reset recycle-bin** [**/force**]	N/A

Verifying the correctness and integrity of a file

Task	Command	Remarks
Verify the correctness and integrity of a file.	**crypto-digest sha256 file** *file-url*	Available in user view.

Managing directories

You can create or remove a directory, display or change the current working directory, and display a specific directory.

Displaying directory information

Perform this task in user view.

Task	Command
Display directory or file information.	**dir** [**/all**] [*file-url* | **/all-filesystems**]

Displaying the current working directory

Perform this task in user view.

Task	Command
Display the current working directory.	**pwd**

Changing the current working directory

Perform this task in user view.

Task	Command
Change the current working directory.	**cd** { *directory* | **..** | **/** }

Creating a directory

Perform this task in user view.

Task	Command
Create a directory.	**mkdir** *directory*

Removing a directory

Before you remove a directory, you must delete all files and subdirectories in this directory. To delete a file, use the **delete** command; to delete a subdirectory, use the **rmdir** command.

The **rmdir** command automatically deletes the files in the recycle bin in the current directory.

Perform this task in user view.

Task	Command
Remove a directory.	**rmdir** *directory*

Managing storage media

Managing storage medium space

When the space of a storage medium becomes inaccessible, you can use the **fixdisk** command to examine the medium for damage and repair any damage.

The **format** command formats the storage medium, and all data on the storage medium is deleted.

CAUTION:

After a storage medium is formatted, all files on it are erased and cannot be restored. If a startup configuration file exists on the storage medium, formatting the storage medium results in loss of the startup configuration file.

To manage the space of a storage medium, perform the following tasks in user view:

Task	Command	Remarks
Repair a storage medium.	**fixdisk** *device*	N/A
Format a storage medium.	**format** *device*	N/A

Performing batch operations

A batch file comprises a set of executable commands. Executing a batch file is the same as executing the commands one by one. However, execution of a batch file does not guarantee successful execution of every command in the batch file. If a command has error settings or the conditions for executing the command are not satisfied, the system skips this command.

You can edit a batch file with any extension on your PC, and then upload or download it to the device to execute it.

To execute a batch file:

Step	Command
1. Enter system view.	**system-view**
2. Execute a batch file.	**execute** *filename*

Setting the file system operation mode

The file systems support the following operation modes:

- **alert**—The system warns you about operations that might cause problems such as file corruption and data loss. To prevent incorrect operations, use the **alert** mode.

- **quiet**—The system does not prompt for any operation confirmation.

To set the file system operation mode:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Set the file system operation mode.	**file prompt** { **alert** | **quiet** }	Optional. The default is **alert**.

File system management examples

Display the files and the subdirectories in the current directory.

```
<Sysname> dir
Directory of flash:/
   0     -rw-  13308645  Mar 22 2011 11:34:07   main.bin
   1     -rw-      7380  Mar 25 2011 10:47:36   patch-package.bin
   2     -rw-       228  Mar 25 2011 10:50:39   patchstate
   3     -rw-      3921  Apr 01 2011 17:56:30   startup.cfg
   4     -rw-       151  Apr 01 2011 17:56:24   system.xml
15240 KB total (2521 KB free)
```

Create new folder **mytest** in the test directory.

```
<Sysname> cd test
<Sysname> mkdir mytest
%Created dir flash:/test/mytest.
```

Display the current working directory.

```
<Sysname> pwd
flash:/test
```

Display the files and the subdirectories in the test directory.

```
<Sysname> dir
Directory of flash:/test/
   0   drw-         -  Apr 01 2011 18:28:14   mytest
15240 KB total (2519 KB free)
```

Return to the upper directory.

```
<Sysname> cd ..
```

Display the current working directory.

```
<Sysname> pwd
flash:
```

Managing configuration files

You can use the CLI or the Boot menu to manage configuration files. This chapter explains how to manage configuration files from the CLI.

Overview

A configuration file saves a set of commands for configuring software features on the device. You can save any configuration to a configuration file so they can survive a reboot. You can also back up configuration files to a host for future use.

Configuration types

The configuration loaded at startup is called "startup configuration" and the configuration that is running on the device is called "running configuration."

Startup configuration

The device uses startup configuration to configure software features during startup.

The following are sources of startup configuration:

- **Initial settings**—Initial values or states for parameters. If the device starts up with empty configuration, all parameters are set to their initial settings at startup.
- **Default configuration file**—Contains product-specific default settings that are different from initial default settings. The file is included in the .bin software image file. If you do not configure the device to start up with empty configuration or a startup configuration file, the device loads the default configuration file to configure features at startup. If a parameter is not included in the file, the device loads its initial setting.
- **Startup configuration file**—Configuration file you specify in the Boot menu or CLI for startup. The file is called the "next-startup configuration file." After the file is loaded at startup, it is also called the "current startup configuration file." For high availability, you can specify two next-startup configuration files, one main and one backup (see "Specifying a configuration file for the next startup").

No commands are available to display the initial default settings. For more information about these settings, see the command references.

To display the product-specific default settings, use the **display default-configuration** command.

To display the current startup configuration file and the next-startup configuration files, use the display startup command.

To display the contents of the main next-startup configuration file, use the display saved-configuration command. This command does not display settings that have not been saved to the main next-startup configuration file.

Running configuration

Running configuration includes startup settings that have not been changed and new settings you have made. It is stored in a volatile storage medium and takes effect while the device is operating.

New settings take effect immediately, but they must be saved to a configuration file to survive a reboot.

To view the running configuration, including settings that have not been saved yet, use the display current-configuration command. The displayed configuration does not include parameters that use initial settings.

Configuration file format and content

IMPORTANT:

To run on the device, a configuration file must meet the content and format requirements of the device. To ensure a successful configuration loading at startup, use a configuration file that was automatically created on the device or created by using the **save** command. If you edit the configuration file, make sure all edits are compliant with the requirements of the device.

A configuration file must meet the following requirements:

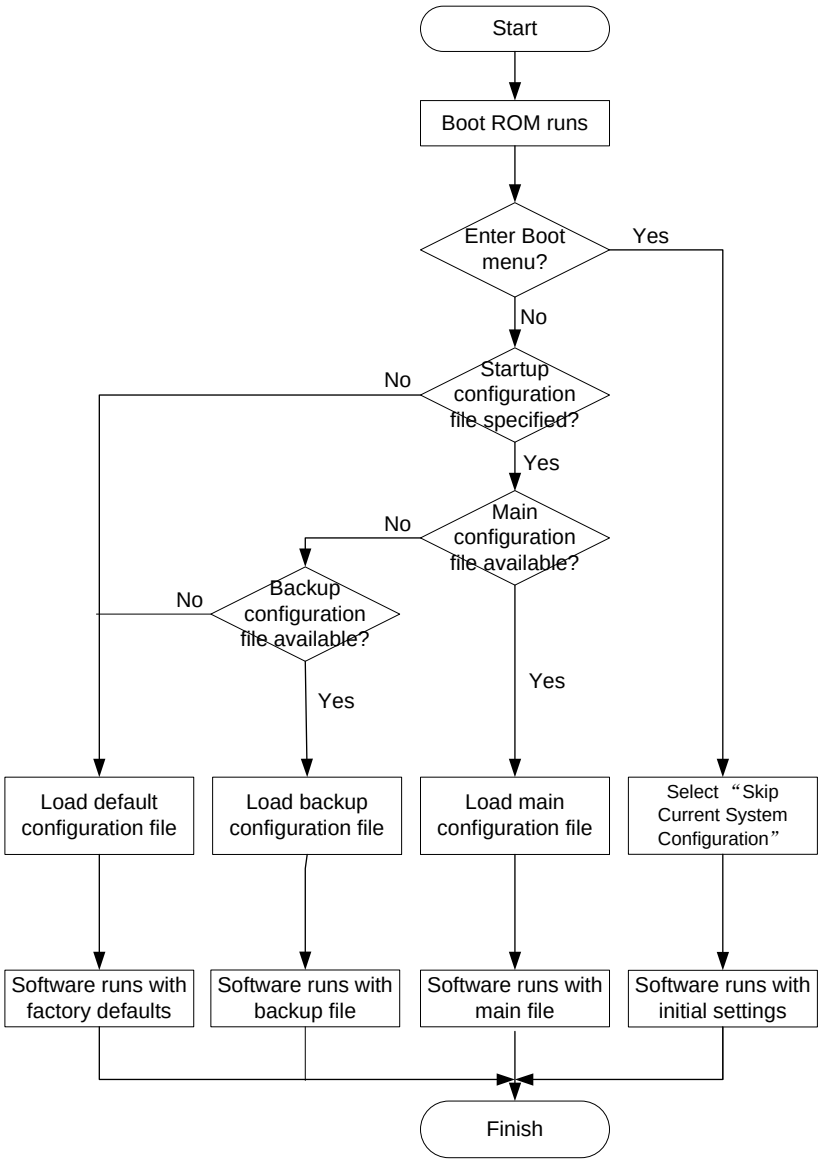
- All commands are saved in their complete form.
- Commands are sorted in sections by view, typically in this order: system view, interface view, protocol views, and user interface view.
- Sections are separated with one or more blank lines or comment lines that start with a pound sign (#).
- The configuration file ends with the word **return**.

You can execute the **save** command to save the running configuration to a configuration file. To make sure the configuration file can be loaded, HP recommends that you not edit the content and format of the configuration file.

Startup configuration loading process

Figure 32 shows the configuration loading process during startup.

Figure 32 Configuration loading process during startup



The device uses the following process to select the startup configuration file to load at startup:

1. If you access the Boot menu to select the **Skip Current System Configuration** option, the device starts up with empty configuration. All parameters are set to their initial settings.
2. If you do not start the device with empty configuration, the following process applies:
   a. If you have specified a main startup configuration file, and this configuration file is available, the device starts up with the main startup configuration file.
   b. If you have not specified a main startup configuration file, or the specified main startup configuration file is not available, the device starts up with the backup startup configuration file.
   c. If you have not specified a backup startup configuration file, or the specified backup startup configuration file is not available, the device starts up with the default configuration file (factory defaults).

FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Saving the running configuration

To make configuration changes take effect at the next startup of the device, save the running configuration to the startup configuration file to be used at the next startup before the device reboots.

Complete these tasks to save the current configuration:

Task	Remarks
Enabling configuration file auto-update	Optional. Perform this task to ensure configuration consistency across member devices.
Saving configuration by using different methods	Required.

The task described in "Using automatic configuration backup after a software upgrade" is automatically performed the first time you use the **save** command to save the running configuration to the next-startup configuration file that contains settings incompatible with the software version after a software upgrade.

Enabling configuration file auto-update

The configuration auto-update function enables all subordinate switches to automatically save the running configuration as the master does when you execute the **save** [**safely**] [**backup** | **main**] [**force**] command or the **save** *file-url* **all** command. If this function is disabled, only the master saves the configuration.

To ensure configuration consistency, HP recommends enabling the function.

To enable configuration auto-update:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable configuration file auto-update.	**slave auto-update config**	By default, this function is enabled.

Saving configuration by using different methods

When saving the running configuration to a configuration file, you can specify the file as the next-startup configuration file.

If you are specifying the file as the next-startup configuration file, use one of the following methods to save the configuration:

- **Fast mode**—Use the **save** command without the **safely** keyword. In this mode, the device directly overwrites the target next-startup configuration file. If a reboot or power failure occurs during this

process, the next-startup configuration file is lost. You must re-specify a new startup configuration file after the device reboots (see "Specifying a configuration file for the next startup").

- **Safe mode**—Use the **save** command with the **safely** keyword. Safe mode is slower than fast mode, but more secure. In safe mode, the system saves configuration in a temporary file and starts overwriting the target next-startup configuration file after the save operation is complete. If a reboot or power failure occurs during the save operation, the next-startup configuration file is still retained

Use the safe mode if the power source is not reliable or you are remotely configuring the device.

The configuration file extension must be .cfg.

To save the running configuration, perform either of the following tasks in any view:

Task	Command	Remarks
Save the running configuration to a configuration file without specifying the file as a next-startup configuration file.	**save** *file-url* [**all** | **slot** *slot-number*]	The **save** command executed with only the *file-url* argument saves the running configuration only to the specified path, regardless of whether the configuration auto-update function has been enabled.
Save the running configuration to a configuration file and specify the file as a next-startup configuration file.	**save** [**safely**] [**backup** | **main**] [**force**]	If you execute the **save** [**safely**] command without specifying any other keyword, the command saves the configuration to the main startup configuration file. If the **force** keyword is specified, the command saves the configuration to the next-startup configuration file that has been specified. If the **force** keyword is not specified, you may choose to re-specify a next-startup configuration file as instructed by the system.

If configuration auto-update is enabled, the **save** *file-url* **all** command and the **save** [**safely**] [**backup** \| **main**] [**force**] command save the configuration to the master device and all member devices. If the function is disabled, the commands save the configuration only to the master device.

Using automatic configuration backup after a software upgrade

After a software upgrade, the system by default starts up with the next-startup configuration file created on the old software version, but the system does not load settings that are incompatible with the new software version to the current configuration.

In case a future downgrade is needed, the system automatically checks for configuration incompatibility and backs up the old next-startup configuration file the first time you use the **save** command to save the running configuration to the file.

The backup file is named in the *_old-filename*_**bak.cfg** format. For example, if the old configuration file is named config.cfg, the backup file is named _config_bak.cfg.

The overwrite and backup operations are performed on each member device, regardless of whether configuration auto-update is enabled.

If the backup attempt fails on an IRF member device, choose one of the following failure handling actions at prompt:

- **Give up saving the configuration**—The system does not save the running configuration on any member device.
- **Overwrite the configuration file**—The system uses the running configuration to overwrite the old configuration file on the member device without backing up the file. You can copy the backup configuration file from the master device to this member device for future rollback.

To ensure a successful backup, verify that:

- Each device has enough space for the backup configuration file and the new next-startup configuration file.
- The file name length of the backup file is no more than 91 characters.

To load the backup configuration file after a software downgrade, specify the backup file as the next-startup configuration file on each member device.

Configuring configuration rollback

To replace the running configuration with the configuration in a configuration file without rebooting the device, use the configuration rollback function. This function helps you revert to a previous configuration state or adapt the running configuration to different network environments.

The configuration rollback function compares the running configuration against the specified replacement configuration file and handles configuration differences as follows:

- If a command in the running configuration is not in the replacement file, executes its **undo** form.
- If a command in the replacement file is not in the running configuration, adds it to the running configuration.
- If a command has different settings in the running configuration and the configuration file, replaces its running configuration with the setting in the configuration file.

To facilitate configuration rollback, the configuration archive function is developed. This function enables the system to automatically save the running configuration at regular intervals as checkpoint references.

Configuration task list

Task	Remarks
Configuring configuration archive parameters	Required.
• Enabling automatic configuration archiving • Manually archiving running configuration	Required. Use either method.
Performing configuration rollback	Required.

Configuring configuration archive parameters

Before archiving the running configuration, either manually or automatically, you must configure a file directory and file name prefix for configuration archives.

