Abstract

This document describes the software features for the HP 5820X & 5800 Series products and guides you through the software configuration procedures. These configuration guides also provide configuration examples to help you apply software features to different network scenarios.

This documentation is intended for network planners, field technical support and servicing engineers, and network administrators working with the HP 5820X & 5800 Series products.
Legal and notice information

© Copyright 2013 Hewlett-Packard Development Company, L.P.

No part of this documentation may be reproduced or transmitted in any form or by any means without prior written consent of Hewlett-Packard Development Company, L.P.

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

## Configuring the CLI

- Entering the CLI .................................................................................................................. 1
- Command conventions ......................................................................................................... 2
- Undo form of a command ...................................................................................................... 3
- CLI view description .............................................................................................................. 3
  - Entering system view ............................................................................................................ 4
  - Exiting the current view ...................................................................................................... 4
  - Returning to user view ...................................................................................................... 4
- Using online help ................................................................................................................. 5
- Entering commands .............................................................................................................. 6
  - Editing command lines ...................................................................................................... 6
  - Entering incomplete keywords .......................................................................................... 6
  - Configuring command aliases .......................................................................................... 6
  - Configuring CLI hotkeys .................................................................................................... 7
  - Redisplaying entered but not submitted commands ........................................................ 8
- Checking command line errors ............................................................................................ 9
- Using command history ....................................................................................................... 9
  - Accessing history commands ............................................................................................. 9
  - Configuring the history buffer size .................................................................................. 10
- Controlling the CLI display ................................................................................................ 10
  - Multi-screen display ......................................................................................................... 10
  - Filtering output information ............................................................................................... 11
- Configuring user privilege and command levels ............................................................... 14
  - Configuring a user privilege level ..................................................................................... 15
  - Switching user privilege level ........................................................................................... 18
  - Modifying the level of a command .................................................................................... 20
- Saving the current configuration .......................................................................................... 21
- Displaying and maintaining CLI ......................................................................................... 21

## Login methods

- Users and user interfaces .................................................................................................. 23
  - Numbering user interfaces ............................................................................................... 24

## CLI login

- Logging in through the console port .................................................................................... 25
  - Configuration requirements .............................................................................................. 25
  - Login procedure ............................................................................................................... 26
  - Console login authentication modes .................................................................................. 28
    - Configuring none authentication for console login ....................................................... 29
    - Configuring password authentication for console login .............................................. 30
    - Configuring scheme authentication for console login .................................................. 32
- Configuring common settings for console login (optional) ................................................ 35
- Logging in through Telnet ................................................................................................... 36
  - Telnet login authentication modes .................................................................................... 37
    - Configuring none authentication for Telnet login ....................................................... 38
    - Configuring password authentication for Telnet login .............................................. 40
    - Configuring scheme authentication for Telnet login ................................................... 41
    - Configuring common settings for VTY user interfaces (optional) ................................ 44
    - Configuring the device to log in to a Telnet server as a Telnet client ......................... 46
- Logging in through SSH ...................................................................................................... 47
Configuring the CLI

CLI enables you to interact with your device by typing text commands. At the CLI, instruct your device to perform a given task by typing a text command and then pressing **Enter**. Compared with the graphical user interface (GUI) where you can use a mouse to perform configurations, the CLI allows you to enter more information in one command line.

**Figure 1 CLI example**

```
User interface aux0 is available.

Press ENTER to get started.
<HP>system-view
System View: return to User View with Ctrl+Z.
[HP]
```

Entering the CLI

HP devices provide multiple methods for entering the CLI, such as through the console port, through Telnet, or through SSH. For more information, see “Login methods.”
Command conventions

Command conventions help you understand command meanings. Commands in HP product manuals comply with the conventions listed in Table 1.

Table 1 Command conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
<td>Bold text represents commands and keywords you enter literally as shown.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Italic text represents arguments you replace with actual values.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose syntax choices (keywords or arguments) that are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>&amp;&lt;1-n&gt;</td>
<td>The argument or keyword and argument combination before the ampersand (&amp;) sign can be entered 1 to n times.</td>
</tr>
<tr>
<td>#</td>
<td>A line that starts with a pound (#) sign is comments.</td>
</tr>
</tbody>
</table>

**NOTE:**

The keywords of HP command lines are case insensitive.

Use `clock datetime time date` as an example to understand the meaning of the command line parameters according to Figure 2.

**Figure 2 Read command line parameters**

For example, enter the following at the CLI of your device and press **Enter** to set the device system time to 10 o’clock 30 minutes 20 seconds, February 23, 2010.

<sysname> clock datetime 10:30:20 2/23/2010

Read any command that is more complicated by referring to Table 1.
Undo form of a command

The **undo** form of a command restores the default, disables a function, or removes a configuration.

Almost all configuration commands have an **undo** form. For example, `info-center enable` enables the information center and `undo info-center enable` disables the information center.

### CLI view description

Commands are grouped into different classes by function. To use a command, you must enter the class view of the command.

CLI views adopt a hierarchical structure. See Figure 3.

- After logging in to the switch, you are in user view. The prompt of user view is `<device name>`. In user view, perform display, debugging, and file management operations, set the system time, restart your device, and perform FTP and Telnet operations.
- Enter system view from user view. In system view, configure parameters such as daylight saving time, banners, and short-cut keys.
- From system view, enter different function views. For example, enter interface view to configure interface parameters, create a VLAN and enter its view, enter user interface view to configure login user attributes, create a local user and enter local user view to configure the password and level of the local user, and enter OSPF view to configure OSPF parameters.

---

**NOTE:**

Enter `?` in any view to display all commands that can be executed in this view.

---

**Figure 3 Command line views**

![Command line views diagram](image-url)
**Entering system view**

When you log in to the device, you automatically enter user view, where `<Device name>` is displayed. Perform limited operations in user view, for example, display operations, file operations, and Telnet operations.

To perform further configuration for the device, enter system view.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available in user view</td>
</tr>
</tbody>
</table>

**Exiting the current view**

The CLI is divided into different command views. Each view has a set of specific commands and defines the effective scope of the commands. The commands available to you at any given time depend on the view you are in.

Follow the step below to exit the current view:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Return to the parent view from</td>
<td>quit</td>
<td>Required.</td>
</tr>
<tr>
<td>the current view.</td>
<td></td>
<td>Available in any view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In user view, <code>quit</code> stops the current</td>
</tr>
<tr>
<td></td>
<td></td>
<td>connection between the terminal and the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>device.</td>
</tr>
</tbody>
</table>

In public key code view, use `public-key-code end` to return to the parent view (public key view).

In public key view, use `peer-public-key end` to return to system view.

**Returning to user view**

This feature allows you to return to user view from any other view, without using `quit` command repeatedly. Alternately, press `Ctrl+Z` to return to user view from the current view.

Follow the step below to exit to user view:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>return</td>
<td>Required.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available in any view except user view.</td>
</tr>
</tbody>
</table>
Using online help

Enter a question mark (?) to obtain online help. See the following examples.

1. Enter ? in any view to display all commands available in this view and brief descriptions of these commands. 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
   cd Change current directory
   …Omitted…

2. Enter part of a command and a ? separated by a space.

   If ? is at the position of a keyword, the CLI displays all possible keywords with a brief description for each keyword. For example:

   <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

   If ? is at the position of an argument, the CLI displays a description about this argument. For example:

   <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 a complete command. Execute the command by pressing Enter.

3. Enter an incomplete character string followed by a ?. The CLI displays all commands starting with the entered character(s).

   <sysname> c?
   cd
cfd
clock
cluster
copy
<sysname> display cl?
clipboard
clock
cluster
Entering commands

Editing command lines

Table 2 lists some shortcut keys you can use to edit command lines.

Table 2 Editing functions

<table>
<thead>
<tr>
<th>Key</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common keys</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Backspace</strong></td>
<td>Deletes the character to the left of the cursor and moves the cursor back one character.</td>
</tr>
<tr>
<td><strong>Left arrow key or Ctrl+B</strong></td>
<td>The cursor moves one character space to the left.</td>
</tr>
<tr>
<td><strong>Right arrow key or Ctrl+F</strong></td>
<td>The cursor moves one character space to the right.</td>
</tr>
</tbody>
</table>
| **Tab**           | If you press Tab after entering part of a keyword, the system automatically completes the keyword:  
 | | • If finding a unique match, the system substitutes the complete keyword for the incomplete one and displays it in the next line.  
 | | • If there is more than one match, press Tab repeatedly to view in cycles all keywords starting with the character string you entered.  
 | | • If there is no match, the system does not modify the incomplete keyword and displays it again in the next line. |

Entering incomplete keywords

Enter a command comprising incomplete keywords that 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, enter sy.
- To set the configuration file for next startup, enter st s.

Press Tab to have an incomplete keyword automatically completed.

Configuring command aliases

The command alias function allows you to replace the first keyword of a command with your preferred keyword. For example, if you configure show as the replacement for the display keyword, then to run display xx, enter the command alias show xx.

The following guidelines apply when configuring a command alias:

- Define and use a command alias. The command is not restored in its alias format.
- When you define a command alias, the cmdkey and alias arguments must be in their complete form.
- When you enter an incomplete keyword that partially matches both a defined alias and the keyword of a command, the alias takes effect. To execute the command whose keyword partially matches your entry, enter the complete keyword. When you enter a character string that partially matches multiple aliases, the system gives you prompts.
- If you press Tab after you enter the keyword of an alias, the original format of the keyword is displayed.
- Replace only the first keyword of a non-undo command instead of the complete command; and replace only the second keyword of undo commands.

To configure command aliases:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enable the command alias function. | command-alias enable | Required
|      |                     |          | Disabled by default, which means you cannot configure command aliases. |
| 3.   | Configure a command alias. | command-alias mapping cmdkey alias | Required
|      |                     |          | Not configured by default. |

**Configuring CLI hotkeys**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Configure CLI hotkeys. | hotkey { CTRL_G | CTRL_L | CTRL_O | CTRL_T | CTRL_U } command | Optional
|      | | By default, the Ctrl+G, Ctrl+L and Ctrl+O hotkeys are associated with pre-defined commands and the Ctrl+T and Ctrl+U hotkeys are not.
|      | | • Ctrl+G corresponds to display current-configuration.
|      | | • Ctrl+L corresponds to display ip routing-table.
|      | | • Ctrl+O corresponds to undo debugging all. |
| 3.   | Display hotkeys. | display hotkey | Available in any view.
|      | | See Table 3 for hotkeys reserved by the system. |

**Table 3 Hotkeys reserved by the system**

The hotkeys in this table above are defined by the switch. If the same hotkeys are defined by the terminal software you use to interact with the switch, the hotkeys defined by the terminal software take effect.

<table>
<thead>
<tr>
<th>Hotkey</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl+A</td>
<td>Moves the cursor to the beginning of the current line.</td>
</tr>
<tr>
<td>Ctrl+B</td>
<td>Moves the cursor one character to the left.</td>
</tr>
<tr>
<td>Ctrl+C</td>
<td>Stops performing a command.</td>
</tr>
<tr>
<td>Ctrl+D</td>
<td>Deletes the character at the current cursor position.</td>
</tr>
<tr>
<td>Ctrl+E</td>
<td>Moves the cursor to the end of the current line.</td>
</tr>
<tr>
<td>Ctrl+F</td>
<td>Moves the cursor one character to the right.</td>
</tr>
<tr>
<td>Ctrl+H</td>
<td>Deletes the character to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl+K</td>
<td>Terminates an outgoing connection.</td>
</tr>
<tr>
<td>Ctrl+N</td>
<td>Displays the next command in the history command buffer.</td>
</tr>
<tr>
<td>Hotkey</td>
<td>Function</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
</tr>
<tr>
<td>Ctrl+P</td>
<td>Displays the previous command in the history command buffer.</td>
</tr>
<tr>
<td>Ctrl+R</td>
<td>Redisplays the current line information.</td>
</tr>
<tr>
<td>Ctrl+V</td>
<td>Pastes the content in the clipboard.</td>
</tr>
<tr>
<td>Ctrl+W</td>
<td>Deletes all characters in a continuous string to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl+X</td>
<td>Deletes all characters to the left of the cursor.</td>
</tr>
<tr>
<td>Ctrl+Y</td>
<td>Deletes all characters to the right of the cursor.</td>
</tr>
<tr>
<td>Ctrl+Z</td>
<td>Exits to user view.</td>
</tr>
<tr>
<td>Ctrl+]</td>
<td>Terminates an incoming connection or a redirect connection.</td>
</tr>
<tr>
<td>Esc+B</td>
<td>Moves the cursor to the leading character of the continuous string to the left.</td>
</tr>
<tr>
<td>Esc+D</td>
<td>Deletes all characters of the continuous string at the current cursor position and to the right of the cursor.</td>
</tr>
<tr>
<td>Esc+F</td>
<td>Moves the cursor to the front of the next continuous string to the right.</td>
</tr>
<tr>
<td>Esc+N</td>
<td>Moves the cursor down by one line (available before you press Enter)</td>
</tr>
<tr>
<td>Esc+P</td>
<td>Moves the cursor up by one line (available before you press Enter)</td>
</tr>
<tr>
<td>Esc+&lt;</td>
<td>Specifies the cursor as the beginning of the clipboard.</td>
</tr>
<tr>
<td>Esc+&gt;</td>
<td>Specifies the cursor as the ending of the clipboard.</td>
</tr>
</tbody>
</table>

Redisplaying entered but not submitted commands

If your command input is interrupted by output system information, use this feature to redisplay the previously entered but not submitted commands.