Configuration archives are saved with the file name format *prefix_serial number***.cfg**, for example, **20080620archive_1.cfg** and **20080620archive_2.cfg**. The serial number is automatically assigned from 1 to 1000, increasing by 1. After the serial number reaches 1000, it restarts from 1.

After you change the file directory or file name prefix, or reboot the device, the old configuration archives are regarded as common configuration files, the configuration archive counter resets, and the **display archive configuration** command does not display them. The serial number for new configuration archives starts from 1.

After the maximum number of configuration archives is reached, the system deletes the oldest archive for the new archive.

Configuration guidelines

In an IRF fabric, the configuration archive function saves running configuration only on the master device. To make sure the system can archive running configuration after a master/subordinate switchover, create the directory on all IRF members.

Configuration procedure

To configure configuration archive parameters:

Step		Command	Remarks
1.	Create the configuration archive directory.	See "Managing the file system."	In an IRF fabric, create the directory at least on the master.
2.	Enter system view.	**system-view**	N/A
3.	Configure the directory and file name prefix for archiving the running configuration.	**archive configuration location** *directory* **filename-prefix** *filename-prefix*	Do not include member ID information in the directory name. By default, no path or file name prefix is set for configuration archives, and the system does not regularly save configuration. IMPORTANT: The **undo** form of this command disables both manual and automatic configuration archiving, restores the default settings for the **archive configuration interval** and **archive configuration max** commands, and deletes all saved configuration archives.
4.	Set the maximum number of configuration archives.	**archive configuration max** *file-number*	Optional. The default number is 10. Change the setting depending on the available storage space.

Enabling automatic configuration archiving

To avoid decreasing system performance, follow these guidelines when you configure automatic configuration archiving:

- If the device configuration does not change frequently, manually archive the running configuration as needed.
- If a low-speed storage medium (such as a flash) is used, archive the running configuration manually, or configure automatic archiving with an interval longer than 1440 minutes (24 hours).

Make sure you have set an archive path and file name prefix before performing this task.

To enable automatic configuration archiving:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable automatic configuration archiving and set the archiving interval.	**archive configuration interval** *minutes*	By default, this function is disabled. To view configuration archive names and their archiving time, use the **display archive configuration** command.

Manually archiving running configuration

To save system resources, disable automatic configuration archiving and manually archive configuration if the configuration will not be changed very often. You can also manually archive configuration before performing complicated configuration tasks so you can use the archive for configuration recovery after the configuration attempt fails.

Make sure you have set an archive path and file name prefix before performing this task.

Perform the following task in user view:

Task	Command
Manually archive the running configuration.	**archive configuration**

Performing configuration rollback

To avoid rollback failure, follow these guidelines:

- Do not reboot member devices while the system is executing the **configuration replace file** command.
- Make sure the replacement configuration file is created by using the configuration archive function or the **save** command on the current device.
- If the configuration file is not created on the current device, make sure the configuration file content format is fully compatible with the current device.
- The replacement configuration file is not encrypted.

To perform a configuration rollback:

Step	Command
1. Enter system view.	**system-view**
2. Perform configuration rollback.	**configuration replace file** *filename*

The configuration rollback function might fail to reconfigure some commands in the running configuration for one of the following reasons:

- A command cannot be undone, because prefixing the **undo** keyword to the command does not result in a valid **undo** command. For example, if the **undo** form designed for the **A** [**B**] **C** command is **undo A C**, the configuration rollback function cannot undo the **A B C** command, because the system does not recognize the **undo A B C** command.
- A command (for example, a hardware-dependent command) cannot be deleted, overwritten, or undone due to system restrictions.
- The commands in different views are dependent on each other.
- Commands or command settings that the device does not support cannot be added to the running configuration.

Specifying a configuration file for the next startup

You can specify a .cfg configuration file as the main startup configuration file to be used at the next startup when you use the **save** command to save the running configuration to it.

Alternatively, perform the following task in user view to specify the next-startup configuration file:

Task	Command	Remarks
Specify the next-startup configuration file.	**startup saved-configuration** *cfgfile* [**backup** | **main**]	The setting applies to all member devices. IMPORTANT: The configuration file must use the .cfg extension and be saved in the root directory of storage media. If the storage medium has been partitioned, save the file on the first partition.

Backing up the next-startup configuration file to a TFTP server

Before performing this task, make sure the following requirements are met:

- The server is reachable and enabled with TFTP service.
- You have read and write permissions.

This task backs up only the main next-startup configuration file.

To back up the next-startup configuration file to a TFTP server:

Step	Command	Remarks
1. Verify that a next-startup configuration file has been specified in user view.	**display startup**	Optional. If no next-startup configuration file has been specified, the backup operation will fail.
2. Back up the next-startup configuration file to a TFTP server in user view.	**backup startup-configuration to** *dest-addr* [*dest-filename*]	This command is not supported in FIPS mode.

Deleting the next-startup configuration file

CAUTION:

This task permanently deletes the next-startup configuration file from all member devices. Before performing this task, back up the file as needed.

You can delete the main, the backup, or both. If the main and backup next-startup configuration files are the same file, the system sets the attribute of the configuration file to NULL instead of deleting the file. You can permanently delete the file after its attribute changes to NULL.

You may need to delete the next-startup configuration file for one of the following reasons:

- After you upgrade system software, the file does not match the new system software.
- The file has been corrupted or is not fully compatible with the device.

After the file is deleted, the device uses factory defaults at the next startup.

Perform the following task in user view:

Task	Command
Delete the next-startup configuration file.	**reset saved-configuration** [**backup** | **main**]

Restoring the next-startup configuration file from a TFTP server

To download a configuration file from a TFTP server to the root directory of each member's storage medium, and specify the file as the next-startup configuration file, perform the task in this section.

Before restoring the next-startup configuration file, make sure the following requirements are met:

- The server is reachable and enabled with TFTP service.
- You have read and write permissions.

To restore the next-startup configuration file from a TFTP server:

Step	Command	Remarks
1. Restore the main next-startup configuration file from a TFTP server in user view.	**restore startup-configuration from** *src-addr src-filename*	This command is not supported in FIPS mode.
2. Verify that the specified configuration file has been set as the main next-startup configuration file.	**display startup**	Optional.

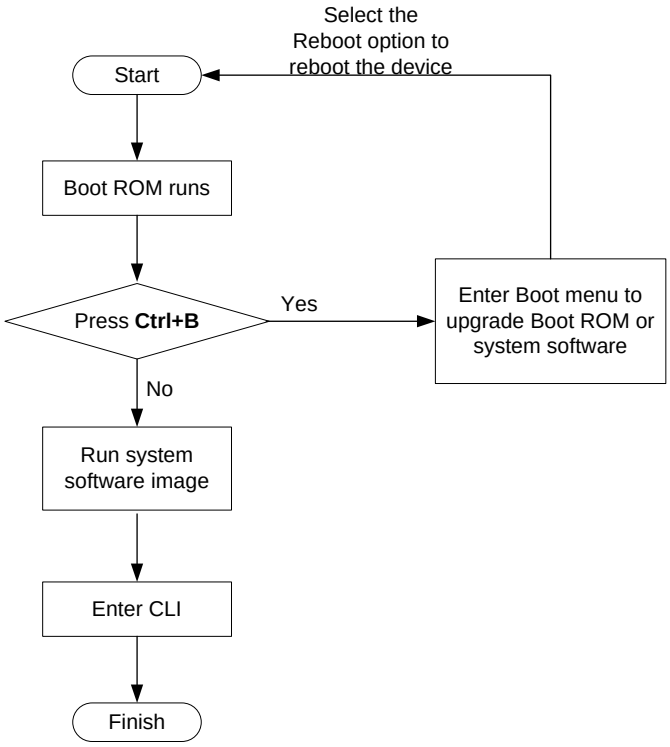
Displaying and maintaining a configuration file

Task	Command	Remarks
Display information about configuration rollback.	**display archive configuration** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the running configuration.	**display current-configuration** [**configuration** [*configuration*] | **interface** [*interface-type* [*interface-number*]] | **exclude** *modules*] [**by-linenum**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the factory defaults.	**display default-configuration** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the running configuration file saved on the storage media of the device.	**display saved-configuration** [**by-linenum**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display names of the configuration files used at this startup and the next startup.	**display startup** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the valid configuration in the current view.	**display this** [**by-linenum**] [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Upgrading software

Upgrading software includes upgrading the Boot ROM and system software. Each time the switch is powered on, it runs the Boot ROM image to initialize hardware and display hardware information, and then runs the system software image (called the "boot file" in software code) so you can access the software features, as shown in Figure 33.

Figure 33 Relationship between the Boot ROM image and the system software image



FIPS compliance

The device supports the FIPS mode that complies with NIST FIPS 140-2 requirements. Support for features, commands, and parameters might differ in FIPS mode and non-FIPS mode. For more information about FIPS mode, see *Security Configuration Guide*.

Software upgrade methods

You can upgrade system software by using one of the following methods:

Upgrading method	Software types	Remarks
Upgrading from the CLI:		

Upgrading method	Software types	Remarks
Upgrading without performing ISSU	• Boot ROM image • System software images (excluding patches)	You must reboot the entire device to complete the upgrade. This method is disruptive.
Installing hotfixes	System software images	Hotfixes repair software defects without requiring a reboot or service interruption. Hotfixes do not add new features to system software images.
Performing ISSU	Comware images	The ISSU method enables a software upgrade without service disruption. Use this method for an IRF fabric or MPU-redundant device. For more information about ISSU, see "Performing ISSU."
Upgrading from the Boot menu	• Boot ROM image • Comware software images	Use this method when the device cannot correctly start up. For information about this upgrading method, see the release notes for your switch. IMPORTANT: Upgrading an IRF fabric from the CLI rather than the Boot menu. The Boot menu method requires that you upgrade the member devices one by one and has a larger impact on services than other methods.

NOTE:

Only the HP 5500 EI switch supports the ISSU method.

Upgrading Boot ROM without performing ISSU

Step	Command	Remarks
1. Use FTP or TFTP to transfer the Boot ROM image to the root directory of a member switch's storage medium.	See "Configuring FTP " or "Configuring TFTP."	N/A
2. Copy the image to the root directory of each member device's storage medium in user view.	**copy** *fileurl-source fileurl-dest*	N/A
3. Enter system view.	**system-view**	N/A

Step	Command	Remarks
4. Enable Boot ROM image validity check.	**bootrom-update security-check enable**	Optional. By default, the validity check function is enabled. This feature examines the upgrade Boot ROM image for version and hardware incompatibility to ensure a successful upgrade.
5. Return to user view.	**quit**	N/A
6. Upgrade Boot ROM on member switches.	**bootrom update file** *file-url* **slot** *slot-number-list*	In FIPS mode, the file must pass authenticity verification before it can be set as the Boot ROM image file.
7. Reboot the member switches.	**reboot**	N/A

Upgrading system software without performing ISSU (method 1)

Step	Command	Remarks
1. Use FTP or TFTP to transfer the system software image to the root directory of the master device's storage medium.	See ""Configuring FTP " or "Configuring TFTP."	The image file must be saved in the root directory for a successful upgrade.
2. Copy the system software image to the root directory of each subordinate switch's storage medium.	**copy** *fileurl-source fileurl-dest*	You can assign different names to the image files on different member switches, but must make sure the image versions are the same.
3. Specify the file as the startup software image for each member switch in user view.	**boot-loader file** *file-url* **slot** { **all** | *slot-number* } { **main** | **backup** }	In FIPS mode, the specified file must pass authenticity verification before it can be set as a startup system software image.
4. Reboot the entire IRF fabric.	**reboot**	N/A

Upgrading system software without performing ISSU (method 2)

This method simplifies the software upgrade procedure described in "Upgrading system software without performing ISSU (method 1)" for a multiple-MPU context by using one command to complete copying a system software image to an MPU and specifying the file as the system software image to be used at the next startup.

To use this method to upgrade system software:

Step	Command	Remarks
1. Use FTP or TFTP to transfer the system software image to the root directory of the master switch's storage medium.	See ""Configuring FTP " or "Configuring TFTP."	The image file must be saved in the root directory for a successful upgrade.
2. Specify the file as the startup software image for each member switch in user view.	**boot-loader update file** *file-url* **slot** { *slot-number* | **all** } { **main** | **backup** }	In FIPS mode, the specified file must pass authenticity verification before it can be set as a startup system software image.
3. Reboot the entire IRF fabric.	**reboot**	N/A

Upgrading software by installing hotfixes

Hotfixes (called "patches" in this document) can repair software defects without requiring a system reboot.

Basic concepts

Patch, patch file, and patch package file

A patch fixes certain software defects.

A patch file contains one or more patches. After being loaded from the storage medium to the patch memory area, each patch is assigned a unique number, which starts from 1. For example, if a patch file has three patches, they are numbered 1, 2, and 3.

A patch package file contains patch files for multiple modules. It enables you to use one command to bulk-fix bugs for multiple modules.

Incremental patch

Incremental patches are dependent on previous patches and cannot separately run. For example, if a patch file has three patches, patch 3 can be running only after patch 1 and 2 take effect. You cannot run patch 3 separately.

Patches that have been released are all incremental patches.

Common patch and temporary patch

Common patches are formally released to users.

Temporary patches are interim solutions that are provided to fix critical bugs. They are not formally released.

A common patch always includes the functions of its previous temporary patches. The system deletes all the temporary patches before loading the common patch.

Patch states

A patch is in IDLE, DEACTIVE, ACTIVE, or RUNNING state, depending on the patch manipulation command.

Patch manipulation commands include **patch load** (load), **patch active** (run temporarily), **patch run** (confirm running), **patch deactive** (stop running), **patch delete** (delete), **patch install** (install), and **undo patch install** (uninstall).

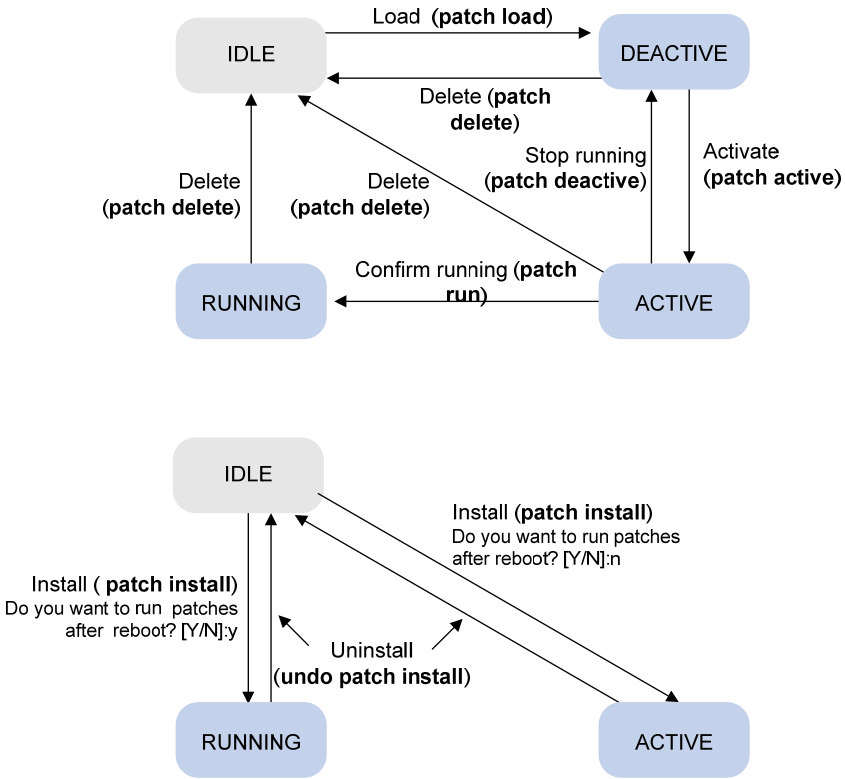
For example, if you execute the **patch active** command, patches in DEACTIVE state change to the ACTIVE state.

Figure 34 shows the patch manipulation commands and how they affect the patch state.

IMPORTANT:

Patch state information is saved in a file named **patchstate**. To make sure the switch can correctly find the patches, do not edit, delete, move the file, or change the file name.

Figure 34 Impact of patch manipulation commands on patch state

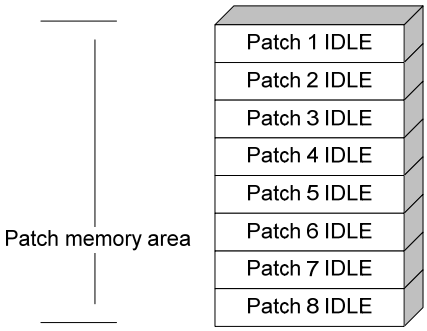


IDLE state

Patches that have not been loaded are in IDLE state. You cannot install or run these patches. In the example in Figure 35, the patch memory area can load up to eight patches.

The patch memory area supports up to 200 patches.

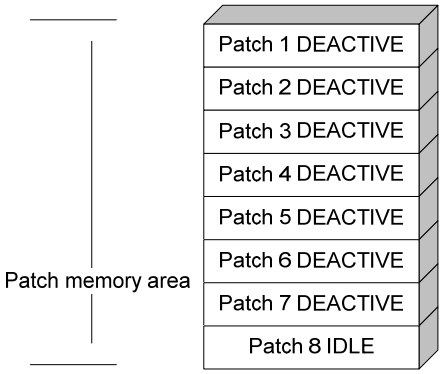
Figure 35 Patches that are not loaded to the patch memory area



DEACTIVE state

Patches in DEACTIVE state have been loaded to the patch memory area but have not yet run in the system. Suppose that the patch file you are loading has seven patches. After the seven patches successfully pass the version check and CRC check, they are loaded to the patch memory area and are in DEACTIVE state. In the patch area, patch states are as shown in Figure 36.

Figure 36 Patch states in the patch memory area after a patch file is loaded

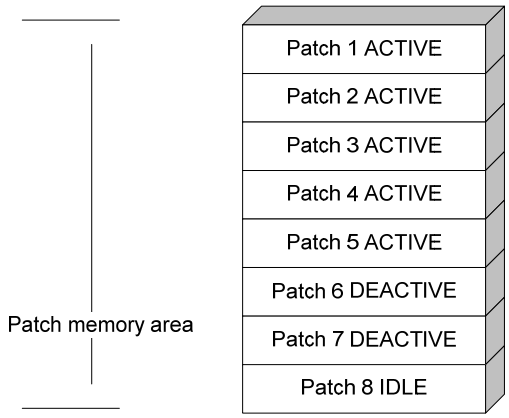


ACTIVE state

Patches in ACTIVE state run temporarily in the system and become DEACTIVE at a reboot. For the seven patches in Figure 36, if you activate the first five patches, their states change from DEACTIVE to ACTIVE. The patch states in the system are as shown in Figure 37.

The patches that are in ACTIVE state are in DEACTIVE state after system reboot.

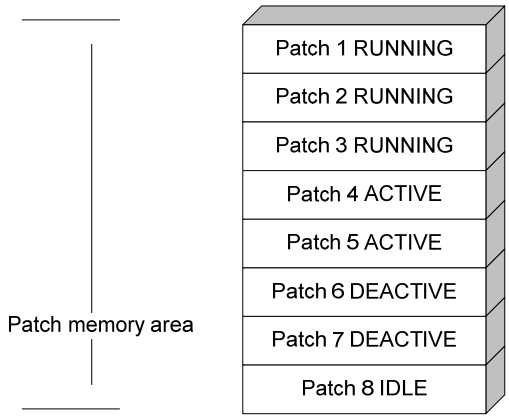
Figure 37 Patches are activated



RUNNING state

After you confirm ACTIVE patches, their states change to RUNNING and persist after a reboot. In contrast to ACTIVE patches, RUNNING patches continue to take effect after a reboot. For example, if you confirm the first three patches in Figure 37, their state changes from ACTIVE to RUNNING, and the RUNNING state persists after a reboot. The patch states of the system are shown in Figure 38.

Figure 38 Patches in RUNNING state



Hotfix configuration task list

Task	Remarks
Installing patches: • Installing and running a patch in one step • Installing a patch step by step	Use either method. Step-by-step patch installation allows you to control the patch status.
Uninstalling a patch step by step	Optional.

Installation prerequisites

To ensure a successful hotfix operation and normal switch operation after the hotfix operation:

- Make sure each patch file you are installing matches the switch model and software version.

- Save patch files to the root directory of each member device's storage medium.
- Correctly name a patch file in the **patch_***PATCH-FlAG suffix***.bin** format. The PATCH-FLAG suffix is predefined and must be the same as the first three characters of the value for the **Version** field in the output from the **display patch information** command. If a patch file is not correctly named, the system cannot identify the file.

  The default system patch file name is **patch_xxx.bin**.

Installing and running a patch in one step

To install and run patches in one step, use the **patch install** command. This command changes the state of installed patches from IDLE to ACTIVE or RUNNING, depending on your choice.

When executing the **patch install** command, you must choose to run installed patches or disable running them after a reboot. If you choose to have installed patches continue to run after a reboot, the installed patches are set in RUNNING state and remain in this state after a reboot. If not, the installed patches are set in ACTIVE state and change to the DEACTIVE state at a reboot.

The system verifies the signatures of the path files after you execute the command **patch install**. If the verification succeeds, the commands take effect.

To install and run patches in one step:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Verify that no patches have been installed.	**display patch information**	You can execute this command in any view. Only one patch package file can be installed on the device. If no patches have been installed, skip the next step. If patches have been installed, move to the next step.
3. Uninstall patches that have been installed.	**undo patch install**	N/A
4. Install and run patches in one step.	**patch install** { *patch-location* | **file** *patch-package* }	• *patch-location*: Specifies the directory where the patch file is located. • **file** *patch-package*: Specifies a patch package file name. In FIPS mode, the patch file or the patch package file must pass authenticity verification before the command can be executed.

If you execute the **patch install** *patch-location* command, the directory specified for the *patch-location* argument replaces the directory specified with the **patch location** command after the upgrade is complete.

If you execute the **patch install file** *patch-package* command, the directory specified with the **patch location** command does not change.

To uninstall all ACTIVE and RUNNING patches in one step, use the **undo patch install** command. HP recommends this command for uninstalling patches in an IRF fabric. For information about the step-by-step patch uninstall method, see "Uninstalling a patch step by step."

Installing a patch step by step

In contrast to the one-step patch installation method, step-by-step patch installation enables you to control patch status during the patch installation process.

Step-by-step patch installation task list

Task	Remarks
Configuring the patch file location	Optional. To install a patch package, skip this step.
Loading a patch file	Required.
Activating patches	Required.
Confirming ACTIVE patches	Optional.

Configuring the patch file location

For reliable patch loading, HP recommends saving patch files to the root directory of the flash. To use a storage medium other than flash, you must specify the directory for saving patch files on the storage medium.

Make sure the specified patch file directory exists on all MPUs.

Make sure the specified directory exists on each member switch in the IRF fabric.

If the switch has only one storage medium, you do not need to perform this task.

To configure the patch file location:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the patch file location.	**patch location** *patch-location*	Optional. By default, the patch file location is **flash:**.

NOTE:

If you execute the **patch install** *patch-location* command, the directory specified for the *patch-location* argument replaces the directory specified with the **patch location** command after the upgrade is complete.

Loading a patch file

You must load the correct patch file before performing any patch installation operations.

If you install a patch from a patch file, the system loads the patch file from the patch file location.

If you install a patch from a patch package, the system finds the correct patch file in the patch package file and loads the patch file.

In FIPS mode, the patch package file or the patch file must pass authenticity verification before it can be loaded.

IMPORTANT:

Set the file transfer mode to binary mode before using FTP or TFTP to upload or download patch files. Otherwise, patch files cannot be parsed properly.

To load a patch file:

Step	Command
1. Enter system view.	**system-view**
2. Load the patch file on from the storage medium to the patch memory area.	**patch load slot** *slot-number* [**file** *patch-package*]

Activating patches

Activating a patch changes its state to ACTIVE. An ACTIVE patch runs in memory until a reboot occurs. To have a patch continue to run after a reboot, you must change its state to RUNNING.

To activate patches:

Step	Command
1. Enter system view.	**system-view**
2. Activate patches.	**patch active** [*patch-number*] **slot** *slot-number*

Confirming ACTIVE patches

To have an ACTIVE patch continue to run after a reboot, perform the task in this section.

After you confirm an ACTIVE patch, its state changes to RUNNING and persists after a reboot.

To confirm ACTIVE patches:

Step	Command
1. Enter system view.	**system-view**
2. Confirm ACTIVE patches.	**patch run** [*patch-number*] [**slot** *slot-number*]

Uninstalling a patch step by step

To uninstall a patch by using the step-by-step method, you must first stop running the patch and then remove it from the patch memory area.

Stopping running patches

When you stop running a patch, the patch state becomes DEACTIVE, and the system runs the way it did before the patch was installed.

To stop running patches:

Step	Command
1. Enter system view.	**system-view**

Step	Command
2. Stop running patches.	**patch deactive** [*patch-number*] **slot** *slot-number*

Removing patches from the patch memory area

After being removed from the patch memory area, a patch is still retained in IDLE state in the storage medium. The system runs the way it did before the patch was installed.

In an IRF fabric, HP recommends that you uninstall all patches by using the **undo patch install** command.

To remove patches from the patch memory area:

Step	Command
1. Enter system view.	**system-view**
2. Remove patches from the patch memory area.	**patch delete** [*patch-number*] **slot** *slot-number*

Displaying and maintaining software upgrade

Task	Command	Remarks
Display information about system software	**display boot-loader** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display information about the patch package.	**display patch** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the patch information.	**display patch information** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Software upgrade examples

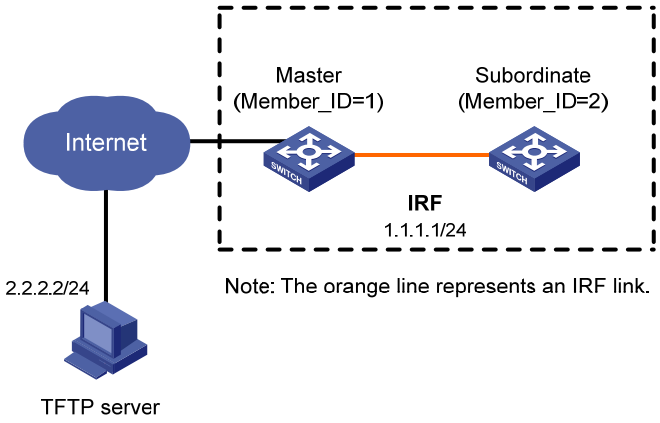
Non-ISSU software upgrade example

Network requirement

The IRF fabric in Figure 39 comprises two member switches, the master use the member ID 1 and the subordinate switch uses the member ID 2. The current software version of the IRF fabric is **soft-version1**. The latest system software image **soft-version2.bin** and the latest configuration file **new-config.cfg** are both saved on the TFTP server. The TFTP server and IRF fabric can reach each other.

Upgrade the software version of the IRF fabric to **soft-version2** and the configuration file to **new-config**.

Figure 39 Network diagram



Configuration procedure

1. Configure the TFTP server (the configuration varies with server vendors):

   # Obtain the system software image and configuration file, and save these files under the TFTP server's working path. (Details not shown.)

2. Configure the members of the IRF fabric:

   # Download **new-config.cfg** from the TFTP server to the master.

```
<IRF> tftp 2.2.2.2 get new-config.cfg
  ..
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait.....
  TFTP:       917 bytes received in 1 second(s)
File downloaded successfully.
```

   # Download **new-config.cfg** to the subordinate switch with the member ID of 2.

```
<IRF> tftp 2.2.2.2 get new-config.cfg slot2#flash:/new-config.cfg
```

   # Download **soft-version2.bin** from the TFTP server to the master and the subordinate switch.

```
<IRF> tftp 2.2.2.2 get soft-version2.bin
  ...
  File will be transferred in binary mode
  Downloading file from remote TFTP server, please wait............
  TFTP: 10058752 bytes received in 141 second(s)
  File downloaded successfully.
<IRF> tftp 2.2.2.2 get soft-version2.bin slot2#flash:/soft-version2.bin
```

   # Specify **new-config.cfg** as the next-startup configuration file for all members of the IRF fabric.

```
<IRF> startup saved-configuration new-config.cfg main
Please wait ...
Setting the master board ...
... Done!
Setting the slave board ...
Slot 2:
 Set next configuration file successfully
```

   # Specify **soft-version2.bin** as the startup system software image for all IRF members.

```
<IRF> boot-loader file soft-version2.bin slot all main
  This command will set the boot file of the specified board. Continue? [Y/N]:y
```

```
  The specified file will be used as the main boot file at the next reboot on slot
1!
  The specified file will be used as the main boot file at the next reboot on slot
2!
```

Reboot the IRF fabric to complete the upgrade.

```
<IRF> reboot
```

3. Use the **display version** command to verify that the upgrade has succeeded. (Details not shown.)

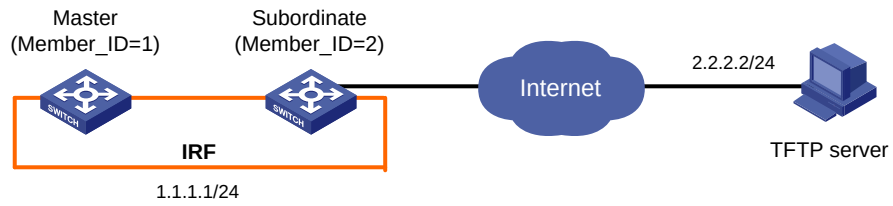
Hotfix configuration example

Network requirements

The IRF fabric in Figure 40 is formed by two member switches, the master and subordinate switch. The software running on the member switches has a bug. The patch files **patch_xxx.bin** are saved on the TFTP server. The IRF fabric and TFTP server can reach each other.

From the IRF fabric, use TFTP to download the patch files and then hotfix the software on the fabric.

Figure 40 Network diagram



Note: The orange line represents the IRF link.