If you have no input at the command line prompt and the system outputs system information such as logs, the system will not display the command line prompt after the output.

If the system outputs system information when you are typing interactive information (not YES/NO for confirmation), the system will not redisplay the prompt information but a line break after the output and then display what you have entered.

To enable redisplaying of entered but not submitted commands:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable redisplaying of entered but not submitted commands.</td>
<td>info-center synchronous</td>
</tr>
</tbody>
</table>

Required.
Disabled by default.
For more information about info-center synchronous, see Network Management and Monitoring Configuration Guide.
Checking command line errors

If a command contains syntax errors, the CLI reports error information.

Table 4 Common command line errors

<table>
<thead>
<tr>
<th>Error information</th>
<th>Cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>% Unrecognized command found at ‘^’ position.</td>
<td>The command was not found.</td>
</tr>
<tr>
<td>% Incomplete command found at ‘^’ position.</td>
<td>Incomplete command</td>
</tr>
<tr>
<td>% Ambiguous command found at ‘^’ position.</td>
<td>Ambiguous command</td>
</tr>
<tr>
<td>Too many parameters</td>
<td>Too many parameters</td>
</tr>
<tr>
<td>% Wrong parameter found at ‘^’ position.</td>
<td>Wrong parameters</td>
</tr>
</tbody>
</table>

Using command history

The CLI automatically saves the commands recently used in the history command buffer. Access and execute them again.

Accessing history commands

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display history commands.</td>
<td>display history-command</td>
<td>Displays valid history commands you used.</td>
</tr>
<tr>
<td>Display the previous history command.</td>
<td>Up arrow key or Ctrl+P</td>
<td>Displays the previous history command, if any.</td>
</tr>
<tr>
<td>Display the next history command.</td>
<td>Down arrow key or Ctrl+N</td>
<td>Displays the next history command, if any.</td>
</tr>
</tbody>
</table>

NOTE:

Use arrow keys to access history commands in Windows 200X and XP Terminal or Telnet. However, the up and down arrow keys are invalid in Windows 9X HyperTerminal, because they are defined differently. Use Ctrl+P or Ctrl+N instead.

- The commands saved in the history command buffer are in the same format in which you entered the commands. If you enter an incomplete command, the command saved in the history command buffer is also an incomplete one.
- If you execute the same command repeatedly, the switch saves only the earliest record. However, if you execute the same command in different formats, the system saves them as different commands. For example, if you run display cu repeatedly, the system saves only one command in the history command buffer. If you execute the command in the format of display cu and display current-configuration respectively, the system saves them as two commands.
- By default, the CLI can save up to 10 commands for each user. To set the capacity of the history command buffer for the current user interface, use history-command max-size. (For more information about history-command max-size, see “Logging in to the switch commands.”)
Configuring the history buffer size

To configure the history buffer size:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>user-interface { first-num1 [ last-num1 ]</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>[ aux</td>
<td>vty ] first-num2 [ last-num2 ] }</td>
</tr>
<tr>
<td>Set the maximum number of</td>
<td>history-command max-size size-value</td>
<td>Optional</td>
</tr>
<tr>
<td>commands that can be saved in</td>
<td></td>
<td>By default,</td>
</tr>
<tr>
<td>the history buffer</td>
<td></td>
<td>the history</td>
</tr>
<tr>
<td></td>
<td></td>
<td>buffer can</td>
</tr>
<tr>
<td></td>
<td></td>
<td>save up to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10 commands.</td>
</tr>
</tbody>
</table>

**NOTE:**

For more information about `user-interface` and `history-command max-size`, see “Logging in to the switch commands.”

Controlling the CLI display

Multi-screen display

Controlling multi-screen display

If the output information spans multiple screens, each screen pauses after it is displayed. Perform one of the following operations to proceed.

<table>
<thead>
<tr>
<th>Action</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Press <code>Space</code></td>
<td>Displays the next screen.</td>
</tr>
<tr>
<td>Press <code>Enter</code></td>
<td>Displays the next line.</td>
</tr>
<tr>
<td>Press <code>Ctrl+C</code></td>
<td>Stops the display and the command execution.</td>
</tr>
<tr>
<td>Press <code>&lt;PageUp&gt;</code></td>
<td>Displays the previous page.</td>
</tr>
<tr>
<td>Press <code>&lt;PageDown&gt;</code></td>
<td>Displays the next page.</td>
</tr>
</tbody>
</table>

By default, each screen displays up to 24 lines. To change the maximum number of lines displayed on the next screen, use `screen-length`. For more information about `screen-length`, see “Logging in to the switch commands.”
Disabling multi-screen display

Use the following command to disable the multi-screen display function. All of the output information is displayed at one time and the screen is refreshed continuously until the last screen is displayed.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable the multi-screen display function</td>
<td><code>screen-length disable</code></td>
<td>Required By default, a login user uses the settings of the <code>screen-length</code>. The default settings of the <code>screen-length</code> command are: multiple-screen display is enabled and up to 24 lines are displayed on the next screen. This command is executed in user view, and takes effect for the current user only. When the user re-logs into the switch, the default configuration is restored.</td>
</tr>
</tbody>
</table>

Filtering output information

Use regular expressions in `display` commands to filter output information.

The following methods are available for filtering output information:

- Enter the `begin`, `exclude`, or `include` keyword plus a regular expression in the `display` to filter the output information.
- When the system displays the output information in multiple screens, use the slash (`/`), hyphen (`-`), or plus (`+`) with a regular expression to filter subsequent output information. The slash character (`/`) equals the keyword `begin`, the character hyphen (`-`) equals the keyword `exclude`, and the character plus (`+`) 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. It supports the following special characters:

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>^string</td>
<td>Starting sign. string appears only at the beginning of a line.</td>
<td>For example, regular expression “^user” only matches a string beginning with “user,” not “Auser.”</td>
</tr>
<tr>
<td>string$</td>
<td>Ending sign. string appears only at the end of a line.</td>
<td>For example, regular expression “user$” only matches a string ending with “user,” not “userA.”</td>
</tr>
<tr>
<td>.</td>
<td>Matches any single character, such as a single character, a special character, and a blank.</td>
<td>For example, “.s” matches “as” and “bs.”</td>
</tr>
<tr>
<td></td>
<td>Matches the preceding character or character group zero or multiple times.</td>
<td>For example, “zo*” matches “z” and “zoo”; “(zo)*” matches “zo” and “zozo.”</td>
</tr>
<tr>
<td>+</td>
<td>Matches the preceding character or character group one or multiple times</td>
<td>For example, “zo+” matches “zo” and “zoo,” but not “z.”</td>
</tr>
<tr>
<td></td>
<td>Matches the preceding or succeeding character string</td>
<td>For example, “def</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td>For example, “a_b” matches “a b” or “a(b”; “<em>ab” only matches a line starting with “ab”; “ab</em>” only matches a line ending with “ab.”</td>
</tr>
<tr>
<td></td>
<td>It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].</td>
<td>For example, “1-9” means 1 to 9 (inclusive); “a-h” means a to h (inclusive).</td>
</tr>
<tr>
<td></td>
<td>Matches a single character contained within the brackets.</td>
<td>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}.</td>
</tr>
<tr>
<td></td>
<td>A character group. It is usually used with “+” or “*.”</td>
<td>For example, (123A) means a character group “123A”; “408(12)+” matches 40812 or 408121212. But it does not match 408.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>Character</td>
<td>Meaning</td>
<td>Remarks</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>[^]</td>
<td>Matches a single character not contained within the brackets.</td>
<td>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 these three characters only. For example, [^16A] matches “abc” and “m16,” but not 1, 16, or 16A.</td>
</tr>
<tr>
<td>&lt;string&gt;</td>
<td>Matches a character string starting with string.</td>
<td>For example, “&lt;do” matches word “domain” and string “doa.”</td>
</tr>
<tr>
<td>string&gt;</td>
<td>Matches a character string ending with string.</td>
<td>For example, “do&gt;” matches word “undo” and string “abcdo.”</td>
</tr>
<tr>
<td>\bcharacter2</td>
<td>Matches character1character2. character1 can be any character except number, letter or underline, and \b equals [^A-Za-z0-9_].</td>
<td>For example, “\ba” matches “-a” with “-” being character1, and “a” being character2, but it does not match “2a” or “ba.”</td>
</tr>
<tr>
<td>\Bcharacter</td>
<td>Matches a string containing character and no space is allowed before character.</td>
<td>For example, “\Bt” matches “t” in “install,” but not “t” in “big top.”</td>
</tr>
<tr>
<td>character1\w</td>
<td>Matches character1character2. character2 must be a number, letter, or underline, and \w equals [^A-Za-z0-9_].</td>
<td>For example, “v\w” matches “vlan,” with “v” being character1, and “l” being character2. \w also matches “service,” with “i” being character2.</td>
</tr>
<tr>
<td>\W</td>
<td>Equals \b.</td>
<td>For example, “\Wa” matches “-a,” with “-” being character1, and “a” being character2, but does not match “2a” or “ba.”</td>
</tr>
<tr>
<td>\</td>
<td>Escape character. If a special character listed in this table follows , the specific meaning of the character is removed.</td>
<td>For example, “\” matches a string containing “,” “\” matches a string containing “^,” and “\b” matches a string containing “\b.”</td>
</tr>
</tbody>
</table>
Example of filtering output information

1. Example of using the `begin` keyword

# Display the configuration from the line containing “user-interface” to the last line in the current configuration (the output information depends on the current configuration).

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

2. Example of using the `exclude` keyword

# Display the non-direct routes in the routing table (the output depends on the current configuration).

```bash
<Sysname> display ip routing-table | exclude Direct
```

3. Example of using the `include` keyword

# Display the route entries that contain Vlan in the routing table (the output depends on the current configuration).

```bash
<Sysname> display ip routing-table | include Vlan
```

Configuring user privilege and command levels

To avoid unauthorized access, the switch defines user privilege levels and command levels. User privilege levels correspond to command levels. When a user at a specific privilege level logs in, the user can only use 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 2 describes the command levels.

<table>
<thead>
<tr>
<th>Level</th>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Visit</td>
<td>Involves commands for network diagnosis and 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.</td>
</tr>
</tbody>
</table>

Table 2 Default command levels
<table>
<thead>
<tr>
<th>Level</th>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Monitor</td>
<td>Involves commands for system maintenance and service fault diagnosis. Commands at this level are not allowed to be saved after being configured. After the switch is restarted, the commands at this level are restored to the default settings. Commands at this level include <code>debugging</code>, <code>terminal</code>, <code>refresh</code>, <code>reset</code>, and <code>send</code>.</td>
</tr>
<tr>
<td>2</td>
<td>System</td>
<td>Involves service configuration commands, such as 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 the manage level.</td>
</tr>
<tr>
<td>3</td>
<td>Manage</td>
<td>Involves 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).</td>
</tr>
</tbody>
</table>

**Configuring a user privilege level**

A user privilege level can be configured by using AAA authentication parameters or under a user interface.

**Configuring user privilege level by using AAA authentication parameters**

If the authentication mode of a user interface is scheme, the user privilege level of users logging into the user interface is specified in AAA authentication configuration.