Configuration procedure

1. Configure the TFTP server (the configuration varies with server vendors):

   # Enable the TFTP server function. (Details not shown.)

   # Save the patch files **patch_xxx.bin** to the directory of TFTP server. (Details not shown.)

2. Configure the IRF fabric:

   # Before upgrading the software, use the **save** command to save the current system configuration. (Details not shown.)

   # Examine the free space of the flash on the switch. If the free space is not sufficient for the patch files, delete unused files to release enough space. (Details not shown.)

   # Load the patch files **patch_xxx.bin** from the TFTP server to the root directory of the master's storage medium.

   ```
   <IRF> tftp 2.2.2.2 get patch_xxx.bin
   ```

   # Load the patch files **patch_xxx.bin** from the TFTP server to the root directory of the subordinate switch's storage medium.

   ```
   <IRF> tftp 2.2.2.2 get patch_xxx.bin slot2#flash:/patch_xxx.bin
   ```

   # Install the patch.

   ```
   <IRF> system-view
   [IRF] patch install flash:
   Patches will be installed. Continue? [Y/N]:y
   Do you want to continue running patches after reboot? [Y/N]:y
   Installing patches........
   ```

3. Use the **display patch information** command to verify that the patches have been installed and are running. (Details not shown.)

Performing ISSU

This chapter describes how to use the In-Service Software Upgrade (ISSU) feature to upgrade software.

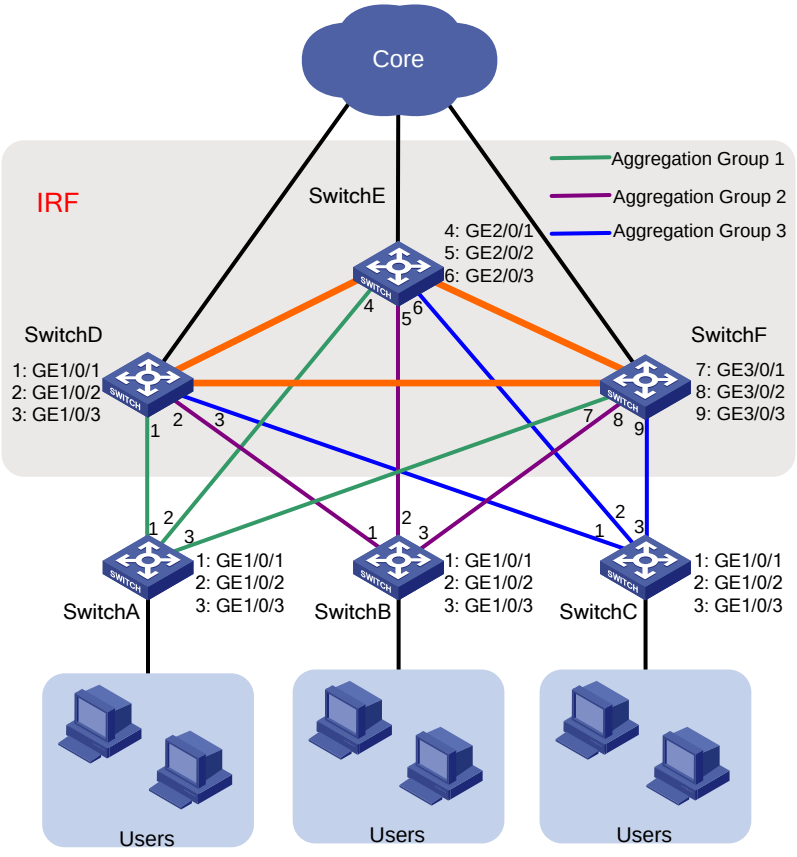
The ISSU feature is available only on the HP 5500 EI switch.

Overview

ISSU enables software upgrade and ensures continuous packet forwarding.

As shown in Figure 41, to ensure high availability for user networks, cross-device link aggregation is configured on the IRF member switches at the distribution layer so every three physical links with the same color between the IRF member switches and access switches are aggregated as one logical link. In this scenario, you can use ISSU to upgrade system software of each IRF member switch to ensure non-stop forwarding or reduce down time for users connected to Switch A, Switch B, and Switch C.

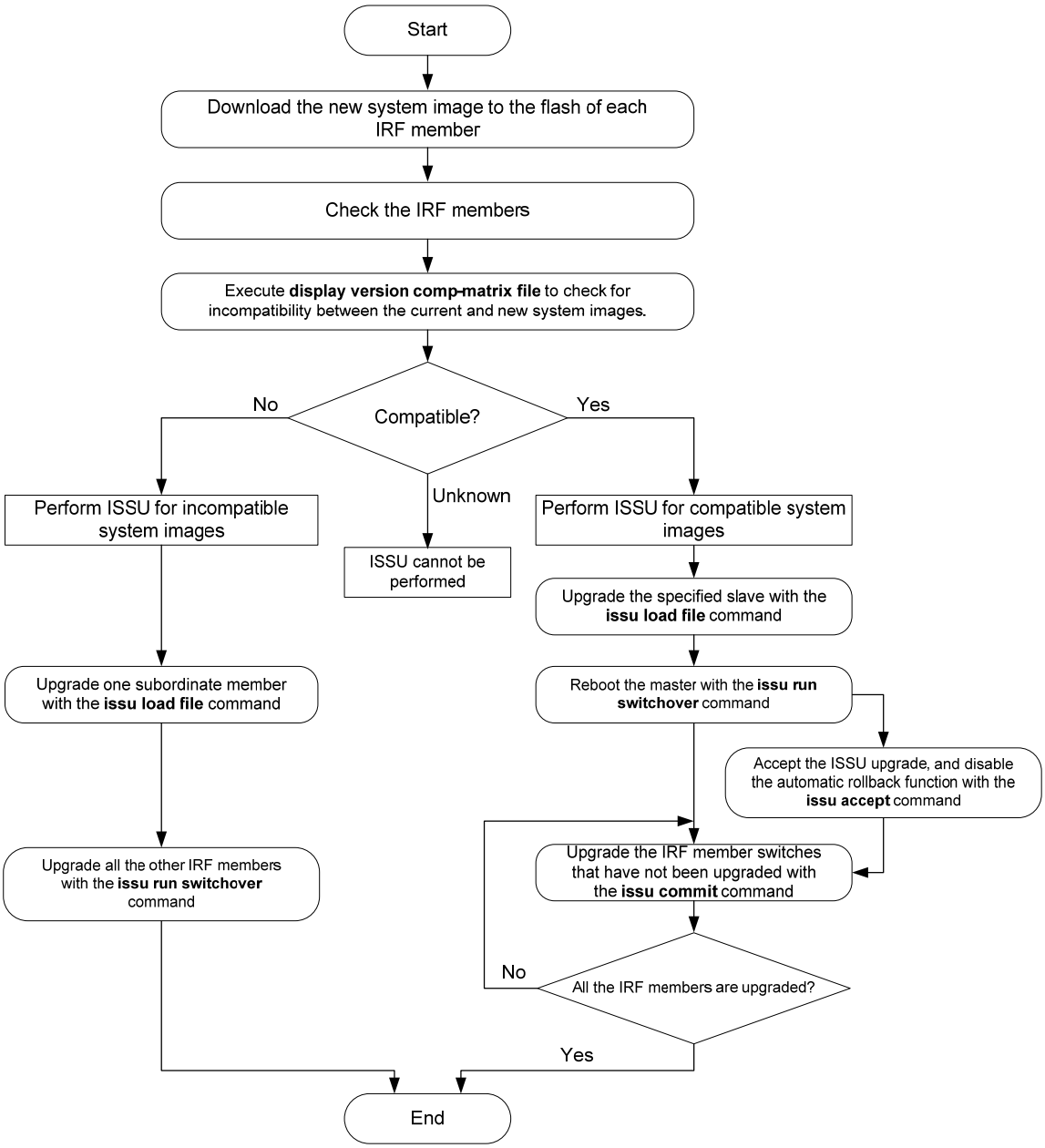
Figure 41 IRF network diagram



ISSU upgrade procedure

ISSU follows a strict procedure, as shown in Figure 42.

Figure 42 ISSU flow chart



IMPORTANT:

- Do not modify the current configuration, plug or unplug cables connected to IRF ports, or delete or modify the system software image during ISSU. Otherwise, the upgrade might fail.
- To upgrade system software of IRF member switches through ISSU, make sure the member switches form a ring topology.

ISSU states

During the ISSU process, you can use the **display issu state** command to display the ISSU state of the IRF fabric, including whether the new system software image is compatible with the current system software image, and the adopted ISSU method.

Table 19 ISSU state description

State	Remarks
Init (Initial state)	No ISSU starts or an ISSU upgrade has completed.
Load	A subordinate switch is being upgraded or has been upgraded. To stop the loading process, perform a manual or automatic roll back to revert system software to its original version.
Switchover	The master is being rebooted to trigger a new master election.
Accept	The ISSU has been accepted. To stop the loading process, you have to perform a manual roll back to revert system software to its original version. The automatic roll back function is not available in this state.
Commit	At least one member switch has not been upgraded to the new version. In this state, neither manual nor automatic rollback can be performed.

System software version rollback

The HP 5500 EI switch series supports version rollback during ISSU. When ISSU fails to proceed on an IRF member switch (for example, the new system software image file is broken), you can use this feature to revert system software to the previous version.

The HP 5500 EI switches support the following version rollback methods.

Automatic rollback

When you reboot the specified subordinate switch with the **issu load** command, the system automatically creates a configurable version rollback timer.

During ISSU for a compatible version, if you do not execute the **issu accept** command on the specified subordinate switch or the **issu commit** command on any other member switch before the rollback timer expires, the system automatically stops the upgrade and rolls back the system software image of the upgraded IRF member switches to the previous version.

During ISSU for an incompatible version, if you do not execute the **issu run switchover** command to upgrade all the IRF member switches that have not been upgraded in one operation before the rollback timer expires, the system automatically rolls back the system software image of all the upgraded IRF member switches to the previous version.

For information about compatible and incompatible ISSU methods, see "Displaying version compatibility."

Manual rollback

You can use the **issu rollback** command to roll back the system software image of an IRF member switch to the previous version. Whether manual rollback can be performed depends on the ISSU state. For more information, see Table 19.

Performing an ISSU

This section describes how to perform an ISSU.

ISSU upgrade task list

Task	Remarks
Downloading the new system software image to the Flash of all the IRF member switches	Required.
ISSU upgrade prerequisites	Required.
Displaying version compatibility	Required.
Performing an ISSU for a compatible version	Required.
Performing an ISSU for an incompatible version	Use either approach.
Setting the ISSU version rollback timer	Optional.
Performing a manual version rollback	Optional.
Displaying and maintaining ISSU	Optional.

ISSU upgrade prerequisites

Task	Command	Remarks
Save the current configuration.	**save**	Before performing ISSU, make sure the current configuration of the IRF fabric has been saved to the configuration file.
Display the running status of each IRF member switch.	**display device**	Before performing ISSU, make sure all the member switches of the IRF fabric are in normal state.
Display the information about system software.	**display boot-loader**	Before performing an ISSU upgrade, make sure the system software image of all the IRF member switches is identical, which means the version, name, and directory of the system software image are the same.
Display the roles of IRF member switches.	**display irf**	N/A
Display information about the files in the Flash.	**dir**	Before performing an ISSU upgrade, make sure the new and current system software images exist in the Flash of each IRF member switch, and they are saved in the same directory.

Displaying version compatibility

Before performing an ISSU upgrade, check the version compatibility between the new and current system software images, to determine whether ISSU can be performed, and which ISSU method is adopted.

After downloading and saving the new system software image, select an ISSU upgrade method according to one of the following version compatibility check results:

- **Compatible**—The running system software image is compatible with the new system software image. You can use the compatible ISSU method to upgrade system software of the IRF fabric. For more information, see "Performing an ISSU for a compatible version."
- **Incompatible**—The current running system software image is incompatible with the new system software image. You can use the incompatible ISSU method to upgrade system software of the IRF fabric. For more information, see "Performing an ISSU for an incompatible version."

- **Unknown**—The current and new system software images have big differences, or the current system software image does not support ISSU. You cannot upgrade system software through ISSU.

To display version compatibility:

Step		Command
1.	Enters system view.	**system-view**
2.	Check whether the new system software image is compatible with the current system software image.	**display version comp-matrix file** *upgrading-filename*

Performing an ISSU for a compatible version

Use the **display version comp-matrix file** *upgrading-filename* command to view the versions of the new and current system software images. If the new system software image is compatible with the current system software image, use this task for ISSU.

IMPORTANT:

Before performing compatible ISSU, make sure the priorities of the current master switch and the specified subordinate switch are higher than other IRF member switches so the specified subordinate switch can be elected as the new master after the master is rebooted. Otherwise, modify the priorities of the current master switch and the specified subordinate switch with the **irf member** *member-id* **priority** *priority* command.

To perform an ISSU for a compatible version:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Upgrade the specified subordinate switch (the new master after the upgrade).	**issu load file** *upgrading-filename* **slot** *slot-number*	The *slot-number* argument is the member ID of the subordinate switch. The specified subordinate switch reboots with the new system software image when this command is executed. Perform the next operation after the subordinate switch is rebooted.
3.	Reboot the master current manually.	**issu run switchover slot** *slot-number*	With this command executed: • The master reboots with the current system software image, and becomes a subordinate switch after reboot. • The subordinate switches of the IRF fabric perform master election. The winner (the subordinate switch specified with the **issu load** command) becomes the new master. The *slot-number* argument provided in this command must be the same as that specified in the **issu load** command. Perform the next operation after the reboot process is completed.

Step	Command	Remarks
4. Accept the ISSU.	**issu accept slot** *slot-number*	Optional. By default, the rollback timer is 45 minutes. If you do not execute the **issu accept** command on the specified subordinate switch or you do not execute the **issu commit** command on any other member switch before the rollback timer expires, the system automatically stops the ISSU process and reverts to the previous software version. The *slot-number* argument provided in this command must be the same as that specified in the **issu load** command. When this command is executed, the rollback timer becomes invalid and system software cannot be automatically rolled back.
5. Upgrade an IRF member switch that has not been upgraded.	**issu commit slot** *slot-number*	This command upgrades one IRF member switch at a time. If the IRF fabric has three or more than three member switches, repeat this command to upgrade them one by one. When all the IRF member switches reboot with the new system software image, the ISSU process completes.

The roles of some IRF member switches change after an ISSU upgrade.

If you do not execute the **issu accept** or **issu commit** command on the specified IRF member switch before the specified rollback timer expires, the system automatically stops the ISSU process and reverts to the previous software version.

After executing the **issu commit** command, you cannot perform version rollback with the **issu rollback** command.

Performing an ISSU for an incompatible version

Use the **display version comp-matrix file** *upgrading-filename* command to view the versions of the new and current system software images. If they are incompatible, use this task for ISSU.

To perform an ISSU for an incompatible version:

Step	Command	Remarks
1. Enters system view.	**system-view**	N/A
2. Upgrade the specified subordinate switch (the new master after the upgrade).	**issu load file** *upgrading-filename* **slot** *slot-number* **force**	The *slot-number* argument is the member ID of the subordinate switch. Before executing this command, make sure the subordinate switch to be upgraded has the highest priority and save the running configuration. After this command is executed, the specified subordinate switch (the new master after the upgrade) reboots with the new system software image, and stays in the Recover state after reboot. Perform the next operation after the reboot process completes.

Step	Command	Remarks
3. Upgrade all the IRF member switches that have not been upgraded in one operation.	**issu run switchover slot** *slot-number*	The *slot-number* argument provided in this command must be the same as that specified in the **issu load** command. When this command is executed, all the IRF member switches except the specified subordinate switch (the new master) are upgraded to the new version, and the ISSU process completes after reboot.

If you do not execute the **issu run switchover** command before the rollback timer expires, the ISSU upgrade ends automatically, the software reverts to the previous version, and the MPUs resume their former roles.

The **issu run switchover** command deletes the rollback timer. After this command is executed, no manual or automatic rollback can be performed for the upgrade.

Setting the ISSU version rollback timer

Step	Command	Remarks
1. Enters system view.	**system-view**	N/A
2. Set the rollback timer.	**issu rollback-timer** *minutes*	Optional. By default, the rollback timer is 45 minutes.

During an ISSU upgrade process, if you modify the rollback timer after executing the **issu load** command, the new rollback timer does not take effect for this ISSU process.

Performing a manual version rollback

Step	Command	Remarks
1. Enters system view.	**system-view**	N/A
2. Perform a manual version rollback.	**issu rollback slot** *slot-number*	Optional. By default, automatic rollback is performed to revert to the previous version. The *slot-number* argument provided in this command must be the same as that specified in the **issu load** command.

Displaying and maintaining ISSU

Task	Command	Remarks
Display information about the rollback timer.	**display issu rollback-timer** [| { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the ISSU state.	**display issu state**	Available in any view

Task	Command	Remarks
Display version compatibility information.	**display version comp-matrix** [**file** *upgrading-filename*]	Available in any view

ISSU upgrade example

Network status

As shown in Figure 43, access layer switches Switch A, Switch B, and Switch C connect to user networks. Distribution layer switches Switch D, Switch E, and Switch form an IRF fabric. The member ID of the master is 1, and those of the subordinate switches are 2 and 3.

To ensure high availability, configure cross-device link aggregation using the following guidelines so every three physical links with the same color between the IRF member switches and access switches are aggregated as one logical link:

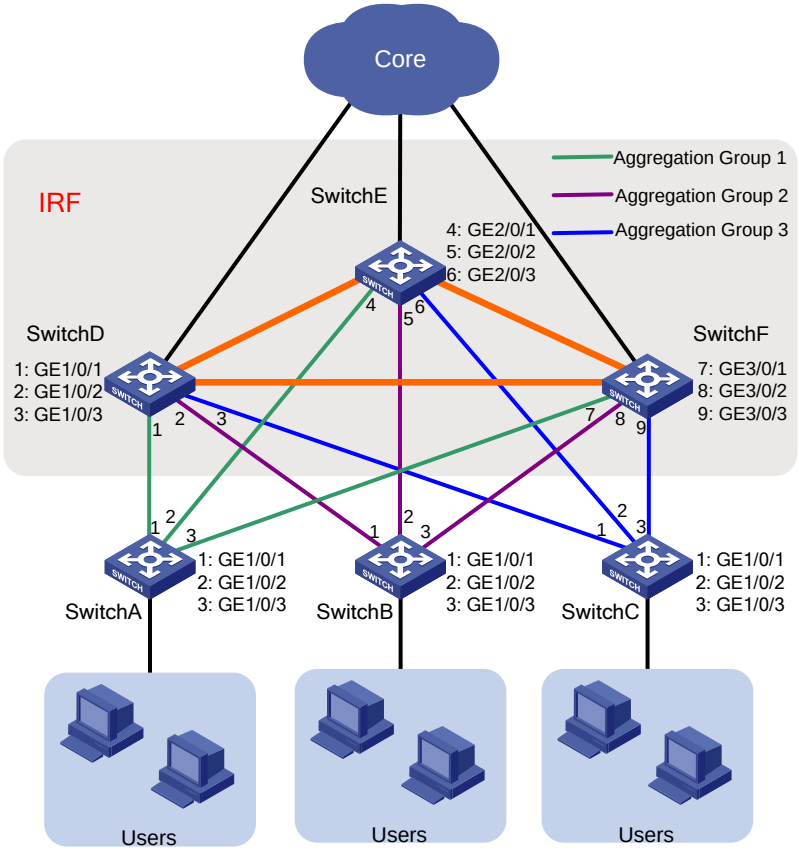
- On the IRF fabric, create three dynamic aggregation groups. Ports in aggregation group 1 connect to Switch A, ports in aggregation group 2 connect to Switch B, and ports in aggregation group 3 connect to Switch C.
- On Switch A, create aggregation group 1 that corresponds to aggregation group 1 on the IRF fabric.
- On Switch B, create aggregation group 2 that corresponds to aggregation group 2 on the IRF fabric.
- On Switch C, create aggregation group 3 that corresponds to aggregation group 3 on the IRF fabric.

Network requirements

The current system software image on each IRF member switch is **soft-version1.bin**. The new system software image **soft-version2.bin** is saved on the TFTP server. The IP address of the IRF fabric is 1.1.1.1/24, and that of the TFTP server is 2.2.2.2/24. The IRF fabric and the TFTP server can reach each other.

Use ISSU to upgrade system software of the IRF member switches to avoid traffic interruption.

Figure 43 Network diagram



Upgrade procedure

Configuring link aggregation

1. Configure the IRF fabric:

   # Create three dynamic aggregation groups 1, 2, and 3.

```
<IRF> system-view
[IRF] interface bridge-aggregation 1
[IRF-Bridge-Aggregation1] link-aggregation mode dynamic
[IRF-Bridge-Aggregation1] quit
[IRF] interface bridge-aggregation 2
[IRF-Bridge-Aggregation2] link-aggregation mode dynamic
[IRF-Bridge-Aggregation2] quit
[IRF] interface bridge-aggregation 3
[IRF-Bridge-Aggregation3] link-aggregation mode dynamic
[IRF-Bridge-Aggregation3] quit
```

   # Add ports GigabitEthernet 1/0/1, GigabitEthernet 2/0/1, and GigabitEthernet 3/0/1 that connect to Switch A to aggregation group 1.

```
[IRF] interface GigabitEthernet 1/0/1
[IRF-GigabitEthernet1/0/1] port link-aggregation group 1
[IRF-GigabitEthernet1/0/1] quit
[IRF] interface GigabitEthernet 2/0/1
```

```
[IRF-GigabitEthernet2/0/1] port link-aggregation group 1
[IRF-GigabitEthernet2/0/1] quit
[IRF] interface GigabitEthernet 3/0/1
[IRF-GigabitEthernet3/0/1] port link-aggregation group 1
[IRF-GigabitEthernet3/0/1] quit
```

Add ports GigabitEthernet 1/0/2, GigabitEthernet 2/0/2, and GigabitEthernet 3/0/2 that connect to Switch B to aggregation group 2.

```
[IRF] interface GigabitEthernet 1/0/2
[IRF-GigabitEthernet1/0/2] port link-aggregation group 2
[IRF-GigabitEthernet1/0/2] quit
[IRF] interface GigabitEthernet 2/0/2
[IRF-GigabitEthernet2/0/2] port link-aggregation group 2
[IRF-GigabitEthernet2/0/2] quit
[IRF] interface GigabitEthernet 3/0/2
[IRF-GigabitEthernet3/0/2] port link-aggregation group 2
[IRF-GigabitEthernet3/0/2] quit
```

Add ports GigabitEthernet 1/0/3, GigabitEthernet 2/0/3, and GigabitEthernet 3/0/3 that connect to Switch C to aggregation group 3.

```
[IRF] interface GigabitEthernet 1/0/3
[IRF-GigabitEthernet1/0/3] port link-aggregation group 3
[IRF-GigabitEthernet1/0/3] quit
[IRF] interface GigabitEthernet 2/0/3
[IRF-GigabitEthernet2/0/3] port link-aggregation group 3
[IRF-GigabitEthernet2/0/3] quit
[IRF] interface GigabitEthernet 3/0/3
[IRF-GigabitEthernet3/0/3] port link-aggregation group 3
[IRF-GigabitEthernet3/0/3] quit
```

2. Configure Switch A:

Create dynamic aggregate interface 1.

```
<SwitchA> system-view
[SwitchA] interface bridge-aggregation 1
[SwitchA-Bridge-Aggregation1] link-aggregation mode dynamic
[SwitchA-Bridge-Aggregation1] quit
```

#Add ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 that connect to IRF member switches to aggregation group 1 (corresponding to aggregate interface 1).

```
[SwitchA] interface GigabitEthernet 1/0/1
[SwitchA-GigabitEthernet1/0/1] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/1] quit
[SwitchA] interface GigabitEthernet 1/0/2
[SwitchA-GigabitEthernet1/0/2] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/2] quit
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port link-aggregation group 1
[SwitchA-GigabitEthernet1/0/3] quit
```

3. Configure Switch B:

Create dynamic aggregate interface 2.

```
<SwitchB> system-view
```

```
[SwitchB] interface bridge-aggregation 2
[SwitchB-Bridge-Aggregation2] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation2] quit
```

#Add ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 that connect to IRF member switches to aggregation group 2 (corresponding to aggregate interface 2).

```
[SwitchB] interface GigabitEthernet 1/0/1
[SwitchB-GigabitEthernet1/0/1] port link-aggregation group 2
[SwitchB-GigabitEthernet1/0/1] quit
[SwitchB] interface GigabitEthernet 1/0/2
[SwitchB-GigabitEthernet1/0/2] port link-aggregation group 2
[SwitchB-GigabitEthernet1/0/2] quit
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port link-aggregation group 2
[SwitchB-GigabitEthernet1/0/3] quit
```

4. Configure Switch C:

Create dynamic aggregate interface 3.

```
<SwitchC> system-view
[SwitchC] interface bridge-aggregation 3
[SwitchC-Bridge-Aggregation3] link-aggregation mode dynamic
[SwitchB-Bridge-Aggregation3] quit
```

Add ports GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 that connect to IRF member switches to aggregation group 3 (corresponding to aggregate interface 3).

```
[SwitchC] interface GigabitEthernet 1/0/1
[SwitchC-GigabitEthernet1/0/1] port link-aggregation group 3
[SwitchC-GigabitEthernet1/0/1] quit
[SwitchC] interface GigabitEthernet 1/0/2
[SwitchC-GigabitEthernet1/0/2] port link-aggregation group 3
[SwitchC-GigabitEthernet1/0/2] quit
[SwitchC] interface GigabitEthernet 1/0/3
[SwitchC-GigabitEthernet1/0/3] port link-aggregation group 3
[SwitchC-GigabitEthernet1/0/3] quit
```

Configuring the TFTP server

Obtain the new system software image through a legal channel, and save the file to the working directory of the TFTP server so the TFTP client can access the file. The working directory varies with TFTP server models.

Downloading the new system software image

Download system software image soft-version2.bin to the root directory of the Flash of each IRF member switch.

```
<IRF> tftp 2.2.2.2 get soft-version2.bin
 File will be transferred in binary mode
 Downloading file from remote TFTP server, please wait……
 TFTP: 10058752 bytes received in 141 second(s)
 File downloaded successfully.
<IRF> copy soft-version2.bin slot2#flash:/
<IRF> copy soft-version2.bin slot3#flash:/
```

Checking all IRF member switches before the ISSU upgrade

1. Check the running status of all IRF member switches. If the running state of a member switch is abnormal, the ISSU upgrade cannot be performed.

```
<IRF> display device
Slot 1
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      28      REV.C  NULL    002     CC1        IVL    MAIN       Normal
1      2       REV.A  NULL    NULL    NULL       IVL    2*10GE     Normal
Slot 2
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      28      REV.C  NULL    002     CC1        IVL    MAIN       Normal
2      2       REV.A  NULL    NULL    NULL       IVL    2*10GE     Normal
Slot 3
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      28      REV.C  NULL    002     CC1        IVL    MAIN       Normal
3      2       REV.A  NULL    NULL    NULL       IVL    2*10GE     Normal
```

   The output shows that all IRF member switches are in normal state.

2. Check whether the current system software images on IRF member switches are the same. If not, the ISSU upgrade cannot be performed.

```
<IRF> display boot-loader
 Slot 1
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
 Slot 2
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
 Slot 3
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
```

   The output shows that the current system software image file on each IRF member switch is **soft-version1.bin**.

3. View the role of each IRF member switch.

```
<IRF> display irf
Switch   Role    Priority  CPU-Mac         Description
 *+1     Master  10        0023-8927-ad54  -----
   2     Slave   9         0023-8927-afdc  -----
   3     Slave   1         0023-89d9-3223  -----
--------------------------------------------------

 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The Bridge MAC of the IRF is: 0023-8927-ad53
 Auto upgrade                : yes
```

```
Mac persistent              : 6 min
Domain ID                   : 0
```

The output shows the following information:

- The member ID and priority of the master are 1 and 10 respectively.
- The member ID and priority of one subordinate switch are 2 and 9 respectively.
- The member ID and priority of the other subordinate switch are 3 and 1 respectively.

During the ISSU upgrade process, you must select subordinate switch 2 as the specified subordinate switch.

Before performing compatible ISSU, make sure the priorities of the master switch and the specified subordinate switch are higher than other IRF member switches so the specified subordinate switch can be elected as the new master after the master is rebooted. Otherwise, modify the priorities of the master switch and the specified subordinate switch with the **irf member** *member-id* **priority** *priority* command.

4. Check whether the new system software image has been saved in the Flash of each IRF member switch. If not, the ISSU upgrade cannot be performed.

   # Verify whether the new system software image **soft-version2.bin** has been saved to the Flash of the master.

```
<IRF> dir
Directory of flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  12397691  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  13308645  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml

31496 KB total (5981 KB free)
```

   The output shows that the new system software image has been saved to the Flash of the master.

   # Verify whether the new system software image **soft-version2.bin** has been saved to the Flash of subordinate switch 2.

```
<IRF> dir slot2#flash:/
Directory of slot2#flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  12397691  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  13308645  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml

31496 KB total (5981 KB free)
```

   The output shows that the new system software image has been saved to the Flash of subordinate switch 2.

   # Verify whether the new system software image **soft-version2.bin** has been saved to the Flash of subordinate switch 3.

```
<IRF> dir slot3#flash:/
Directory of slot3#flash:/

   0     -rw-      6085  May 29 2010 11:38:45   config.cfg
   1     -rw-     10518  Apr 26 2011 12:45:05   logfile.log
   2     -rw-  12397691  Apr 26 2011 14:24:11   soft-version1.bin
   3     -rw-  13308645  Apr 26 2011 14:13:46   soft-version2.bin
   4     drw-         -  Apr 26 2011 12:00:33   seclog
   5     -rw-       287  Apr 26 2011 12:19:52   system.xml

31496 KB total (5981 KB free)
```

The output shows that the new system software image has been saved to the Flash of subordinate switch 3.