To configure the user privilege level by using AAA authentication parameters:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td><code>system-view</code></td>
<td>—</td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>`user-interface { first-num1 [ last-num1 ]</td>
<td>{ aux</td>
</tr>
<tr>
<td>Specify the scheme authentication mode</td>
<td><code>authentication-mode scheme</code></td>
<td>Required By default, the authentication mode for VTY users is <code>password</code>, and no authentication is needed for AUX login user.</td>
</tr>
<tr>
<td>Return to system view</td>
<td><code>quit</code></td>
<td>—</td>
</tr>
<tr>
<td>Configure the authentication mode for SSH users as <code>password</code></td>
<td>For more information about SSH, see <code>Security Configuration Guide</code>. Required if users use SSH to log in, and username and password are needed at authentication</td>
<td></td>
</tr>
<tr>
<td>Configure the user privilege level by using AAA authentication</td>
<td>• Use <code>local-user</code> to create a local user and enter local user view. • Use <code>level</code> keyword in the <code>authorization-attribute</code> to configure the user privilege level. Use either approach • For local authentication, if you do not configure the user privilege level, the user privilege level is 0.</td>
<td></td>
</tr>
</tbody>
</table>
Using remote authentication (RADIUS, HWTACACS, and LDAP authentications)

Configure the user privilege level on the authentication server

• 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.

### Example of configuring a user privilege level by using AAA authentication parameters

```
# You are required to authenticate the users that Telnet to the switch through VTY 1, verify their username and password, and specify the user privilege level as 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 cipher 12345678
[Sysname-luser-test] service-type telnet

When users Telnet to the switch through VTY 1, they must enter username test and password 12345678. After passing the authentication, the users can only use the commands of level 0. If the users want to use commands of levels 0, 1, 2 and 3, the following configuration is required:

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

### Configuring the user privilege level under a user interface

- If the authentication mode of a user interface is scheme, and SSH publickey authentication type (only a username is needed for this authentication type) is adopted, the user privilege level of users logging into the user interface is the user interface level.

- If the authentication mode of a user interface is none or password, the user privilege level of users logging into the user interface is the user interface level.

### To configure the user privilege level under a user interface (SSH publickey authentication type):

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the authentication type for SSH users as publickey</td>
<td>authentification-mode scheme</td>
<td>Required if the SSH login mode is adopted, and only username is needed during authentication. After the configuration, the authentication mode of the corresponding user interface must be set to scheme.</td>
</tr>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>user-interface { first-num1</td>
<td>last-num1 }</td>
</tr>
<tr>
<td>Enter user interface view</td>
<td>vty first-num2</td>
<td>—</td>
</tr>
<tr>
<td>Configure the authentication mode for any user who uses the current user interface to log in to the switch</td>
<td>authentication-mode scheme</td>
<td>Required By default, the authentication mode for VTY users is password, and no authentication is needed for AUX users.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Configure the privilege level for users that log in through the</td>
<td>user privilege level level</td>
<td>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 the VTY interfaces is 0.</td>
</tr>
<tr>
<td>current user interface</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| To configure the user privilege level under a user interface (none or password authentication mode): |
|-----------------------------------------------------------------------------------------------|-------------------------------------------------|
| Step                                                                                         | Command                                      | Remarks                                                                 |
| Enter system view                                                                           | system-view                                   | —                                                                       |
| Enter user interface view                                                                   | user-interface { first-num1 | { last-num1 } | { aux | vty } | first-num2 | { last-num2 } } | — |
| Configure the authentication mode for any user who uses the current user interface to log in to the switch | authentication-mode { none | password } | Optional By default, the authentication mode for VTY user interfaces is password, and no authentication is needed for AUX login user. |
| 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 the VTY interfaces is 0. |

**Example of configuring a user privilege level under a user interface**