5. Save the current configuration.

```
<IRF> save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/config.cfg]
(To leave the existing filename unchanged, press the enter key):
flash:/config.cfg exists, overwrite? [Y/N]:y
 Validating file. Please wait....
 Saved the current configuration to mainboard device successfully.
Slot 2:
 Save next configuration file successfully.
Slot 3:
 Save next configuration file successfully.
 Configuration is saved to device successfully.
```

The output shows that the current configuration has been saved to the configuration file of each IRF member switch.

Viewing the version compatibility

Check whether the current and new system software images are compatible.

```
<IRF> display version comp-matrix file soft-version2.bin
```

- If they are compatible, the output is like the following:

```
Number of Matrices in Table = 1
Matrix for 5500-EI

Running Version: version1
Version Compatibility List:
version2 (Compatible)
```

The output shows that the new and current versions are fully compatible. You can use the compatible ISSU upgrade method. For more information, see "Performing compatible ISSU upgrade."

- If the two versions are incompatible, the output is like the following:

```
Number of Matrices in Table = 1
Matrix for 5500-EI

Running Version: version1
Version Compatibility List:
```

```
version2 (Incompatible)
```

The output shows that the two versions are incompatible. You must use the incompatible ISSU method. For more information, see "Performing incompatible ISSU upgrade."

Performing compatible ISSU upgrade

Upgrade the specified subordinate switch (the new master after the upgrade), which is subordinate switch 2 in this example.

```
<IRF> system-view
[IRF] issu load file soft-version2.bin slot 2
This command will begin ISSU, and the specified board will reboot and be upgraded. Please
save the current running configuration first; otherwise, the configuration may be
lost.Continue? [Y/N]:y
```

After the reboot of subordinate switch 2, check whether the system software image of salve switch 2 is **soft-version2.bin**.

```
[IRF] display boot-loader
Slot 1
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
 Slot 2
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
 Slot 3
The current boot app is:  flash:/soft-version1.bin
The main boot app is:     flash:/soft-version1.bin
The backup boot app is:   flash:/
```

The output shows that the system software image of subordinate switch 2 is soft-version2.bin.

Reboot the master manually.

```
[IRF] issu run switchover slot 2
Master will reboot, switch the specified board to master and update the line card. Continue?
[Y/N]:y
```

In this example, the member ID of the master is 1. After reboot, the master becomes a subordinate switch in the IRF fabric. Then the subordinate switches perform a role election, and salve 2 becomes the new master because the priority of subordinate switch 2 is higher than that of subordinate switch 3.

Accept the ISSU upgrade and delete the rollback timer.

```
[IRF] issu accept slot 2
```

Upgrade switch 1 and switch 3.

```
[IRF] issu commit slot 1
The specified board will reboot and be upgraded. Continue? [Y/N]:y
[IRF] issu commit slot 3
The specified board will reboot and be upgraded. Continue? [Y/N]:y
```

Then the ISSU upgrade process completes and the system software images of all IRF member switches have been upgraded to the new version.

Verify whether the current system software images on the IRF member switches are **soft-version2.bin**.

```
[IRF] display boot-loader
```

```
Slot 1
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
 Slot 2
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
 Slot 3
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
```

Performing incompatible ISSU upgrade

Upgrade the specified subordinate switch (the new master after the upgrade), which is subordinate switch 2 in this example.

```
<IRF> system-view
[IRF] issu load file soft-version2.bin slot 2
This command will begin ISSU, and the specified board will reboot and be upgraded. Please
save the current running configuration first; otherwise, the configuration may be
lost.Continue? [Y/N]: y
```

After the reboot of subordinate switch 2, reboot and upgrade all IRF member switches that have not been upgraded.

```
[IRF] issu run switchover slot 2
Master will reboot, switch the specified board to master and update the line card. Continue?
[Y/N]:y
```

Then, the ISSU upgrade process completes and the system software images of all IRF member switches have been upgraded to the new version.

Verify whether the current system software images on the IRF member switches are **soft-version2.bin**.

```
[IRF] display boot-loader
Slot 1
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
 Slot 2
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
 Slot 3
The current boot app is:  flash:/soft-version2.bin
The main boot app is:     flash:/soft-version2.bin
The backup boot app is:   flash:/
```

Managing the device

Device management includes monitoring the operating status of devices and configuring their running parameters.

The configuration tasks in this document are order independent. You can perform these tasks in any order.

Configuring the device name

A device name identifies a device in a network and works as the user view prompt at the CLI. For example, if the device name is **Sysname**, the user view prompt is <Sysname>.

To configure the device name:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the device name.	**sysname** *sysname*	The default device name is **HP**.

Changing the system time

You must synchronize your device with a trusted time source by using NTP or changing the system time before you run it on the network. Network management depends on an accurate system time setting, because the timestamps of system messages and logs use the system time. For more information about NTP configuration, see *Network Management and Monitoring Configuration Guide*.

In a small-sized network, you can manually set the system time of each device.

Configuration guidelines

You can change the system time by configuring the relative time, time zone, and daylight saving time. The configuration result depends on their configuration order (see Table 20). In the first column of this table, 1 represents the **clock datetime** command, 2 represents the **clock timezone** command, and 3 represents the **clock summer-time** command. To verify the system time setting, use the **display clock** command. This table assumes that the original system time is 2005/1/1 1:00:00.

Table 20 System time configuration results

Command	Effective system time	Configuration example	System time
1	*date-time*	`clock datetime 1:00 2007/1/1`	01:00:00 UTC Mon 01/01/2007.
2	**Original system time ±** ***zone-offset***	`clock timezone zone-time add 1`	02:00:00 zone-time Sat 01/01/2005.
1, 2	*date-time* ± ***zone-offset***	`clock datetime 2:00 2007/2/2` `clock timezone zone-time add 1`	03:00:00 zone-time Fri 02/02/2007.

Command	Effective system time	Configuration example	System time
2, 1	*date-time*	`clock timezone zone-time add 1` `clock datetime 3:00 2007/3/3`	03:00:00 zone-time Sat 03/03/2007.
3	The original system time outside the daylight saving time range: The system time does not change until it falls into the daylight saving time range.	`clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2`	01:00:00 UTC Sat 01/01/2005.
	The original system time in the daylight saving time range: The system time increases by *summer-offset*.	`clock summer-time ss one-off 00:30 2005/1/1 1:00 2005/8/8 2`	03:00:00 ss Sat 01/01/2005. NOTE: If the original system time plus *summer-offset* is beyond the daylight saving time range, the original system time does not change. After you disable the daylight saving setting, the system time automatically decreases by *summer-offset*.
1, 3	*date-time* outside the daylight saving time range: *date-time*	`clock datetime 1:00 2007/1/1` `clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2`	01:00:00 UTC Mon 01/01/2007.
	date-time in the daylight saving time range: *date-time* + *summer-offset*	`clock datetime 8:00 2007/1/1` `clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2`	10:00:00 ss Mon 01/01/2007. NOTE: If the *date-time* plus *summer-offset* is outside the daylight saving time range, the system time equals *date-time*. After you disable the daylight saving setting, the system time automatically decreases by *summer-offset*.
3, 1 (*date-time* outside the daylight saving time range)	*date-time*	`clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2` `clock datetime 1:00 2008/1/1`	01:00:00 UTC Tue 01/01/2008.

Command	Effective system time	Configuration example	System time
3, 1 (*date-time* in the daylight saving time range)	*date-time* – *summer-offset* outside the daylight saving time range: *date-time* – *summer-offset*	`clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2` `clock datetime 1:30 2007/1/1`	23:30:00 UTC Sun 12/31/2006.
	date-time – *summer-offset* in the daylight saving time range: *date-time*	`clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2` `clock datetime 3:00 2007/1/1`	03:00:00 ss Mon 01/01/2007.
2, 3 or 3, 2	Original system clock ± zone-offset outside the daylight saving time range: Original system clock ± *zone-offset*	`clock timezone zone-time add 1` `clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2`	02:00:00 zone-time Sat 01/01/2005.
	Original system clock ± zone-offset outside the daylight saving time range: Original system clock ± *zone-offset* + summer-offset	`clock timezone zone-time add 1` `clock summer-time ss one-off 1:00 2005/1/1 1:00 2005/8/8 2`	System clock configured: 04:00:00 ss Sat 01/01/2005.

1, 2 , 3 or 1, 3, 2	*date-time* ± *zone-offset* outside the daylight saving time range:
	date-time ± *zone-offset*
		`clock datetime 1:00 2007/1/1`
		`clock timezone zone-time add 1`
		`clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2`
			02:00:00 zone-time Mon 01/01/2007.

	date-time ± *zone-offset* outside the daylight saving time range:
	date-time ± *zone-offset* + *summer-offset*
		`clock datetime 1:00 2007/1/1`
		`clock timezone zone-time add 1`
		`clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2`
			04:00:00 ss Mon 01/01/2007.

2, 3, 1 or 3, 2, 1	*date-time* outside the daylight saving time range:
	date-time
		`clock timezone zone-time add 1`
		`clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2`
		`clock datetime 1:00 2007/1/1`
			01:00:00 zone-time Mon 01/01/2007.

Command	Effective system time	Configuration example	System time

	date-time in the daylight saving time range, but *date-time* – *summer-offset* outside the summer-time range:
	date-time – *summer-offset*
		`clock timezone zone-time add 1`
		`clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2`
		`clock datetime 1:30 2008/1/1`
			23:30:00 zone-time Mon 12/31/2007.

	Both *date-time* and *date-time* – *summer-offset* in the daylight saving time range:
	date-time
		`clock timezone zone-time add 1`
		`clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2`
		`clock datetime 3:00 2008/1/1`
			03:00:00 ss Tue 01/01/2008.

Configuration procedure

To change the system time:

Step	Command	Remarks
1. Set the system time and date.	**clock datetime** *time date*	Optional. Available in user view.
2. Enter system view.	**system-view**	N/A
3. Set the time zone.	**clock timezone** *zone-name* { **add** | **minus** } *zone-offset*	Optional. UTC time zone by default.
4. Set a daylight saving time scheme.	• Set a non-recurring scheme: **clock summer-time** *zone-name* **one-off** *start-time start-date end-time end-date add-time* • Set a recurring scheme: **clock summer-time** *zone-name* **repeating** *start-time start-date end-time end-date add-time*	Optional. Use either command. By default, daylight saving time is disabled, and the UTC time zone applies.

Enabling displaying the copyright statement

The device by default displays the copyright statement when a Telnet or SSH user logs in, or when a console user quits user view. You can disable or enable the function as needed. The following is a sample copyright statement:

```
**************************************************************************
* Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P.      *
* Without the owner's prior written consent,                             *
* no decompiling or reverse-engineering shall be allowed.                *
**************************************************************************
```

To enable displaying the copyright statement:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Enable displaying the copyright statement.	**copyright-info enable**	Enabled by default.

Changing the brand name

Some HP, H3C, and 3Com switches (see Table 21) can form an IRF fabric. If different brand switches are used in an IRF fabric, change their brand names to be the same to prevent a master re-election from causing network management problems.

Table 21 HP, H3C, and 3Com switch model mappings

HP switch model	H3C switch model	3COM switch model
HP 5500-24G EI Switch with 2 Interface Slots (JD377A)	S5500-28C-EI	Switch 4800G 24-Port
HP 5500-48G EI Switch with 2 Interface Slots (JD375A)	S5500-52C-EI	Switch 4800G 48-Port
HP 5500-24G-SFP EI Switch with 2 Interface Slots (JD374A)	S5500-28F-EI	Switch 4800G 24-Port SFP
HP 5500-24G-PoE+ EI Switch with 2 Interface Slots(JG241A)	S5500-28C-PWR-EI	Switch 4800G PWR 24-Port
HP 5500-48G-PoE+ EI Switch with 2 Interface Slots (JG240A)	S5500-52C-PWR-EI	Switch 4800G PWR 48-Port
HP 5500-24G SI Switch with 2 Interface Slots (JD369A)	S5500-28C-SI	N/A
HP 5500-48G SI Switch with 2 Interface Slots (JD370A)	S5500-52C-SI	N/A
HP 5500-24G-PoE+ SI Switch with 2 Interface Slots (JG238A)	S5500-28C-PWR-SI	N/A
HP 5500-48G-PoE+ SI Switch with 2 Interface Slots (JG239A)	S5500-52C-PWR-SI	N/A

Configuration preparation

Before you change the brand name for an HP, H3C, or 3Com switch, prepare the proper Boot ROM and system software image file according to the switch model mappings as listed in Table 21. The following describes the procedure for changing the brand name of an H3C or 3Com switch to HP. The procedure is the same for changing the brand names among HP, H3C, and 3Com switches.

1. Load the proper HP Boot ROM to the flash memory of the H3C or 3Com switch and use the HP Boot ROM to upgrade the Boot ROM of the switch.
2. Load the proper HP system software image file to the flash memory of the H3C or 3Com switch, specify the file as the main system software image file, and reboot the switch.
3. Execute the **brand** command and reboot the switch.

NOTE:

For HP 5500 EI and HP 5500 SI , use the **bootrom update** command to upgrade the Boot ROM.

Configuration guidelines

- After you change the brand name of a 3Com switch to HP or H3C, the default baudrate of the console port changes from 19200 to 9600.
- The port numbering rule for 3Com switches is different from that for HP and H3C switches. After you change the brand name for a 3Com switch, the port numbers become inconsistent with the silkscreen marks. Configure the port (if necessary) according to the numbering rules for the models in Table 21.
- The default settings for some features on 3Com switches are different from those on HP and H3C switches. After you change the brand name for a switch, the default settings for those features become the default settings of the target brand.

Configuration procedure

You can use the **display brand** command to display the brand names of the member switches. If any consistent brand names exist in the IRF fabric, change them to the same.

To change brand name for a member switch:

Step		Command	Remarks
1.	Change the brand name for a member switch.	**brand** { **hp** | **h3c**| **3com** } [**slot** *slot-number*]	Only the HP 5500 SI switches support the **3com** keyword.
2.	Reboot the member switch.	**reboot slot** *slot-number*	N/A

After you change the brand name for a member switch, the switch can use the later software versions for the new brand.

NOTE:

The default settings vary with different brands. Changing the brand name might affect the running configuration. After you change the brand name of a member switch, verify the configuration and re-configure the switch if necessary.

Configuring banners

Banners are messages that the system displays during user login.

The system supports the following banners:

- **Legal banner**—Appears after the copyright or license statement. To continue login, the user must enter **Y** or press **Enter**. To quit the process, the user must enter **N**. **Y** and **N** are case-insensitive.
- **Message of the Day (MOTD) banner**—Appears after the legal banner and before the login banner.
- **Login banner**—Appears only when password or scheme authentication has been configured.
- **Incoming banner**—Appears for Modem users.
- **Shell banner**—Appears for non-Modem users.

Banner message input modes

You can configure a banner in one of the following ways:

- Single-line input

  Input the entire banner in the same line as the command. The start and end delimiters for the banner must be the same but can be any visible character. The input text, including the command keywords and the delimiters cannot exceed 510 characters. In this mode, do not press **Enter** before you input the end delimiter. For example, you can configure the shell banner "Have a nice day." as follows:

  ```
  <System> system-view
  [System] header shell %Have a nice day.%
  ```

- Multiple-line input

  Input message text in multiple lines. In this approach, the message text can be up to 2000 characters. Use one of the following methods to implement multi-line input mode:

  - **Method 1**—Press **Enter** after the last command keyword. At the system prompt, enter the banner message and end with the delimiter character %. For example, you can configure the banner "Have a nice day. Please input the password." as follows:

    ```
    <System> system-view
    [System] header shell
    Please input banner content, and quit with the character '%'.--System prompt
    Have a nice day.
    Please input the password.%
    ```

  - **Method 2**—After you type the last command keyword, type any character as the start delimiter for the banner message and press **Enter**. At the system prompt, type the banner message and end the last line with a delimiter that is the same as the start delimiter. For example, you can configure the banner "Have a nice day. Please input the password." as follows:

    ```
    <System> system-view
    [System] header shell A
    Please input banner content, and quit with the character 'A'.--System prompt
    Have a nice day.
    Please input the password.A
    ```

  - **Method 3**—After you type the last keyword, type the start delimiter and part of the banner message and press **Enter**. At the system prompt, enter the rest of the banner and end the last line with a delimiter that is the same as the start delimiter. In this approach, you can use any character as the start and end delimiters but must make sure that it is not the same as the end character of the message text in the first line. For example, you can configure the banner "Have a nice day. Please input the password." as follows:

    ```
    <System> system-view
    [System] header shell AHave a nice day.
    Please input banner content, and quit with the character 'A'.--System prompt
    Please input the password.A
    ```

Configuration procedure

To configure a banner:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the incoming banner.	**header incoming** *text*	Optional
3.	Configure the login banner.	**header login** *text*	Optional
4.	Configure the legal banner.	**header legal** *text*	Optional
5.	Configure the shell banner.	**header shell** *text*	Optional
6.	Configure the MOTD banner.	**header motd** *text*	Optional

Configuring the exception handling method

You can configure the device to handle system exceptions in one of the following methods:

- **reboot**—The device automatically reboots to recover from the error condition.
- **maintain**—The device stays in the error condition so you can collect complete data, including error messages, for diagnosis. In this approach, you must manually reboot the device.

To configure the exception handling method:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Configure the exception handling method.	**system-failure** { **maintain** | **reboot** }	By default, the system reboots when an exception occurs.

NOTE:

In an IRF fabric, the exception handling method applies to only the master member switch.

Rebooting the device

CAUTION:

- A reboot can interrupt network services.
- To avoid data loss, use the **save** command to save the current configuration before a reboot.
- Use the **display startup** and **display boot-loader** commands to verify that you have correctly set the startup configuration file and the main system software image file. If the main system software image file has been corrupted or does not exist, the device cannot reboot. You must re-specify a main system software image file, or power off the device and then power it on so the system can reboot with the backup system software image file.

You can reboot the device in one of the following ways to recover from an error condition:

- Reboot the device immediately at the CLI.
- At the CLI, schedule a reboot to occur at a specific time and date or after a delay.
- Power off and then power on the device. This method might cause data loss and hardware damage, and is the least preferred method.
- Reboot at the CLI enables easy remote device maintenance.

Rebooting devices immediately at the CLI

To reboot a device, perform the following task in user view:

Task	Command	Remarks
Reboot a switch or all IRF member switches immediately.	**reboot** [**slot** *slot-number*]	If you do not specify any IRF member ID for the *slot-number* argument, all IRF member switches reboot.

Scheduling a device reboot

The switch supports only one device reboot schedule. If you configure the **schedule reboot delay** command multiple times, the last configuration takes effect.

The **schedule reboot at** command and the **schedule reboot delay** command overwrite each other, and whichever is configured last takes effect.

For data security, if you are performing file operations at the reboot time, the system does not reboot.

To schedule a device reboot, perform the following task in user view:

Task	Command	Remarks
Schedule a reboot.	• Schedule a reboot to occur at a specific time and date: **schedule reboot at** *hh:mm* [*date*] • Schedule a reboot to occur after a delay: **schedule reboot delay** { *hh:mm* | *mm* }	Use either command. The scheduled reboot function is disabled by default. Changing any clock setting can cancel the reboot schedule.

Scheduling jobs

You can schedule a job to automatically run a command or a set of commands without administrative interference. The commands in a job are polled every minute. When the scheduled time for a command is reached, the job automatically executes the command. If a confirmation is required while the command is running, the system automatically inputs **Y** or **Yes**. If characters are required, the system automatically inputs a default character string, or inputs an empty character string when there is no default character string.

Job configuration approaches

You can configure jobs in a non-modular or modular approach. Use the non-modular approach for a one-time command execution and use non-modular approach for complex maintenance work.

Table 22 A comparison of non-modular and modular approaches

Comparison item	Scheduling a job in the non-modular approach	Scheduling a job in the modular approach
Configuration method	Configure all elements in one command	Separate job, view, and time settings.
Can multiple jobs be configured?	No	Yes
Can a job have multiple commands?	No If you use the **schedule job** command repeatedly, only the last configuration takes effect.	Yes You can use the **time** command in job view to configure commands to be executed at different time points.
Supported views	User view and system view. In the **schedule job** command, shell represents user view, and system represents system view.	All views. In the **time** command, monitor represents user view.
Supported commands	Commands in user view and system view	Commands in all views.
Can a job be repeatedly executed?	No	Yes
Can a job be saved to the configuration file?	No	Yes

Configuration guidelines

- To ensure an accurate system time setting, you must configure the correct system time and date or configure NTP for the device. For NTP configuration, see *Network Management and Monitoring Configuration Guide*.
- To have a job successfully run a command, check that the specified view and command are valid. The system does not verify their validity.
- The configuration interface, view, and user status that you have before job execution restores even if the job ran a command to change the user interface (for example, **telnet**, **ftp**, and **ssh2**), the view (for example, **system-view** and **quit**), or the user status (for example, **super)**.
- The jobs run in the background without displaying any messages except log, trap and debugging messages.
- In the modular approach:
  - Every job can have only one view and up to 10 commands. If you specify multiple views, the one specified the last takes effect.
  - Input a view name in its complete form. Most commonly used view names include **monitor** for user view, **system** for system view, **GigabitEthernet x/x/x**, and **Ten-GigabitEthernet x/x/x** for Ethernet interface view, and **Vlan-interfacex** for VLAN interface view.
  - The time ID (*time-id*) must be unique in a job. If two time and command bindings have the same time ID, the one configured last takes effect.

Scheduling a job in the non-modular approach

Perform one of the following commands in user view to schedule a job:

Step	Command	Remarks
Schedule a job.	• Schedule a job to run a command at a specific time: **schedule job at** *time* [*date*] **view** *view command* • Schedule a job to run a command after a delay: **schedule job delay** *time* **view** *view command*	Use either command. NOTE: • If you execute the **schedule job** command repeatedly, the last configuration takes effect. • Changing any clock setting can cancel the job set by using the **schedule job** command.

Scheduling a job in the modular approach

To configure a scheduled job:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Create a job and enter job view.	**job** *job-name*	N/A
3.	Specify the view in which the commands in the job run.	**view** *view-name*	You can specify only one view for a job. The job executes all commands in the specified view.
4.	Add commands to the job.	• Configure a command to run at a specific time and date: **time** *time-id* **at** *time date* **command** *command* • Configure a command to run at a specific time: **time** *time-id* { **one-off** | **repeating** } **at** *time* [**month-date** *month-day* | **week-day** *week-daylist*] **command** *command* • Configure a command to run after a delay: **time** *time-id* { **one-off** | **repeating** } **delay** *time* **command** *command*	Use any of the commands. NOTE: Changing a clock setting does not affect the schedule set by using the **time at** or **time delay** command.

Disabling Boot ROM access

By default, anyone can press **Ctrl+B** during startup to enter the Boot menu and configure the Boot ROM. To protect the system, you can disable Boot ROM access so the users can access only the CLI.

You can also set a Boot ROM password the first time you access the Boot menu to protect the Boot ROM.

To view Boot ROM accessibility status, use the **display startup** command. For more information about the **display startup** command, see *Fundamentals Command Reference*.

To disable Boot ROM access, execute the following command in user view:

Task	Command	Remarks
Disable Boot ROM access.	**undo startup bootrom-access enable**	By default, Boot ROM access is enabled. Before using this command, make sure the versions of the Boot ROM image and the Comware images are consistent. For information about Boot ROM image and Comware image versions, see the release notes.

Configuring the port status detection timer

Some protocols might shut down ports under specific circumstances. For example, MSTP shuts down a BPDU guard enabled port when the port receives a BPDU. Then, the device starts the detection timer. If the port is still down when the detection timer expires, the port quits the shutdown status and resumes its actual physical status.

To configure the port status detection timer:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure the port status detection timer.	**shutdown-interval** *time*	The detection timer is 30 seconds by default.

Configuring temperature thresholds for a device

You can set the temperature thresholds to monitor the temperature of a device.

The temperature thresholds include lower threshold, warning threshold, and shutdown threshold. The shutdown threshold is not user configurable.

- When the device temperature drops below the lower threshold or reaches the warning threshold, the device logs the event and outputs a log message and a trap.
- When the device temperature reaches the shutdown threshold, the device logs the event, outputs a log message and a trap, and automatically shuts down.

To configure temperature thresholds for an IRF member device:

Step	Command	Remarks
1. Enter system view.	**system-view**	N/A
2. Configure temperature thresholds for an IRF member device.	**temperature-limit slot** *slot-number* **hotspot** *sensor-number lowerlimit warninglimit*	By default, the lower threshold is –5°C (23°F), and the warning threshold is 55°C (131°F). The warning threshold must be higher than the lower threshold.

Clearing unused 16-bit interface indexes

The device must maintain persistent 16-bit interface indexes and keep one interface index match one interface name for network management. After deleting a logical interface, the device retains its 16-bit interface index so the same index can be assigned to the interface at interface re-creation.

To avoid index depletion causing interface creation failures, you can clear all 16-bit indexes that have been assigned but not in use. The operation does not affect the interface indexes of the interfaces that have been created but the indexes assigned to re-recreated interfaces might change.

A confirmation is required when you execute this command. The command will not run if you fail to make a confirmation within 30 seconds or enter **N** to cancel the operation.

To clear unused 16-bit interface indexes, perform the following task in user view:

Task	Command	Remarks
Clear unused 16-bit interface indexes.	**reset unused porttag**	In an IRF fabric, the command applies to all member switches.

Disabling password recovery capacity

Password recovery capability controls console user access to the device configuration and SDRAM from BootROM menus.

If password recovery capability is enabled, a console user can access the device configuration without authentication and reconfigure the console login password and user privilege level passwords.

If password recovery capability is disabled, a console user must restore the factory-default configuration before configuring new passwords. Restoring the factory-default configuration deletes the next-startup configuration files.

Availability of related BootROM options varies with the password recovery capability setting. For more information, see *the release notes*.

To enhance system security:

Step		Command	Remarks
1.	Enter system view.	**system-view**	N/A
2.	Enable password recovery capacity.	**password-recovery enable**	By default, password recovery capability is enabled.
3.	Disable password recovery capacity.	**undo password-recovery enable**	

Verifying and diagnosing transceiver modules

Support for the pluggable transceivers and the transceiver type depends on the device model.

Verifying transceiver modules

You can verify the genuineness of a transceiver module in the following ways:

- Display the key parameters of a transceiver module, including its transceiver type, connector type, central wavelength of the transmit laser, transfer distance and vendor name.
- Display its electronic label. The electronic label is a profile of the transceiver module and contains the permanent configuration including the serial number, manufacturing date, and vendor name. The data is written to the storage component during debugging or testing.

To verify transceiver modules, perform the following tasks in any view:

Task	Command
Display key parameters of transceiver modules.	**display transceiver interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
Display electronic label data for transceiver modules.	**display transceiver manuinfo interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Diagnosing transceiver modules

The device provides the alarm function and digital diagnosis function for transceiver modules. When a transceiver module fails or inappropriately operates, you can check for alarms present on the transceiver module to identify the fault source or examine the key parameters monitored by the digital diagnosis function, including the temperature, voltage, laser bias current, TX power, and RX power.

To diagnose transceiver modules, perform the following tasks in any view:

Task	Command
Display alarms present on transceiver modules.	**display transceiver alarm interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]
Display the present measured values of the digital diagnosis parameters for pluggable transceivers.	**display transceiver diagnosis interface** [*interface-type interface-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

Displaying and maintaining device management

For diagnosis or troubleshooting, you can use separate **display** commands to collect running status data module by module, or use the **display diagnostic-information** command to bulk collect running data for multiple modules. The **display diagnostic-information** command equals this set of commands: **display clock**, **display version**, **display device**, and **display current-configuration**.

Task	Command	Remarks
Display system version information.	**display version** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the system time and date.	**display clock** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display or save operating statistics for multiple feature modules.	**display diagnostic-information** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Task	Command	Remarks
Display CPU usage statistics.	**display cpu-usage** [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*] **display cpu-usage** *entry-number* [*offset*] [**verbose**] [**slot** *slot-number*] [**cpu** *cpu-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display historical CPU usage statistics in a chart.	**display cpu-usage history** [**task** *task-id*] [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display hardware information.	**display device** [[**slot** *slot-number* [**subslot** *subslot-number*]] | **verbose**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the electronic label data for the device.	**display device manuinfo** [**slot** *slot-number* [**subslot** *subslot-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display device temperature statistics.	**display environment** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the operating states of fan trays.	**display fan** [**slot** *slot-number* [*fan-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display memory usage statistics.	**display memory** [**slot** *slot-number* [**cpu** *cpu-number*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display power supply information.	**display power** [**slot** *slot-number* [*power-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the mode of the last reboot.	**display reboot-type** [**slot** *slot-number*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display RPS status information.	**display rps** [**slot** *slot-number* [*rps-id*]] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the configuration of the job configured by using the **schedule job** command.	**display schedule job** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the device reboot setting.	**display schedule reboot** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the configuration of jobs configured by using the **job** command.	**display job** [*job-name*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view
Display the exception handling method.	**display system-failure** [**|** { **begin** | **exclude** | **include** } *regular-expression*]	Available in any view

Automatic configuration

Only the 5500 EI switches support Layer 3 Ethernet port configuration.

The term "interface" in this chapter collectively refers to VLAN interfaces and Layer 3 Ethernet interfaces. You can set an Ethernet port as a Layer 3 interface by using the **port link-mode route** command (see *Layer 2—LAN Switching Configuration Guide*).

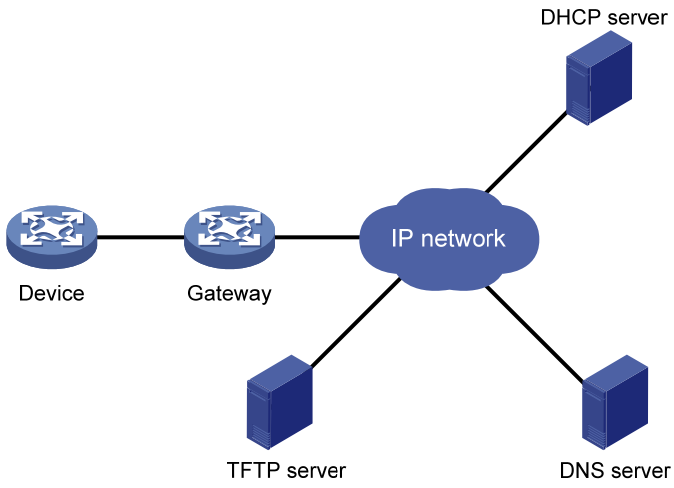
Overview

Automatic configuration enables a device without any configuration file to automatically obtain and execute a configuration file during startup. Automatic configuration simplifies network configuration, facilitates centralized management, and reduces maintenance workload.