```
# Authenticate users logged in to the switch through Telnet, verify their password, and specify their user privilege level as 2.
<Sysname> system-view
<Sysname> user-interface vty 0 15
<Sysname-ui-vty0-15> authentication-mode password
<Sysname-ui-vty0-15> set authentication password cipher 123
<Sysname-ui-vty0-15> user privilege level 2
```

By default, Telnet users can use the commands of level 0 after passing authentication. After the configuration above is completed, when users log in to the switch through Telnet, they must enter password 123, and then they can use commands of levels 0, 1, and 2.

**NOTE:**

- For more information about user interfaces, see “Logging in to the switch configuration.” For more information about `user-interface`, `authentication-mode`, and `user privilege level`, see “Logging in to the switch commands.”
- For more information about AAA authentication, see Security Configuration Guide. For more information about `local-user` and `authorization-attribute`, see Security Command Reference.
- For more information about SSH, see Security Configuration Guide.
Switching user privilege level

Users can switch to a different user privilege level temporarily without logging out and terminating the current connection. After the privilege level switch, users can continue to configure the switch without the must re-log in, but the commands that they can execute have changed. For example, if the current user privilege level is 3, the user can configure system parameters. After switching to user privilege level 0, the user can only execute simple commands, like ping and tracert, and only 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 to the switch by using a lower privilege level and view switch operating parameters, and when they have to maintain the switch, they can switch to a higher level temporarily.
- If the administrators need to leave for a while or ask someone else to manage the switch temporarily, they can switch to a lower privilege level before they leave to restrict the operation by others.

Setting the authentication mode for user privilege level switch

⚠️ CAUTION:

- If no user privilege level is specified when you configure the password for switching the user privilege level with super password, the user privilege level defaults to 3.
- If you specify the simple keyword, the password is saved in the configuration file in plain text, which is easy to be stolen. If you specify the cipher keyword, the password is saved in the configuration file in cipher text, which is safer.
- If the user logs in from the AUX user interface (the console port), the user can switch the privilege level to a higher level even if the authentication mode is local and no password for user privilege level switch is configured.

- 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 the password (if any) to switch to a higher privilege level. The authentication falls into one of the following four categories:

<table>
<thead>
<tr>
<th>Authentication mode</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local</td>
<td>Local password authentication</td>
<td>The switch authenticates a user by using the privilege level switch password entered by the user. When this mode is applied, you must set the password for privilege level switch with super password.</td>
</tr>
</tbody>
</table>
| scheme              | Remote AAA authentication through HWTACACS or RADIUS | The switch sends the username and password for privilege level switch to the HWTACACS or RADIUS server for remote authentication. When this mode is applied, you must perform the following configurations:  
  - Configure HWTACACS or RADIUS scheme and reference the created scheme in the ISP domain. For more information, see Security Configuration Guide.  
  - Create the corresponding user and configure password on the HWTACACS or RADIUS server. |
### Authentication mode

<table>
<thead>
<tr>
<th>Mode</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>local scheme</strong></td>
<td>Performs the local password authentication first and then the remote AAA authentication</td>
<td>The switch authenticates a user by using the local password first. If no local password is set, the privilege level is switched directly for the users logged in from the Console port, and remote AAA authentication is performed on the users logged in from VTY user interfaces.</td>
</tr>
<tr>
<td><strong>scheme local</strong></td>
<td>Performs remote AAA authentication first and then the local password authentication</td>
<td>AAA authentication is performed first, and if the remote HWTACACS or RADIUS server does not respond or AAA configuration on the switch is invalid, the local password authentication is performed.</td>
</tr>
</tbody>
</table>

### To set the authentication mode for user privilege level switch:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Set the authentication mode for</td>
<td>super authentication-mode { local</td>
<td>Optional</td>
</tr>
<tr>
<td>user privilege level switch</td>
<td>scheme } *</td>
<td>local by default.</td>
</tr>
<tr>
<td>Configure the password for user</td>
<td>super password { level user-level</td>
<td>Required if the authentication</td>
</tr>
<tr>
<td>privilege level switch</td>
<td>simple</td>
<td>cipher } password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no privilege level switch password is configured.</td>
</tr>
</tbody>
</table>

### Switching the user privilege level

**CAUTION:**
- When the authentication mode is set to **local**, configure the local password before switching to a higher user privilege level.
- When the authentication mode is set to **scheme**, configure AAA related parameters before switching to a higher user privilege level.
- The privilege level switch fails after three consecutive unsuccessful password attempts.
- For more information about user interface authentication, see “Logging in to the switch configuration.”

Follow the step to switch the user privilege level:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch the user privilege level</td>
<td>super [ level ]</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When logging in to the switch, a user has a user privilege level, which depends on user interface or authentication user level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available in user view.</td>
</tr>
</tbody>
</table>
When you switch the user privilege level, the information you must provide varies with combinations of the user interface authentication mode and the super authentication mode.

**Table 3 Information input for user privilege level switch**

<table>
<thead>
<tr>
<th>User interface authentication mode</th>
<th>User privilege level switch authentication mode</th>
<th>Information entered for the first authentication mode</th>
<th>Information entered after the authentication mode changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>none/password</td>
<td>local</td>
<td>Local user privilege level switch password (configured on the switch)</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>local scheme</td>
<td>Local user privilege level switch password</td>
<td>Username and password for privilege level switch (configured on the AAA server)</td>
</tr>
<tr>
<td></td>
<td>scheme</td>
<td>Username and password for privilege level switch</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>scheme local</td>
<td>Username and password for privilege level switch</td>
<td>Local user privilege level switch password</td>
</tr>
<tr>
<td></td>
<td>local</td>
<td>Local user privilege level switch password</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>local scheme</td>
<td>Local user privilege level switch password</td>
<td>Password for privilege level switch (configured on the AAA server). The system uses the username used for logging in as the privilege level switch username.</td>
</tr>
<tr>
<td></td>
<td>scheme</td>
<td>Password for privilege level switch (configured on the AAA server). The system uses the username used for logging in as the privilege level switch username.</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>scheme local</td>
<td>Password for privilege level switch (configured on the AAA server). The system uses the username used for logging in as the privilege level switch username.</td>
<td>Local user privilege level switch password</td>
</tr>
</tbody>
</table>

**Modifying the level of a command**

⚠️ **CAUTION:**

HP recommends using the default command level or modify the command level under the guidance of professional staff. An improper change of the command level may bring inconvenience to your maintenance and operation, or even potential security problems.

All commands in a view default to different levels. The administrator can change the default level of a command to a lower level or a higher level as needed.
To modify the command level:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Configure the command level in a specified view</td>
<td>command-privilege level level view</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>view command</td>
<td>See Table 1 for the default settings.</td>
</tr>
</tbody>
</table>

### Saving the current configuration

On the device, enter 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, such as **display** commands, which display specified information, and **reset** commands, which clear specified information. The one-time commands executed are never saved.

### Displaying and maintaining CLI

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display defined command aliases and the corresponding commands.</td>
<td>display command-alias [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display the clipboard information.</td>
<td>display clipboard [</td>
<td>{ begin</td>
</tr>
</tbody>
</table>
Login methods

Log in to the switch by using the following methods.

Table 4 Login methods

<table>
<thead>
<tr>
<th>Login method</th>
<th>Default state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging in through the console port</td>
<td>By default, log in to a device through the console port, the authentication mode is None (no username or password required), and the user privilege level is 3.</td>
</tr>
</tbody>
</table>
| Logging in through Telnet         | By default, you cannot log in to a device through Telnet. To do so, log in to the device through the console port, and complete the following configuration:  
  • Enable the Telnet function.  
  • Configure the IP address of the VLAN interface, and make sure that your device and the Telnet client can reach each other (by default, the device does not have an IP address.).  
  • Configure the authentication mode of VTY login users (password by default).  
  • Configure the user privilege level of VTY login users (0 by default). |
| CLI login                         | By default, you cannot log in to a device through SSH. To do so, log in to the device through the console port, and complete the following configuration:  
  • Enable the SSH function and configure SSH attributes.  
  • Configure the IP address of the VLAN interface, and make sure that your device and the SSH client can reach each other (by default, your device does not have an IP address.).  
  • Configure the authentication mode of VTY login users as scheme (password by default).  
  • Configure the user privilege level of VTY login users (0 by default). |
| Logging in through SSH            | By default, log in to a device through modems. The default user privilege level of modem login users is 3. |
| Web login                         | By default, you cannot log in to a device through web. To do so, log in to the device through the console port, and complete the following configuration:  
  • Configure the IP address of the VLAN interface (by default, your device does not have an IP address.).  
  • Configure a username and password for web login (not configured by default).  
  • Configure the user privilege level for web login (not configured by default).  
  • Configure the Telnet service type for web login (not configured by default). |
<table>
<thead>
<tr>
<th>Login method</th>
<th>Default state</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMS login</td>
<td>By default, you cannot log in to a device through a network management station (NMS). To do so, log in to the device through the console port, and complete the following configuration:</td>
</tr>
<tr>
<td></td>
<td>• Configure the IP address of the VLAN interface, and make sure the device and the NMS can reach each other (by default, your device does not have an IP address.).</td>
</tr>
<tr>
<td></td>
<td>• Configure SNMP basic parameters.</td>
</tr>
</tbody>
</table>

**Users and user interfaces**

User interface, also called "line," allows you to manage and monitor sessions between the terminal and device when you log in to the device through the console port directly, or through Telnet or SSH.

One user interface corresponds to one user interface view where you can configure a set of parameters, such as whether to authenticate users at login, whether to redirect the requests to another device, and the user privilege level after login. When the user logs in through a user interface, the parameters set for the user interface apply.

The system supports the following CLI configuration methods:

- Local configuration via the console port
- Local/Remote configuration through Telnet or SSH

The methods correspond to the following user interfaces.

- AUX user interface: Used to manage and monitor users that log in via the Console port. The type of the Console port is EIA/TIA-232 DCE.
- VTY (virtual type terminal) user interface: Used to manage and monitor users that log in via VTY. A VTY port used for Telnet or SSH access.

Only one user can use a user interface at a time. The configuration made in a user interface view applies to any login user. For example, if user A uses the console port to log in, the configuration in the AUX user interface view applies to user A; if user A logs in through VTY 1, the configuration in VTY 1 user interface view applies to user A.

A device can be equipped with one AUX user interface and 16 VTY user interfaces. These user interfaces do not associate with specific users. When a user initiates a connection request, the system automatically assigns an idle user interface with the smallest number to the user based on the login method. During the login, the configuration in the user interface view takes effect. The user interface varies depending on the login method and the login time.
Numbering user interfaces

User interfaces can be numbered by using absolute numbering or relative numbering.

Absolute numbering

Absolute numbering identifies a user interface or a group of different types of user interfaces. The specified user interfaces are numbered from number 0 with a step of 1 and in the sequence of AUX, and VTY user interfaces. Use `display user-interface` command without any parameters to view supported user interfaces and their absolute numbers.

Relative numbering

Relative numbering allows you to specify a user interface or a group of user interfaces of a specific type. The number format is "user interface type + number." The following rules of relative numbering apply:

- AUX user interfaces are numbered from 0 in the ascending order, with a step of 1.
- VTY user interfaces are numbered from 0 in the ascending order, with a step of 1.
The CLI enables you to interact with a device by typing text commands. At the CLI, instruct your device to perform a given task by typing a text command and then pressing Enter to submit it to your device. Compared with the graphical user interface (GUI), where you can use a mouse to perform configuration, the CLI allows you to enter more information in one command line.

Log in to the device at the CLI through the console port, Telnet, SSH, or modem.

- By default, log in to a device through the console port without any authentication, which introduces security problems.
- By default, you cannot log in to a device through Telnet, SSH, so you cannot remotely manage and maintain the device.

Therefore, you must perform configurations to increase device security and manageability.

Logging in through the console port

Logging in through the console port is the most common login method, and is also the first step to configure other login methods.

By default, log in to a device through its console port only. After logging in to the device through the console port, configure other login methods.

Configuration requirements

<table>
<thead>
<tr>
<th>Object</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>No configuration requirement</td>
</tr>
<tr>
<td>Terminal</td>
<td>Run the hyper terminal program.</td>
</tr>
<tr>
<td></td>
<td>Configure the hyper terminal attributes.</td>
</tr>
</tbody>
</table>

The port properties of the hyper terminal must be the same as the default settings of the console port shown in the following table.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bits per second</td>
<td>9,600 bps</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
</tbody>
</table>
Login procedure

⚠️ WARNING!
Identify interfaces to avoid connection errors.

1. As shown in Figure 2, use the console cable shipped with the device to connect the PC and the device. Plug the DB-9 connector of the console cable into the serial port of the PC, and plug the RJ-45 connector into the console port of your device.

**Figure 2 Connect the device and PC through a console cable**

![Console cable connection](image)

The serial port of a PC does not support hot-swap. Do not plug or unplug the console cable into or from the PC when your device is powered on.

- To connect the PC to the device, first plug the DB-9 connector of the console cable into the PC, and then plug the RJ-45 connector of the console cable into your device.
- To disconnect the PC from the device, first unplug the RJ-45 connector and then the DB-9 connector.

2. Launch a terminal emulation program (such as HyperTerminal in Windows XP/Windows 2000). The following takes the HyperTerminal of Windows XP as an example. Select a serial port to be connected to the device, and set terminal parameters as follows: set **Bits per second** to **9600**, **Data bits** to **8**, **Parity** to **None**, **Stop bits** to **1**, and **Flow control** to **None**, as shown in Figure 3 through Figure 5.

**NOTE:**
On Windows 2003 Server operating system, you must add the HyperTerminal program first, and then log in to and manage the device as described in this document. On Windows 2008 Server, Windows 7, Windows Vista, or some other operating system, you must 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.

**Figure 3 Connection description**

![Connection Description](image)
Figure 4 Specify the serial port used to establish the connection

Figure 5 Set the properties of the serial port
3. Turn on the device. You are prompted to press Enter if the device successfully completes the power-on self-test (POST). A prompt such as <HP> appears after you press Enter, as shown in Figure 6.

Figure 6 Configuration page

Figure 6 Configuration page

Press ENTER to get started.

<HP>

4. Execute commands to configure the device or check the running status of the device. To get help, enter ?.

Console login authentication modes

The following authentication modes are available for console port login: none, password, and scheme.

- **none**—Requires no username and password at the next login through the console port. This mode is insecure.
- **password**—Requires password authentication at the next login through the console port. Keep your password.