To implement automatic configuration, the network administrator saves configuration files on a server and a device automatically obtains and executes a specific configuration file.

Typical application scenario

Figure 44 Network diagram



As shown in Figure 44, the device implements automatic configuration with the cooperation of the following servers:

- **DHCP server**—Assigns an IP address and other configuration parameters such as the configuration file name, TFTP server IP address, and DNS server IP address to the device.
- **TFTP server**—Saves files needed in automatic configuration. The device gets the files needed from the TFTP server, such as the host name file that saves mappings between host IP addresses and host names, and the configuration file.
- **DNS server**—Resolves between IP addresses and host names. In some cases, the device resolves its IP address to the corresponding host name through the DNS server, and then uses the host name to request the configuration file with the same name (**hostname.cfg**) from the TFTP server. If the device

gets the domain name of the TFTP server from the DHCP response, the device can also resolve the domain name of the TFTP server to the IP address of the TFTP server through the DNS server.

If the DHCP server, TFTP server, DNS server, and the device are not in the same network segment, you need to configure the DHCP relay agent on the gateway, and configure routing protocols to enable each server and the device to reach one another.

How automatic configuration works

Automatic configuration works in the following manner:

1. During startup, the device sets the first up interface (if up Layer 2 Ethernet ports exist, the VLAN interface of the default VLAN of the Ethernet ports is selected as the first up interface. Otherwise, the up Layer 3 Ethernet interface with the smallest interface number is selected as the first up interface) as the DHCP client to request parameters from the DHCP server, such as an IP address and name of a TFTP server, IP address of a DNS server, and the configuration file name.
2. After getting related parameters, the device sends a TFTP request to obtain the configuration file from the specified TFTP server and executes the configuration file. If the client cannot get such parameters, it uses the factory defaults.

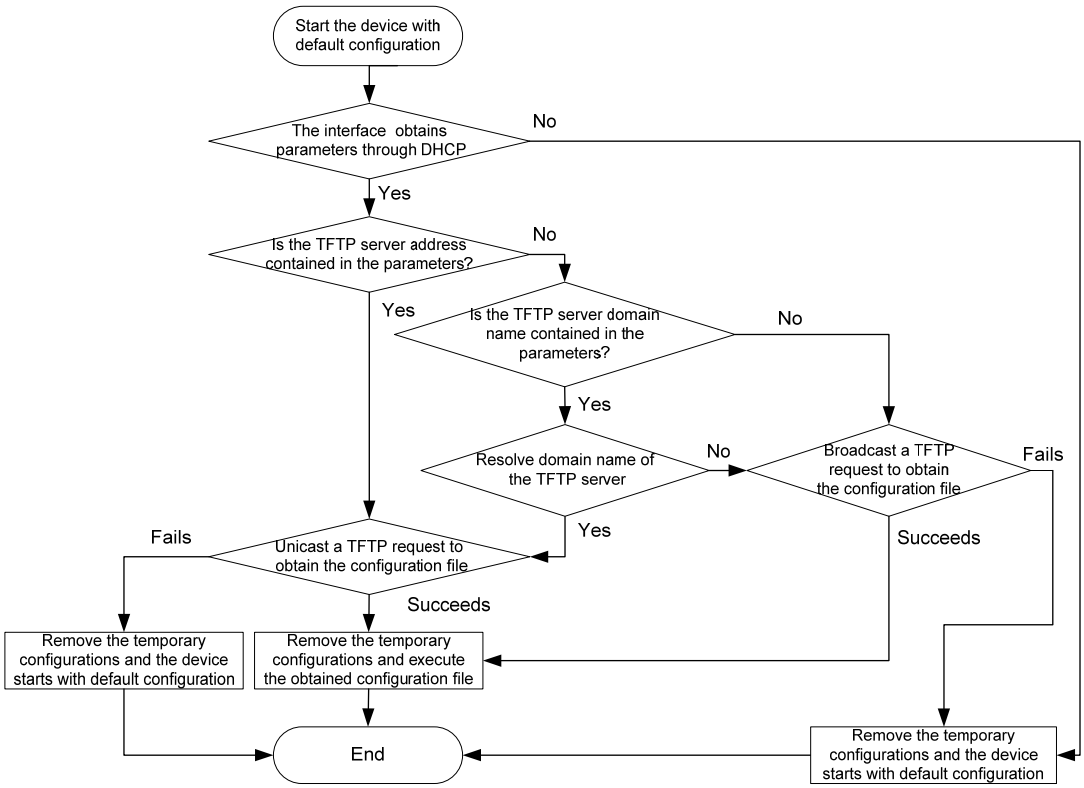
To implement automatic configuration, you must configure the DHCP server, DNS server, and TFTP server, but you do not need to perform any configuration on the device that performs automatic configuration.

Before starting the device, connect only the interface needed in automatic configuration to the network.

Automatic configuration work flow

Figure 45 shows the work flow of automatic configuration.

Figure 45 Automatic configuration work flow



Using DHCP to obtain an IP address and other configuration information

Address acquisition process

As previously mentioned, a device sets the first up interface as the DHCP client during startup. The DHCP client broadcasts a DHCP request, where the Option 55 field specifies the information that the client wants to obtain from the DHCP server such as the configuration file name, domain name and IP address of the TFTP server, and DNS server IP address.

After receiving the DHCP response from the DHCP server, the device obtains the IP address and resolves the following fields in the DHCP response:

- Option 67 or the file field—Obtains the configuration file name. The device resolves Option 67 first. If Option 67 contains the configuration file name, the device does not resolve the file field. If not, the device resolves the file field.
- Option 66—Obtains the TFTP server domain name
- Option 150—Obtains the TFTP server IP address
- Option 6—Obtains the DNS server IP address.

If no response is received from the DHCP server, the device removes the temporary configuration and starts up with the factory defaults.

The temporary configuration contains two parts: the configuration made on the interface through which automatic configuration is performed, and the **ip host** command in the host name file. The temporary configuration is removed by executing the corresponding **undo** commands.

For more information about DHCP, see *Layer 3—IP Services Configuration Guide*. For more information about the **ip host** command, see *Layer 3—IP Services Command Reference*.

Principles for selecting an address pool on the DHCP server

The DHCP server selects IP addresses and other network configuration parameters from an address pool for clients. DHCP supports the following types of address pools:

- **Dynamic address pool**—A dynamic address pool contains a range of IP addresses and other parameters that the DHCP server dynamically assigns to clients.
- **Static address pool**—A static address pool contains the binding of an IP address and a MAC address (or a client ID). The DHCP server assigns the IP address of the binding and specific configuration parameters to a requesting client whose MAC address or ID is contained in the binding. In this way, the client can get a fixed IP address.

Select address pools by using one of the following methods:

- If devices use the same configuration file, you can configure a dynamic address pool on the DHCP server to assign IP addresses and the same configuration parameters (for example, configuration file name) to the devices. In this case, the configuration file can only contain common configurations of the devices, and the specific configurations of each device need to be performed in other ways. For example, the configuration file can enable Telnet and create a local user on devices so the administrator can Telnet to each device to perform specific configurations (for example, configure the IP address of each interface).
- If devices use different configuration files, you need to configure static address pools to make sure each device can get a fixed IP address and a specific configuration file. With this method, no more configuration is required for the devices.

To configure static address pools, you must obtain corresponding client IDs. To obtain a device's client ID, use the **display dhcp server ip-in-use** command to display address binding information on the DHCP server after the device obtains its IP address through DHCP.

Obtaining the configuration file from the TFTP server

A device can obtain the following files from the TFTP server during automatic configuration:

- Configuration file specified by the Option 67 or file field in the DHCP response.
- Host name file named network.cfg that stores mappings between IP addresses and host names.

For example, the host name file can include the following:

```
ip host host1 101.101.101.101
ip host host2 101.101.101.102
ip host client1 101.101.101.103
ip host client2 101.101.101.104
```

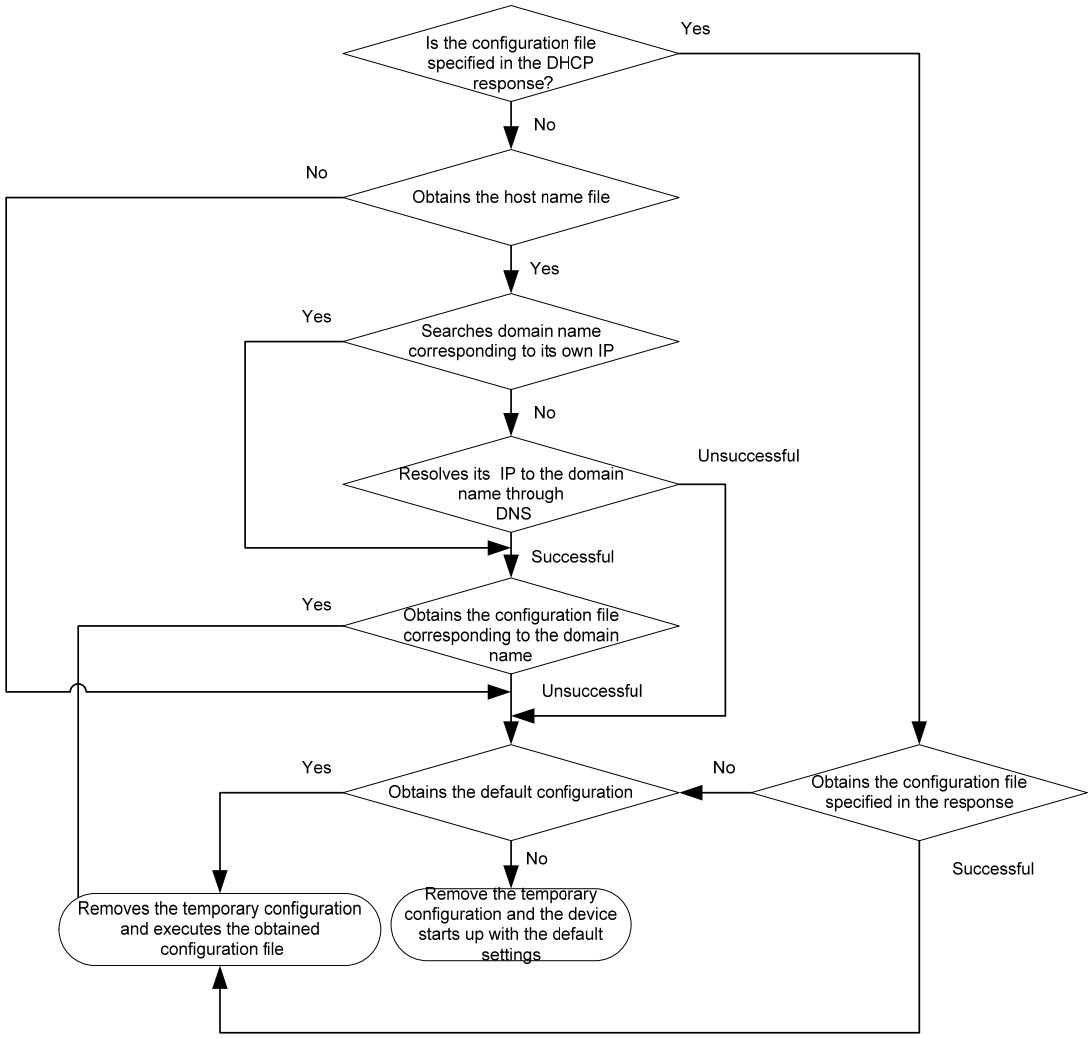
IMPORTANT:

- There must be a space before the keyword **ip host**.
- The host name of a device saved in the host name file must be the same as the configuration file name of the device, and can be identical with or different from that saved in the DNS server.

- Configuration file for the device, which is named *hostname*.cfg (*hostname* is the host name of the device). For example, if the host name of a device is **aaa**, the configuration file for the device is named **aaa.cfg**.
- Default configuration file named **device.cfg**.

Obtaining the configuration file

Figure 46 Obtaining the configuration file



A device obtains its configuration file by using the following workflow:

- If the DHCP response contains the configuration file name, the device requests the specified configuration file from the TFTP server.
- If not, the device tries to get its host name from the host name file obtained from the TFTP server. If it fails, the device resolves its IP address to the host name through DNS server. Once the device gets its host name, it requests the configuration file with the same name from the TFTP server.
- If all the above operations fail, the device requests the default configuration file from the TFTP server.

TFTP request sending mode

The device chooses whether to unicast or broadcast a TFTP request as follows:

- If a legitimate TFTP server IP address is contained in the DHCP response, the device unicasts a TFTP request to the TFTP server.
- If not, the device resolves the TFTP server domain name contained in the DHCP response to the corresponding IP address through the DNS server. If successful, the device unicasts a TFTP request to the TFTP server; if not, the device broadcasts a TFTP request.

- If the IP address and the domain name of the TFTP server are not contained in the DHCP response or they are illegitimate, the device broadcasts a TFTP request.

After broadcasting a TFTP request, the device selects the TFTP server that responds first to obtain the configuration file. If the requested configuration file does not exist on the TFTP server, the request operation fails, and the device removes the temporary configuration and starts up with the factory defaults.

If the device and the TFTP server reside in different subnets, you must configure the UDP Helper function for the gateway to change the broadcast TFTP request from the device to a unicast packet and forward the unicast packet to the specified TFTP server. For more information about UDP Helper, see *Layer 3—IP Services Configuration Guide*.

Executing the configuration file

After obtaining the configuration file, the device removes the temporary configuration and executes the configuration file. If no configuration file is obtained, the device removes the temporary configuration and starts up with the factory defaults.

NOTE:

If the configuration file contains any IRF configuration, the device does not execute the IRF configuration when executing the configuration file.

The configuration file is deleted after executed. Save the configuration by using the **save** command. Otherwise, the device has to perform automatic configuration again after reboot. For more information about the **save** command, see *Fundamentals Command Reference*.

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

http://www.hp.com/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/go/wwalerts

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

http://www.hp.com/support/manuals

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com http://www.hp.com
- HP Networking http://www.hp.com/go/networking
- HP manuals http://www.hp.com/support/manuals
- HP download drivers and software http://www.hp.com/support/downloads
- HP software depot http://www.software.hp.com
- HP Education http://www.hp.com/learn

Conventions

This section describes the conventions used in this documentation set.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the **New User** window appears; click **OK**.
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
TIP	An alert that provides helpful information.

Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the switching engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a security product, such as a firewall, a UTM, or a load-balancing or security card that is installed in a device.
	Represents a security card, such as a firewall card, a load-balancing card, or a NetStream card.

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

Index