- **scheme**—Requires username and password authentication at the next login through the console port. Authentication falls into local authentication and remote authentication. To use local authentication, configure a local user and related parameters. To use remote authentication, configure the username and password on the remote authentication server. For more information about authentication modes and parameters, see Security Configuration Guide. Keep your username and password.
The following table lists console port login configurations for different authentication modes:

<table>
<thead>
<tr>
<th>Authentication mode</th>
<th>Configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Configure not to authenticate users.</td>
<td>For more information, see “Configuring none authentication for console login.”</td>
</tr>
<tr>
<td>Password</td>
<td>Configure the device to authenticate users by using the local password. Set the local password.</td>
<td>For more information, see “Configuring password authentication for console login.”</td>
</tr>
<tr>
<td>Scheme</td>
<td>Select an authentication scheme.</td>
<td>Configure the authentication scheme.</td>
</tr>
<tr>
<td></td>
<td>Configure RADIUS/HWTACACS scheme.</td>
<td>Configure AAA scheme used by the domain.</td>
</tr>
<tr>
<td></td>
<td>Configure AAA scheme used by the domain.</td>
<td>For more information, see “Configuring scheme authentication for console login.”</td>
</tr>
<tr>
<td></td>
<td>Configure username and password on the AAA server.</td>
<td>Configure authentication username and password.</td>
</tr>
<tr>
<td></td>
<td>Configure AAA scheme used by the domain as local.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**
A newly configured authentication mode does not take effect unless you exit and enter the CLI again.

**Configuring none authentication for console login**

**Prerequisites**

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”
**Procedure**

To configure none authentication for console login:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Enter AUX user interface view.</td>
<td><code>user-interface aux first-number [ last-number ]</code></td>
</tr>
<tr>
<td>3.</td>
<td>Specify the none authentication mode.</td>
<td><code>authentication-mode none</code></td>
</tr>
<tr>
<td>4.</td>
<td>Configure common settings for AUX user interface view.</td>
<td>—</td>
</tr>
</tbody>
</table>

After the configuration, the next time you log in to the device through the console port, you are prompted to press enter. A prompt such as `<HP>` appears after you press **Enter**, as shown in Figure 7.

**Figure 7 Configuration page**

User interface aux0 is available.

Press ENTER to get started.

<HP>_

**Configuring password authentication for console login**

**Prerequisites**

You have logged in to the device.
By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”

Procedure

To configure password authentication for console login:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Enter AUX user interface view.</td>
<td>user-interface aux first-number [ last-number ] —</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the authentication mode as local password authentication.</td>
<td>authentication-mode password Required. By default, log in to the device through the console port without authentication and have user privilege level 3 after login.</td>
</tr>
<tr>
<td>4.</td>
<td>Set the local password.</td>
<td>set authentication password { cipher</td>
</tr>
<tr>
<td>5.</td>
<td>Configure common settings for AUX user interface view.</td>
<td>— Optional. See “Configuring common settings for console login (optional).”</td>
</tr>
</tbody>
</table>

When you log in to the device through the console port after the configuration, you are prompted to enter a login password. A prompt such as <HP> appears after you enter the password and press Enter, as shown in Figure 8.

Figure 8 Configuration page

User interface aux0 is available.

Press ENTER to get started.
Login authentication

Password: [red]HP"
### Configuring scheme authentication for console login

#### Prerequisites

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”

#### Procedure

To configure scheme authentication for console login:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Enter AUX user interface view.</td>
<td><strong>user-interface aux</strong> first-number [last-number]</td>
</tr>
<tr>
<td></td>
<td>Specify scheme authentication mode.</td>
<td><strong>authentication-mode scheme</strong></td>
</tr>
<tr>
<td>4.</td>
<td>Enable command authorization.</td>
<td><strong>command authorization</strong></td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
- 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 helps control and monitor user operations 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.  
- Configure the AAA accounting server before enabling command accounting.  |
| 6.   | **quit** | Return to system view. |
| 7.   | **domain domain-name** | Enter ISP domain view. Optional.  
By default, the AAA scheme is **local**.  
If you specify the local AAA scheme, you must perform local user configuration. If you specify an existing scheme by providing the `radius-scheme-name` argument, perform the following configuration as well:  
- For RADIUS and HWTACACS configuration, see Security Configuration Guide.  
- Configure the username and password on the AAA server. (For more information about AAA, see Security Configuration Guide.)  |
| 8.   | **local-user user-name** | Create a local user and enter local user view. Required.  
By default, no local user exists.  |
| 9.   | **password { cipher | simple }** | Set the authentication password for the local user. Required.  |
| 10.  | **authorization-attribute level** | Specifies the command level of the local user. Optional.  
By default, the command level is 0.  |
| 11.  | **service-type terminal** | Specify the service type for the local user. Required.  
By default, no service type is specified.  |
| 12.  | — | Configure common settings for AUX user interface view. Optional.  
See “Configuring common settings for console login (optional).”  |
After you enable command authorization, you must perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters. For more information about AAA, see Security Configuration Guide.
- Reference the created HWTACACS scheme in the ISP domain. For more information about AAA, see Security Configuration Guide.

After you enable command accounting, you must perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the accounting server and other accounting parameters. For more information about AAA, see Security Configuration Guide.
- Reference the created HWTACACS scheme in the ISP domain. For more information about AAA, see Security Configuration Guide.

When users adopt the scheme mode to log in to the device, the level of the commands that the users can access depends on the user privilege level defined in the AAA scheme.

- When the AAA scheme is local, the user privilege level is defined by the authorization-attribute level.
- When the AAA scheme is RADIUS or HWTACACS, the user privilege level is configured on the RADIUS or HWTACACS server.
- For more information about AAA, RADIUS, and HWTACACS, see Security Configuration Guide.

When you log in to the device through the console port after the configuration, you are prompted to enter a login username and password. A prompt such as <HP> appears after you enter the password and username and press Enter, as shown in Figure 9.

Figure 9 Configuration page

User interface aux0 is available.

Please press ENTER.

Login authentication

Username: admin
Password: 
<HP>
**Configuring common settings for console login (optional)**

⚠️ **CAUTION:**

The common settings configured for console login take effect immediately. If you configure the common settings after you log in through the console port, the current connection may be interrupted, so you should use another login method. After you configure common settings for console login, you must modify the settings on the terminal to make them consistent with those on the device.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Enable display of copyright information.</td>
<td>copyright-info enable Optional. Enabled by default.</td>
</tr>
<tr>
<td>3.</td>
<td>Enter AUX user interface view.</td>
<td>user-interface aux first-number [ last-number ] —</td>
</tr>
<tr>
<td>4.</td>
<td>Configure baud rate.</td>
<td>speed speed-value Optional. By default, the transmission rate is 9600 bps. Transmission rate is the number of bits that the device transmits to the terminal per second.</td>
</tr>
<tr>
<td></td>
<td>Configure parity check mode.</td>
<td>parity { even</td>
</tr>
<tr>
<td></td>
<td>Configure stop bits.</td>
<td>stopbits { 1</td>
</tr>
<tr>
<td></td>
<td>Configure data bits.</td>
<td>databits { 5</td>
</tr>
<tr>
<td></td>
<td>Define shortcut key for enabling a terminal session.</td>
<td>activation-key character Optional. By default, press Enter to enable a terminal session.</td>
</tr>
<tr>
<td></td>
<td>Define shortcut key for terminating tasks.</td>
<td>escape-key { default</td>
</tr>
</tbody>
</table>
### Step Command Remarks

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure flow control mode.</td>
<td>`flow-control { hardware</td>
<td>none</td>
</tr>
<tr>
<td>Configure type of terminal display</td>
<td>`terminal type { ansi</td>
<td>vt100 }`</td>
</tr>
<tr>
<td>Configure user privilege level for login users</td>
<td><code>user privilege level level</code></td>
<td>Optional By default, the default command level is 3 for the AUX user interface.</td>
</tr>
<tr>
<td>Set the maximum number of lines on the next screen.</td>
<td><code>screen-length screen-length</code></td>
<td>Optional By default, the next screen displays 24 lines. A value of 0 disables the function.</td>
</tr>
<tr>
<td>Set the size of history command buffer</td>
<td><code>history-command max-size value</code></td>
<td>Optional By default, the buffer saves 10 history commands at most.</td>
</tr>
<tr>
<td>Set the idle-timeout timer</td>
<td><code>idle-timeout minutes [ seconds ]</code></td>
<td>Optional The default idle-timeout is 10 minutes. The system automatically terminates the user’s connection if no information interaction occurs between the device and the user within the idle-timeout time. Setting idle-timeout to 0 disables the timer.</td>
</tr>
</tbody>
</table>

### Loggin in through Telnet

The device supports Telnet. Telnet to the device to remotely manage and maintain it, as shown in Figure 10.

#### Figure 10 Telnet login

![Telnet login diagram](image)
The following table shows the configuration requirements of Telnet login.

<table>
<thead>
<tr>
<th>Object</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet server</td>
<td>Configure the IP address of the VLAN interface, and make sure the Telnet server and client can reach each other.</td>
</tr>
<tr>
<td></td>
<td>Configure the authentication mode and other settings.</td>
</tr>
<tr>
<td>Telnet client</td>
<td>Run the Telnet client program.</td>
</tr>
<tr>
<td></td>
<td>Obtain the IP address of the VLAN interface on the server.</td>
</tr>
</tbody>
</table>

By default, the device is enabled with the Telnet server and client functions.

- On a device that serves as the Telnet client, log in to a Telnet server to perform operations on the server.
- On a device that serves as the Telnet server, configure the authentication mode and user privilege level for Telnet users. By default, you cannot log in to the device through Telnet. Before Telnet to the device, you must log in to the device through the console port, enable Telnet server, and configure the authentication mode, user privilege level, and common settings.

**Telnet login authentication modes**

Three authentication modes are available for Telnet login: none, password, and scheme.

- **none**—Requires no username and password at the next login through Telnet. This mode is insecure.
- **password**—Requires password authentication at the next login through Telnet. Keep your password. If you lose your password, log in to the device through the console port to view or modify the password.
- **scheme**—Requires username and password authentication at the next login through Telnet. Authentication falls into local authentication and remote authentication. To use local authentication, configure a local user and related parameters. To use remote authentication, configure the username and password on the remote authentication server. For more information about authentication modes and parameters, see Security Configuration Guide. Keep your username and password. If you lose your local authentication password, log in to the device through the console port to view or modify the password. If you lose your remote authentication password, contact the administrator.

The following table lists Telnet login configurations for different authentication modes.

<table>
<thead>
<tr>
<th>Authentication mode</th>
<th>Configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Configure not to authenticate users.</td>
<td>For more information, see “Configuring none authentication for Telnet login.”</td>
</tr>
<tr>
<td>Password</td>
<td>Configure the device to authenticate users by using the local password.</td>
<td>For more information, see “Configuring password authentication for Telnet login.”</td>
</tr>
</tbody>
</table>
### Configuring none authentication for Telnet login

**Prerequisites**

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”

**Procedure**

To configure none authentication for Telnet login:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td>telnet server enable</td>
<td>Required. By default, the Telnet service is disabled.</td>
</tr>
<tr>
<td>3.</td>
<td>user-interface vty first-number [ last-number ]</td>
<td>—</td>
</tr>
<tr>
<td>4.</td>
<td>authentication-mode none</td>
<td>Required. By default, authentication mode for VTY user interfaces is password.</td>
</tr>
</tbody>
</table>
5. Configure the command level for login users on the current user interfaces.  

   `user privilege level level`

   Required. By default, the default command level is 0 for VTY user interfaces.

6. Configure common settings for VTY user interfaces. — Optional. See “Configuring common settings for VTY user interfaces (optional).”

When you log in to the device through Telnet again:

- You enter the VTY user interface, as shown in Figure 11.
- If “All user interfaces are used, please try later!” is displayed, it means the current login users exceed the maximum number. Please try later.

Figure 11 Configuration page
Configuring password authentication for Telnet login

Prerequisites

You have logged into the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”

Procedure

To configure password authentication for Telnet login:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable Telnet.</td>
<td>telnet server enable</td>
</tr>
<tr>
<td>3.</td>
<td>Enter one or multiple VTY user interface views.</td>
<td>user-interface vty first-number [ last-number ]</td>
</tr>
<tr>
<td>4.</td>
<td>Specify the password authentication mode.</td>
<td>authentication-mode password</td>
</tr>
<tr>
<td>5.</td>
<td>Set the local password.</td>
<td>set authentication password { cipher</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the user privilege level for login users.</td>
<td>user privilege level level</td>
</tr>
<tr>
<td>7.</td>
<td>Configure common settings for VTY user interfaces.</td>
<td>—</td>
</tr>
</tbody>
</table>

When you log in to the device through Telnet again:

- You are required to enter the login password. A prompt such as <HP> appears after you enter the correct password and press Enter, as shown in Figure 12.
- If “All user interfaces are used, please try later!” is displayed, it means the number of current concurrent login users exceed the maximum. Please try later.
## Configuring scheme authentication for Telnet login

### Prerequisites

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>-</td>
</tr>
<tr>
<td>2.</td>
<td>telnet server enable</td>
<td>Required. By default, the Telnet service is disabled.</td>
</tr>
<tr>
<td>3.</td>
<td>user-interface vty</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>first-number</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>[ last-number ]</td>
<td>-</td>
</tr>
<tr>
<td>4.</td>
<td>authentication-mode</td>
<td>Required. Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme.</td>
</tr>
<tr>
<td></td>
<td>scheme</td>
<td>By default, local authentication is adopted.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>5.</td>
<td>Enable command authorization.</td>
<td><strong>command authorization</strong>&lt;br&gt;Optional.&lt;br&gt;• By default, command authorization is not enabled.&lt;br&gt;• By default, the command level depends on the user privilege level. A user is authorized a command level not higher than the user privilege level. With command authorization enabled, the command level for a login user is determined by both the user privilege level and AAA authorization. If a user executes a command of the corresponding command level, the authorization server checks whether the command is authorized. If it is, the command can be executed.&lt;br&gt;• Before enabling command authorization, configure the AAA authorization server. After you enable command authorization, only commands authorized by the AAA authorization server can be executed.</td>
</tr>
<tr>
<td>6.</td>
<td>Enable command accounting.</td>
<td><strong>command accounting</strong>&lt;br&gt;Optional.&lt;br&gt;• By default, command accounting is disabled. The accounting server does not record the commands executed by users.&lt;br&gt;• Command accounting allows the HWTACACS server to record all executed commands that are supported by the device, regardless of the command execution result. This helps control and monitor user operations 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.&lt;br&gt;• Configure the AAA accounting server before enabling command accounting.</td>
</tr>
<tr>
<td>7.</td>
<td>Exit to system view.</td>
<td><strong>quit</strong>&lt;br&gt;Enter default ISP domain view.</td>
</tr>
</tbody>
</table>
| 8.   | Configure authentication mode. | Specify AAA scheme to be applied to the domain.<br> authentication default { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }<br>Exit to system view. **quit**<br>Optional.<br>By default, the AAA scheme is **local**. If you specify the local AAA scheme, perform the configuration concerning local user as well. If you specify an existing scheme by providing the *radius-scheme-name* argument, perform the following configuration as well:<br>• For RADIUS and HWTACACS configuration, see Security Configuration Guide.<br>• Configure the username and password on the AAA server. (For more information, see Security Configuration Guide.)
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.</td>
<td>Create local user and enter local user view. <strong>local-user</strong> <strong>user-name</strong></td>
<td>By default, no local user exists.</td>
</tr>
<tr>
<td>10.</td>
<td>Set local password. <strong>password</strong> { <strong>cipher</strong></td>
<td>Required. <strong>simple</strong> } <strong>password</strong></td>
</tr>
<tr>
<td>11.</td>
<td>Specify command level of the local user. <strong>authorization-attribute level</strong> <strong>level</strong></td>
<td>Optional. By default, the command level is 0.</td>
</tr>
<tr>
<td>12.</td>
<td>Specify service type for the local user. <strong>service-type</strong> <strong>telnet</strong></td>
<td>Required. By default, no service type is specified.</td>
</tr>
<tr>
<td>13.</td>
<td>Exit to system view. <strong>quit</strong></td>
<td>—</td>
</tr>
<tr>
<td>14.</td>
<td>Configure common settings for VTY user interfaces.</td>
<td>Optional. See “Configuring common settings for VTY user interfaces (optional)”</td>
</tr>
</tbody>
</table>

After you enable command authorization, you must perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters. For more information, see Security Configuration Guide.
- Reference the created HWTACACS scheme in the ISP domain. For more information, see Security Configuration Guide.

After you enable command accounting, you must perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the accounting server and other accounting parameters. For more information, see Security Configuration Guide.
- Reference the created HWTACACS scheme in the ISP domain. For more information, see Security Configuration Guide.

When users adopt the scheme mode to log in to the device, the level of the commands that the users can access depends on the user privilege level defined in the AAA scheme.

- When the AAA scheme is local, the user privilege level is defined by the **authorization-attribute level**.
- When the AAA scheme is RADIUS or HWTACACS, the user privilege level is configured on the RADIUS or HWTACACS server.

For more information about AAA, RADIUS, and HWTACACS, see Security Configuration Guide.

When you log in to the device through Telnet again:

- You are required to enter the login username and password. A prompt such as <HP> appears after you enter the correct username (for example, admin) and password and press **Enter**, as shown in Figure 13.
- After entering the correct username and password, if the device prompts you to enter another password of the specified type, you will be authenticated for the second time. In other words, to pass authentication, you must enter a correct password as prompted.
- If “All user interfaces are used, please try later!” is displayed, it means the current login users exceed the maximum number. Please try later.
### Configuring common settings for VTY user interfaces (optional)

**CAUTION:**

The **auto-execute command** command may disable you from configuring the system through the user interface to which the command is applied. Use it with caution.

Before executing the **auto-execute command** command and saving the configuration (by using **save**). Be sure you can access the device through VTY and AUX user interfaces so you can remove the configuration when a problem occurs.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable display of copyright information.</td>
<td>copyright-info enable</td>
</tr>
<tr>
<td>3.</td>
<td>Create a VLAN interface and enter VLAN interface view.</td>
<td>interface vlan-interface vlan-interface-id</td>
</tr>
<tr>
<td>4.</td>
<td>Specify an IP address for a VLAN interface.</td>
<td>ip address ip-address { mask</td>
</tr>
<tr>
<td>5.</td>
<td>Return to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>6.</td>
<td>Enter one or multiple VTY user interface views.</td>
<td>user-interface vty first-number [ last-number ]</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>7. User interface configuration</td>
<td>Enable the terminal service.</td>
<td><code>shell</code></td>
</tr>
<tr>
<td></td>
<td>Enable the current user interfaces to support either Telnet, SSH, or both of them.</td>
<td><code>protocol inbound</code> { all</td>
</tr>
<tr>
<td></td>
<td>Define a shortcut key for terminating tasks.</td>
<td><code>escape-key</code> { default</td>
</tr>
<tr>
<td></td>
<td>Configure the type of terminal display.</td>
<td><code>terminal type</code> { ansi</td>
</tr>
<tr>
<td></td>
<td>Set the maximum number of lines on the next screen.</td>
<td><code>screen-length</code></td>
</tr>
<tr>
<td></td>
<td>Set the size of history command buffer.</td>
<td><code>history-command max-size</code> <code>value</code></td>
</tr>
<tr>
<td></td>
<td>Set the idle-timeout timer.</td>
<td><code>idle-timeout</code> <code>minutes</code> <code>[ seconds ]</code></td>
</tr>
<tr>
<td></td>
<td>Specify a command to be automatically executed when a user logs in to the current user interface.</td>
<td><code>auto-execute command</code> <code>command</code></td>
</tr>
</tbody>
</table>
**Configuring the device to log in to a Telnet server as a Telnet client**

**Prerequisites**

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see "Configuration requirements."

![Figure 14 Log in to another device from the current device](image)

**NOTE:**

If the Telnet client port and the Telnet server port that connect them are not in the same subnet, make sure that the two devices can reach each other.

**Procedure**

Follow the step below to configure the device to log in to a Telnet server as a Telnet client:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>`[ [ vpn-instance vpn-instance-name ]</td>
<td>`</td>
</tr>
<tr>
<td></td>
<td>`source { interface interface-type interface-number</td>
<td>ip ip-address } ] ]`</td>
</tr>
<tr>
<td></td>
<td><code>telnet ipv6 remote-host [ -i</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>interface-type interface-number ]</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>[ port-number ] [ vpn-instance</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>vpn-instance-name ]</code></td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td><code>telnet client source { interface</code></td>
<td>Optional. By, no source IPv4 address or source interface is specified. The source IPv4 address is selected by routing.</td>
</tr>
<tr>
<td></td>
<td>`interface-type interface-number</td>
<td>ip`</td>
</tr>
<tr>
<td></td>
<td><code>ip ip-address }</code></td>
<td></td>
</tr>
</tbody>
</table>
Logging in through SSH

SSH offers an approach to log into a remote device securely. By providing encryption and strong authentication, it protects devices against attacks such as IP spoofing and plain-text password interception. The device supports SSH, and you can log in to the device through SSH to remotely manage and maintain the device, as shown in Figure 15.

Figure 15 SSH login diagram

The following table shows the configuration requirements of SSH login.

<table>
<thead>
<tr>
<th>Object</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH server</td>
<td>Configure the IP address of the VLAN interface, and make sure the SSH server and client can reach each other. Configure the authentication mode and other settings.</td>
</tr>
<tr>
<td>SSH client</td>
<td>Run the SSH client program. Obtain the IP address of the VLAN interface on the server.</td>
</tr>
</tbody>
</table>

By default, the device is enabled with the SSH server and client functions.
- On a device that serves as the SSH client, log in to an SSH server to perform operations on the server.
- On a device that serves as the SSH server, configure the authentication mode and user level for SSH users. By default, password authentication is adopted for SSH login, but no login password is configured, so you cannot log in to the device through SSH by default. Before log in to the device through SSH, you must log in to the device through the console port and configure the authentication mode, user level, and common settings.

Configuring the SSH server

NOTE:
This chapter describes how to configure an SSH client by using password authentication. For more information about SSH and how to configure an SSH client by using publickey, see Security Configuration Guide.

Prerequisites
You have logged in to the device, and want to log in to the device through SSH in the future.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”
**Procedure**

To configure the device that serves as an SSH server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Create local key pairs.</td>
<td>public-key local create ( { \text{dsa} \mid \text{rsa} } ) Required. By default, no local key pairs are created.</td>
</tr>
<tr>
<td>3.</td>
<td>Enable SSH server.</td>
<td>ssh server enable Required. By default, SSH server is disabled.</td>
</tr>
<tr>
<td>4.</td>
<td>Enter one or more VTY user interface views.</td>
<td>user-interface vty first-number [ last-number ] —</td>
</tr>
<tr>
<td>5.</td>
<td>Specify the scheme authentication mode.</td>
<td>authentication-mode scheme Required. By default, authentication mode for VTY user interfaces is <strong>password</strong>.</td>
</tr>
<tr>
<td>6.</td>
<td>Enable the current user interface to support SSH.</td>
<td>protocol inbound { all \mid ssh } Optional. By default, Telnet and SSH protocols are both supported.</td>
</tr>
</tbody>
</table>
| 7.   | Enable command authorization. | command authorization Optional. By default, command authorization is not enabled. <ul><li>By default, command level for a login user depends on the user privilege level. The user is authorized the command with the default level not higher than the user privilege level. With the command authorization configured, the command level for a login user is determined by both the user privilege level and AAA authorization. If a user executes a command of the corresponding command level, the authorization server checks whether the command is authorized. If it is, the command can be executed.</li></ul>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 8.   | 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 helps control and monitor user operations 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. |
| 9.   | Exit to system view **quit** | — |
| 10.  | Configure the authentication mode.  
- Enter the default ISP domain view. **domain domain-name** | Optional.  
By default, the AAA scheme is local.  
If you specify the local AAA scheme, perform the configuration concerning local user as well.  
If you specify an existing scheme by providing the `radius-scheme-name` argument, perform the following configuration as well:  
- For RADIUS and HWTACACS configuration, see *Security Configuration Guide*.  
- Configure the username and password on the AAA server. (For more information, see *Security Configuration Guide*.) |
|      | Apply the specified AAA scheme to the domain. **authentication default { hwtacacs-scheme hwtacacs-scheme-name [ local ] | local | none | radius-scheme radius-scheme-name [ local ] }** | — |
|      | Exit to system view. **quit** | — |
| 11.  | Create a local user and enter local user view. **local-user user-name** | Required.  
By default, no local user exists. |
| 12.  | Set the local password. **password { cipher | simple } password** | Required.  
By default, no local password is set. |
| 13.  | Specify the command level of the local user. **authorization-attribute level level** | Optional.  
By default, the command level is 0. |
| 14.  | Specify the service type for the local user. **service-type ssh** | Required.  
By default, no service type is specified. |
| 15.  | Return to system view. **quit** | — |
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 )

   Required.
   By default, no SSH user exists, and no authentication mode is specified.

17. Configure common settings for VTY user interfaces.

   Optional.
   See “Configuring common settings for VTY user interfaces (optional).”

After you enable command authorization or command accounting, you must perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters.
- Reference the created HWTACACS scheme in the ISP domain.

For more information, see Security Configuration Guide.

When users adopt the scheme mode to log in to the device, the level of the commands that the users can access depends on the user privilege level defined in the AAA scheme.

- When the AAA scheme is local, the user privilege level is defined by the authorization-attribute level.
- When the AAA scheme is RADIUS or HWTACACS, the user privilege level is configured on the RADIUS or HWTACACS server.
- For more information about AAA, RADIUS, and HWTACACS, see Security Configuration Guide.

Configuring the SSH client to log in to the SSH server

**Prerequisites**

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”

**Figure 16 Log in to another device from the current device**

![Diagram showing PC, SSH client, and SSH server connected](image)

**NOTE:**

If the SSH client and the SSH server are not in the same subnet, make sure that the two devices can reach each other.
Procedure

Configure other settings for the SSH client to work with the SSH server. For more information, see Security Configuration Guide. To configure the SSH client to log in to the SSH server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>ssh2 server</strong></td>
<td>Required server is the IPv4 address or host name of the server. Available in user view</td>
</tr>
<tr>
<td></td>
<td><strong>ssh2 ipv6 server</strong></td>
<td>Required server is the IPv6 address or host name of the server. Available in user view</td>
</tr>
</tbody>
</table>

Logging in through modems

The administrator can use two modems to remotely maintain a switch through its Console port over the Public Switched Telephone Network (PSTN) when the IP network connection is broken.

Configuration requirements

By default, no authentication is needed when you log in through modems, and the default user privilege level is 3.

To use this method, perform necessary configurations at both the device side and administrator side.

The following table shows the configuration requirements of remote login through the console port by using modem dial-in:

<table>
<thead>
<tr>
<th>Object</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator side</td>
<td>The PC is correctly connected to the modem.</td>
</tr>
<tr>
<td></td>
<td>The modem is connected to a telephone cable that works normally.</td>
</tr>
<tr>
<td></td>
<td>The telephone number of the remote modem connected to the Console port of the remote switch is obtained.</td>
</tr>
<tr>
<td>Device side</td>
<td>The Console port is correctly connected to the modem.</td>
</tr>
<tr>
<td></td>
<td>Configurations have been configured on the modem.</td>
</tr>
<tr>
<td></td>
<td>The modem is connected to a telephone cable that works properly.</td>
</tr>
<tr>
<td></td>
<td>Authentication configuration has been completed on the remote switch.</td>
</tr>
</tbody>
</table>
Login procedure

1. Set up a configuration environment as shown in Figure 2: connect the serial port of the PC and the Console port of the device to a modem respectively.

![Figure 2 Set up a configuration terminal](image)

2. Configuration on the administrator side

The PC and the modem are correctly connected, the modem is connected to a telephone cable, and the telephone number of the remote modem connected to the Console port of the remote switch is obtained.

**NOTE:**

On the device:
- The baud rate of the Console port is lower than the transmission rate of the modem. Otherwise, packets may be lost.
- The parity check mode, stop bits, and data bits of the Console port adopt the default settings.

3. Perform the following configurations on the modem that is directly connected to the device:

   - AT&F  ----------------------- Restore the factory defaults
   - ATS0=1  ----------------------- Configure auto-answer on first ring
   - AT&D  ----------------------- Ignore data Terminal Ready signals
   - AT&R0  ----------------------- Disable data Terminal Ready signals
   - AT&R1  ----------------------- Ignore Data Flow Control signals
   - AT&S0  ----------------------- Force DSR to remain on
   - ATEQ1&W ----------------------- Disable the modem from response to commands and save the configuration

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

**NOTE:**

The configuration commands and the output for different modems may be different. For more information, see the user guide of your modem.

4. Launch a terminal emulation utility (such as HyperTerminal in Windows XP/Windows 2000), create a new connection (the telephone number is the number of the modem connected to the device).

**NOTE:**

On Windows 2003 Server operating system, you must add the HyperTerminal program first, and then log in to and manage the device as described in this document. On Windows 2008 Server, Windows 7, Windows Vista, or some other operating system, you must 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.

5. Dial the destination number on the PC to establish a connection with the device, as shown in Figure 3 through Figure 5.
Figure 3 Connection Description

Enter a name and choose an icon for the connection.

- Name: (can be filled in, example: "COMM1")
- Icon: (select an icon from the options)

Options:
- OK
- Cancel

Figure 4 Enter the phone number

Enter details for the phone number that you want to dial:

- Country code: "China (86)"
- Area code: "010"
- Phone number: "82882285"
- Connect using: "Rockwell 33.6 DCP External PrP"

Options:
- OK
- Cancel

Figure 5 Dial the number

Phone number: "82882285"
- Your location: "Engineering Dept." (can be filled in)
- Calling card: None (Direct Dial)

Options:
- Dial
- Cancel
6. Character string CONNECT9600 is displayed on the terminal. Then a prompt appears when you press Enter.

Figure 6 Configuration page

![Configuration page](image)

7. If the authentication mode is **password**, a prompt (for example, HP) appears when you enter the configured password on the remote terminal. Then configure or manage the router. To get help, enter ?.

8. Execute commands to configure the device or check the running status of the device. To get help, enter ?.

**NOTE:**

- To terminate the connection between the PC and device, run **ATH** command on the terminal to terminate the connection between the PC and modem. If you cannot execute the command on the terminal, enter **AT+ + +** and then press Enter. When you are prompted **OK**, run **ATH**, and the connection is terminated if **OK** is displayed. Alternately, terminate the connection between the PC and device by clicking on the hyper terminal window.
- Do not close the hyper terminal directly. Otherwise, the remote modem remains online, and you will fail to dial in at the next time.

**Modem login authentication modes**

The following authentication modes are available for modem dial-in login: **none**, **password**, and **scheme**.

- **none**—Requires no username and password at the next login through modems. This mode is insecure.
- **password**—Requires password authentication at the next login through the console port. Keep your password.
- **scheme**—Requires username and password authentication at the next login through the console port. Authentication falls into local authentication and remote authentication. To use local authentication, configure a local user and related parameters. To use remote authentication, configure the username and password.
password on the remote authentication server. For more information about authentication modes and parameters, see Security Configuration Guide. Keep your username and password.

The following table lists modem login configurations for different authentication modes:

<table>
<thead>
<tr>
<th>Authentication mode</th>
<th>Configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Configure not to authenticate users.</td>
<td>For more information, see “Configuring none authentication for modem login.”</td>
</tr>
<tr>
<td>Password</td>
<td>Configure the device to authenticate users by using the local password. Set the local password.</td>
<td>For more information, see “Configuring password authentication for modem login.”</td>
</tr>
<tr>
<td>Scheme</td>
<td>Configure the authentication scheme.</td>
<td></td>
</tr>
<tr>
<td>Remote AAA</td>
<td>Configure a RADIUS/HWTACACS scheme. Configure the AAA scheme used by the domain.</td>
<td>For more information, see “Configuring scheme authentication for modem login.”</td>
</tr>
<tr>
<td>Select an authentication scheme.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local authentication</td>
<td>Configure the authentication username and password. Configure the AAA scheme used by the domain as local.</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**
Modem login authentication changes do not take effect until you exit the CLI and log in again.

**Configuring none authentication for modem login**

**Prerequisites**

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”
Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. system-view</td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td>Enter one or more AUX user interface views. user-interface aux first-number [ last-number ]</td>
<td>—</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the none authentication mode. authentication-mode none</td>
<td>Required. By default, users that log in through the console port are not authenticated.</td>
</tr>
<tr>
<td>4.</td>
<td>Configuring common settings for modem login. —</td>
<td>Optional. See “Configuring common settings for modem login (optional).”</td>
</tr>
</tbody>
</table>

When you log in to the device through modems after the configuration, you are prompted to press **Enter**. A prompt such as `<HP>` appears after you press **Enter**, as shown in Figure 7.

**Figure 7 Configuration page**

User interface aux0 is available.

Press ENTER to get started.

<HP>

---

**Configuring password authentication for modem login**

**Prerequisites**

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”

56
Procedure

To configure password authentication for modem login:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter system view</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>Enter one or more AUX user</td>
<td>user-interface aux first-number [last-number]</td>
<td>—</td>
</tr>
<tr>
<td>interface views</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specify the password authentication mode</td>
<td>authentication-mode password</td>
<td>Required By default, the authentication mode is none for modem users</td>
</tr>
<tr>
<td>Set the local password</td>
<td>set authentication password {cipher</td>
<td>simple} password</td>
</tr>
<tr>
<td>Configuring common settings for modem login</td>
<td>—</td>
<td>Optional For more information, see “Configuring common settings for modem login (optional).”</td>
</tr>
</tbody>
</table>

When you log in to the device through modems after the configuration, you are prompted to enter a login password. A prompt such as <HP> appears after you enter the password and press Enter, as shown in Figure 8.

**Figure 8 Configuration page**

User interface aux0 is available.

Press ENTER to get started.
Login authentication

Password: 
<HP>
Configuring scheme authentication for modem login

Prerequisites

You have logged in to the device.

By default, log in to the device through the console port without authentication and have user privilege level 3 after login. For information about logging in to the device with the default configuration, see “Configuration requirements.”

Procedure

To configure scheme authentication for modem login:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enter AUX user interface view.</td>
<td>user-interface aux first-number [ last-number ]</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the scheme authentication mode.</td>
<td>authentication-mode scheme</td>
</tr>
<tr>
<td>4.</td>
<td>Enable command authorization.</td>
<td>command authorization</td>
</tr>
</tbody>
</table>

- **Step 1**: Enter system view.
- **Step 2**: Enter AUX user interface view.
- **Step 3**: Specify the scheme authentication mode. Required. Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme. By default, the authentication mode is none for modem users.
- **Step 4**: Enable command authorization. Optional. By default, command authorization is not enabled. By default, command level for a login user depends on the user privilege level. The user is authorized the command with the default level not higher than the user privilege level. With the command authorization configured, the command level for a login user is determined by both the user privilege level and AAA authorization. If a user executes a command of the corresponding command level, the authorization server checks whether the command is authorized. If it is, the command can be executed. Before enabling command authorization, configure the AAA authorization server. After you enable command authorization, only commands authorized by the AAA authorization server can be executed.
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| 5.   | 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 helps control and monitor user operations 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.  
- Configure the AAA accounting server before enabling command accounting. |
| 6.   | quit | — |
| 7.   | domain domain-name 
authentication default ( hwtacacs
scheme hwtacacs
scheme-name [ local ] | local | none | radius
scheme radius
scheme-name [ local ] | Optional.  
- By default, the AAA scheme is local.  
- If you specify the local AAA scheme, perform the configuration concerning local user as well.  
- If you specify an existing scheme by providing the radius-scheme-name argument, perform the following configuration as well:  
  - For RADIUS and HWTACACS configuration, see Security Configuration Guide.  
  - Configure the username and password on the AAA server. (For more information, see Security Configuration Guide.) |
| 8.   | local-user user-name | Required.  
- By default, no local user exists. |
| 9.   | password ( cipher | simple ) password | Required. |
| 10.  | authorization-attribute level level | Optional.  
- By default, the command level is 0. |
| 11.  | service-type terminal | Required.  
- By default, no service type is specified. |
| 12.  | — | Optional.  
- See “Configuring common settings for modem login (optional).” |
After you enable command authorization, you must perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters. For more information, see Security Configuration Guide.
- Reference the created HWTACACS scheme in the ISP domain. For more information, see Security Configuration Guide.

After you enable command accounting, you must perform the following configuration to make the function take effect:

- Create a HWTACACS scheme, and specify the IP address of the accounting server and other accounting parameters. For more information, see Security Configuration Guide.
- Reference the created HWTACACS scheme in the ISP domain. For more information, see Security Configuration Guide.

When users adopt the scheme mode to log in to the device, the level of the commands that the users can access depends on the user privilege level defined in the AAA scheme.

- When the AAA scheme is local, the user privilege level is defined by the authorization-attribute level.
- When the AAA scheme is RADIUS or HWTACACS, the user privilege level is configured on the RADIUS or HWTACACS server.

For more information about AAA, RADIUS, and HWTACACS, see Security Configuration Guide.

When you log in to the device through modems after the configuration, you are prompted to enter a login username and password. A prompt such as <HP> appears after you enter the password and username and press Enter, as shown in Figure 9.

Figure 9 Configuration page

User interface aux0 is available.

Please press ENTER.

Login authentication

Username: admin
Password:
<HP>
# Configuring common settings for modem login (optional)

⚠ **CAUTION:**

- The common settings configured for Console login take effect immediately. If you configure the common settings after you log in through the Console port, the current connection may be interrupted. To avoid this problem, use another login method. After you configure the common settings for Console login, you must modify the settings on the terminal to make them consistent with those on the device.
- The baud rate of the Console port must be lower than the transmission rate of the modem. Otherwise, packets may be lost.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable display of copyright information.</td>
<td>copyright-info enable</td>
</tr>
<tr>
<td>3.</td>
<td>Enter one or more AUX user interface views.</td>
<td>user-interface aux first-number [ last-number ]</td>
</tr>
</tbody>
</table>

<p>| Configure baud rate | speed speed-value | Optional By default, the baud rate is 9600 bps. Transmission rate is the number of bits that the device transmits to the terminal per second. |
| Configure parity check mode | parity { even | mark | none | odd | space } | Optional By default, the parity check mode is none, which means no check bit. |
| Configure stop bits | stopbits { 1 | 1.5 | 2 } | Optional By default, the stop bit of the console port is 1. Stop bits are the last bits transmitted in data transmission to unequivocally indicate the end of a character. The more the bits are, the slower the transmission is. |
| Configure data bits | databits { 5 | 6 | 7 | 8 } | Optional By default, the data bit is 8. Data bits is the number of bits representing one character. The setting depends on the contexts to be transmitted. For example, 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. |
| Define shortcut key for starting a session | activation-key character | Optional By default, press Enter to start a session. |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Define shortcut key for terminating tasks | `escape-key { default | character }` | Optional  
By default, press Ctrl+C to terminate a task. |
| Configure flow control mode | `flow-control { hardware | none | software }` | Optional  
By default, the value is `none` |
| Configure type of terminal display | `terminal type { ansi | vt100 }` | Optional  
By default, the terminal display type is `ANSI`.  
The device supports two types of terminal display: ANSI and VT100. HP recommends setting the display type of both the device and the client to VT100. If the device and the client use different display types (for example, hyper terminal or Telnet terminal) or both are set to ANSI, when the total number of characters of the edited command line exceeds 80, an anomaly such as cursor corruption or abnormal display of the terminal display may occur on the client. |
| Configure user privilege level for login users | `user privilege level level` | Optional  
3 by default. |
| Set maximum number of lines on the next screen | `screen-length` | Optional  
By default, the next screen displays 24 lines at most.  
A value of 0 disables the function. |
| Set size of the history command buffer | `history-command max-size value` | Optional  
By default, the buffer saves 10 history commands at most. |
| Set idle-timeout timer | `idle-timeout minutes [ seconds ]` | Optional  
The default idle-timeout is 10 minutes. The system automatically terminates the user’s connection if no information interaction occurs between the device and the user within the idle-timeout time.  
Setting idle-timeout to 0 disables the timer. |
# Displaying and maintaining CLI login

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the source IP address/</td>
<td>`display telnet client configuration [</td>
<td>{ begin</td>
</tr>
<tr>
<td>interface specified for Telnet packets.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display information about the user</td>
<td>`display users [</td>
<td>{ begin</td>
</tr>
<tr>
<td>interfaces that are being used.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Displays information about all user</td>
<td>`display users all [</td>
<td>{ begin</td>
</tr>
<tr>
<td>interfaces that the device supports.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Display user interface information.</td>
<td>`display user-interface [ num1</td>
<td>{ aux</td>
</tr>
<tr>
<td>Release a specified user interface.</td>
<td>`free user-interface { num1</td>
<td>{ aux</td>
</tr>
<tr>
<td>Lock the current user interface.</td>
<td><code>lock</code></td>
<td>Available in user view. By default, the current user interface is not locked.</td>
</tr>
<tr>
<td>Send messages to the specified user</td>
<td>`send { all</td>
<td>num1</td>
</tr>
<tr>
<td>interfaces.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Web login

Overview

The device provides a built-in web server. It enables you to log in to the web interface of the device from a PC. Web login is disabled by default.

To enable web login, log in to the device via the console port, and perform the following configuration:

- Enable HTTP or HTTPS service.
- Configure the IP address of the VLAN interface.
- Configure a username and password.

The device supports the following web login methods:

- **HTTP login**—Used for transferring web page information across the Internet. It is an application-layer protocol in the TCP/IP protocol suite. The connection-oriented Transport Control Protocol (TCP) is adopted at the transport layer. The device supports HTTP 1.0.

- **HTTPS login**—Supports the SSL protocol and uses it to encrypt the data exchanged between the HTTPS client and the server to ensure data security and integrity. Define a certificate attribute-based access control policy to allow legal clients to access the device securely and prohibit illegal clients.

The following table shows the configuration requirements of web login.

<table>
<thead>
<tr>
<th>Object</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Configure the IP address of the VLAN interface. Make sure the device and the PC can reach each other.</td>
</tr>
<tr>
<td>PC</td>
<td>Install a web browser. Obtain the IP address of the VLAN interface of the device.</td>
</tr>
</tbody>
</table>
# Configuring HTTP login

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the HTTP service.</td>
<td>ip http enable</td>
</tr>
<tr>
<td></td>
<td>Required. Enabled by default.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Configure the HTTP service port number.</td>
<td>ip http port port-number</td>
</tr>
<tr>
<td></td>
<td>Optional. 80 by default. If you execute the command multiple times, the last one takes effect.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Associate the HTTP service with an ACL.</td>
<td>ip http acl acl-number</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td>Create a local user and enter local user view.</td>
<td>local-user user-name</td>
</tr>
<tr>
<td></td>
<td>Required. By default, no local user is configured.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td>Configure a password for the local user.</td>
<td>password { cipher</td>
</tr>
<tr>
<td></td>
<td>Required. By default, no password is configured for the local user.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td>Specify the command level of the local user.</td>
<td>authorization-attribute level level</td>
</tr>
<tr>
<td></td>
<td>Required. No command level is configured for the local user.</td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td>Specify the Telnet service type for the local user.</td>
<td>service-type telnet</td>
</tr>
<tr>
<td></td>
<td>Required. By default, no service type is configured for the local user.</td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td>Exit to system view.</td>
<td>quit</td>
</tr>
<tr>
<td></td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>10.</td>
<td>Create a VLAN interface and enter its view.</td>
<td>interface vlan-interface vlan-interface-id</td>
</tr>
<tr>
<td></td>
<td>Required. If the VLAN interface already exists, the command enters its view.</td>
<td></td>
</tr>
<tr>
<td>11.</td>
<td>Assign an IP address and subnet mask to the VLAN interface.</td>
<td>ip address ip-address { mask</td>
</tr>
<tr>
<td></td>
<td>Required. By default, no IP address is assigned to the VLAN interface.</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring HTTPS login

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td>system-view</td>
<td></td>
</tr>
<tr>
<td>2. Configure PKI and SSL related features.</td>
<td>—</td>
<td>Required by default, PKI and SSL are not configured.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For more information about PKI, see <em>Security Configuration Guide</em>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For more information about SSL, see <em>Security Configuration Guide</em>.</td>
</tr>
<tr>
<td>3. Associate the HTTPS service with an SSL server policy.</td>
<td>ip https ssl-server-policy</td>
<td>Required by default, the HTTPS service is not associated with any SSL server policy.</td>
</tr>
<tr>
<td></td>
<td>policy-name</td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Any changes to the SSL server policy associated with the HTTP service that is enabled do not take effect.</td>
</tr>
<tr>
<td>4. Enable the HTTPS service.</td>
<td>ip https enable</td>
<td>Required by default. Disabling the HTTPS service triggers an SSL handshake negotiation process. During the process:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the local certificate of the device exists, the SSL negotiation succeeds, and the HTTPS service can be started normally.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If no local certificate exists, a certificate application process is triggered by the SSL negotiation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Because the application process takes much time, the SSL negotiation often fails and the HTTPS service cannot be started normally. In that case, you must run <code>ip https enable</code> multiple times to start the HTTPS service.</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| 5.   | **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 `client-verify enable` 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. |
| 6.   | **ip https port port-number** | Optional.  
443 by default. |
| 7.   | **ip https acl acl-number** | Required.  
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. |
| 8.   | **local-user user-name** | Required.  
By default, no local user is configured. |
| 9.   | **password { cipher | simple } password** | Required.  
By default, no password is configured for the local user. |
| 10.  | **authorization-attribute level level** | Required.  
By default, no command level is configured for the local user. |
| 11.  | **service-type telnet** | Required.  
By default, no service type is configured for the local user. |
| 12.  | **quit** | — |
If the VLAN interface already exists, the command enters its view. |
| 14.  | **ip address ip-address { mask | mask-length }** | Required.  
By default, no IP address is assigned to the VLAN interface. |
Displaying and maintaining web login

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about web users.</td>
<td>`display web users [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display HTTP state information.</td>
<td>`display ip http [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display HTTPS state information.</td>
<td>`display ip https [</td>
<td>{ begin</td>
</tr>
</tbody>
</table>

Web login example

HTTP login example

Network requirements

As shown in Figure 10, the PC is connected to the device over an IP network. The IP address of the Device is 192.168.20.66/24.

![Network diagram for configuring HTTP login](image)

**Procedure**

1. Configuration on the device

   # Log in to the device via the console port and configure the IP address of VLAN 1 of the device. VLAN 1 is the default VLAN.

   ```
   <Sysname> system-view
   [Sysname] interface vlan-interface 1
   [Sysname-VLAN-interface1] ip address 192.168.20.66 255.255.255.0
   [Sysname-VLAN-interface1] quit
   ```

   # Create a local user named admin, and set the password to admin for the user. Specify the Telnet 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 telnet
   [Sysname-luser-admin] authorization-attribute level 3
   [Sysname-luser-admin] password simple admin
   ```
2. Configuration on the PC

# On the PC, run the web browser. Enter the IP address of the device in the address bar, 192.168.20.66 in this example. The web login page appears, as shown in Figure 4.

Figure 4 Web login page

![Web login page](image)

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

**HTTPS login example**

**Network requirements**

As shown in Figure 5, to prevent unauthorized users from accessing the Device, configure HTTPS login as follows:

- Configure the Device as the HTTPS server, and request a certificate for it.
- The Host acts as the HTTPS client. Request a certificate for it.

In this example, Windows Server acts as the CA. Install Simple Certificate Enrollment Protocol (SCEP) add-on on the CA. The name of the CA that issues certificates to the Device and Host is new-ca.

Before performing the following configuration, make sure that the Device, Host, and CA can reach each other.
Figure 5 Network diagram for configuring HTTPS login

Procedure

1. Configure the device that acts as the 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 local 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 (DN) 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** for the user, and specify the Telnet service type for the local user.

```
[Device] local-user usera
[Device-luser-usera] password simple 123
[Device-luser-usera] service-type telnet
```

2. Configure the host that acts as the HTTPS client

On the host, run the IE browser. In the address bar, enter **http://10.1.2.2/certsrv** 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**. Then the web login page of the Device appears. On the login page, type the username **usera**, and password **123** to enter the web management page.

To log in to the web interface through HTTPS, enter the URL address starting with **https://**. To log in to the web interface through HTTP, enter the URL address starting with **http://**.

- For more information about PKI configuration commands, see *Security Command Reference*.
- For more information about the publickey local create rsa command, see *Security Command Reference*.
- For more information about SSL configuration commands, see *Security Command Reference*.
NMS login

Overview

A Network Management Station (NMS) runs the SNMP client software. It offers a user-friendly interface to facilitate network management. An agent is a program that resides in the device. It receives and handles requests from the NMS. An NMS is a manager in an SNMP enabled network, whereas agents are managed by the NMS. The NMS and agents exchange information through the SNMP protocol. The device supports multiple NMS programs, such as iMC and CAMS.

By default, you cannot log in to the device through NMS. To enable NMS login, log in to the device via the console port and make the configurations described in the following table.

The following table shows the configuration requirements of NMS login.

<table>
<thead>
<tr>
<th>Object</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Configure the IP address of the VLAN interface.</td>
</tr>
<tr>
<td></td>
<td>Make sure the device and the NMS can reach each other.</td>
</tr>
<tr>
<td></td>
<td>Configure SNMP settings.</td>
</tr>
<tr>
<td>NMS</td>
<td>Configure the NMS. For more information, see the manual of your NMS.</td>
</tr>
</tbody>
</table>

Configuring NMS login

Connect the Ethernet port of the PC to an Ethernet port of VLAN 1 of the device, as shown in Figure 6. Make sure the PC and VLAN 1 interface can reach each other.

The device supports three SNMP versions: SNMPv1, SNMPv2c and SNMPv3. For more information about SNMP, see Network Management and Monitoring Configuration Guide.

Figure 6 Network diagram for configuring NMS login
## Configuring SNMPv1 and SNMPv2c settings

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable SNMP agent.</td>
<td>snmp-agent</td>
</tr>
<tr>
<td>3.</td>
<td>Create or update MIB view information.</td>
<td>snmp-agent mib-view { excluded</td>
</tr>
<tr>
<td>4.</td>
<td>Configure SNMP NMS access right. Directly</td>
<td>snmp-agent community { read</td>
</tr>
<tr>
<td></td>
<td>Indirectly</td>
<td>snmp-agent group { v1</td>
</tr>
<tr>
<td></td>
<td>Add a user to the SNMP group.</td>
<td>snmp-agent usm-user { v1</td>
</tr>
</tbody>
</table>
## Configuring SNMPv3 settings

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
</tbody>
</table>
| 2.   | Enable SNMP agent. | snmp-agent | Optional.  
Disabled by default.  
Enable SNMP agent with this command or any command that begins with **snmp-agent**. |
| 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 ] | Required.  
By default, no SNMP group is configured. |
If the **cipher** keyword is specified, both auth-password and priv-password are cipher-text passwords. |

### NMS login example

In this example, iMC is used as the NMS.

1. Configuration on the device

   # Assign IP address of device. Make sure the device and the NMS can reach each other. (Configuration steps are omitted.)

   # Enter system view.
   ```
   <Sysname> system-view
   ```

   # Enable the SNMP agent.
   ```
   [Sysname] snmp-agent
   ```

   # Configure an SNMP group.
   ```
   [Sysname] snmp-agent group v3 managev3group read-view test write-view test
   ```

   # Add a user to the SNMP group.
   ```
   [Sysname] snmp-agent usm-user v3 managev3user managev3group
   ```
2. Configuration on the NMS

On the PC, start the browser. In the address bar, enter http://192.168.20.107:8080/imc, where 192.168.20.107 is the IP address of the iMC.

Figure 7 iMC login page
Enter the username and password, and then click **Login**. The iMC homepage appears, as shown in Figure 8.

**Figure 8 iMC homepage**

Log in to the iMC and configure SNMP settings for the iMC to find the device. After the device is found, manage and maintain the device through the iMC. For example, query device information or configure device parameters.

The SNMP settings on the iMC must be the same as those configured on the device. If not, the device cannot be found or managed by the iMC. See the iMC manuals for more information.

Click **Help** in the upper right corner of each configuration page to get corresponding help information.
User login control

Overview

The device provides the following login control methods.

<table>
<thead>
<tr>
<th>Login Through</th>
<th>Login control methods</th>
<th>ACL used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telnet</td>
<td>Configuring source IP-based login control over Telnet users</td>
<td>Basic ACL</td>
</tr>
<tr>
<td></td>
<td>Configuring source and destination IP-based login control</td>
<td>Advanced ACL</td>
</tr>
<tr>
<td></td>
<td>over Telnet users</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuring source MAC-based login control over Telnet users</td>
<td>Ethernet frame header ACL</td>
</tr>
<tr>
<td>NMS</td>
<td>Configuring source IP-based login control over NMS users</td>
<td>Basic ACL</td>
</tr>
<tr>
<td>Web</td>
<td>Configuring source IP-based login control over web users</td>
<td>Basic ACL</td>
</tr>
</tbody>
</table>

Configuring login control over Telnet users

Configuration preparation

Before configuration, determine the permitted or denied source IP addresses, source MAC addresses, and destination IP addresses.

Configuring source IP-based login control over Telnet users

Because basic ACLs match the source IP addresses of packets, use basic ACLs to implement source IP-based login control over Telnet users. Basic ACLs are numbered from 2000 to 2999. For more information about ACL, see ACL and QoS Configuration Guide.

To configure source IP-based login control over Telnet users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a basic ACL and enter its view, or enter the view of an existing basic ACL.</td>
<td>acl [ ipv6 ] number acl-number [ match-order { config</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Required. By default, no basic ACL exists.</td>
</tr>
<tr>
<td>3.</td>
<td>Configure rules for this ACL.</td>
<td>rule [ rule-id ] { permit</td>
</tr>
</tbody>
</table>
### Configuring source and destination IP-based login control over Telnet users

Because advanced ACLs can match both source and destination IP addresses of packets, use advanced ACLs to implement source and destination IP-based login control over Telnet users. Advanced ACLs are numbered from 3000 to 3999. For more information about ACL, see *ACL and QoS Configuration Guide*.

To configure source and destination IP-based login control over Telnet users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>3.</td>
<td>rule [ rule-id ] { permit</td>
<td>deny } rule-string</td>
</tr>
<tr>
<td>4.</td>
<td>quit</td>
<td>—</td>
</tr>
<tr>
<td>5.</td>
<td>user-interface [ type ] first-number [ last-number ]</td>
<td>—</td>
</tr>
</tbody>
</table>
  - **inbound**—Filters incoming Telnet packets.  
  - **outbound**—Filters outgoing Telnet packets. |

### Configuring source MAC-based login control over Telnet users

Ethernet frame header ACLs can match the source MAC addresses of packets, so use Ethernet frame header ACLs to implement source MAC-based login control over Telnet users. Ethernet frame header ACLs are numbered from 4000 to 4999. For more information about ACL, see *ACL and QoS Configuration Guide*. 

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td>acl [ ipv6 ] number acl-number</td>
<td>Required. By default, no advanced ACL exists.</td>
</tr>
<tr>
<td>3.</td>
<td>rule [ rule-id ] { permit</td>
<td>deny } rule-string</td>
</tr>
<tr>
<td>4.</td>
<td>quit</td>
<td>—</td>
</tr>
<tr>
<td>5.</td>
<td>user-interface [ type ] first-number [ last-number ]</td>
<td>—</td>
</tr>
</tbody>
</table>
  - **inbound**—Filters incoming Telnet packets.  
  - **outbound**—Filters outgoing Telnet packets. |
To configure source MAC-based login control over Telnet users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Create an Ethernet frame header ACL and enter its view.</td>
<td>acl number acl-number [ match-order { config</td>
</tr>
<tr>
<td>3.</td>
<td>Configure rules for the ACL.</td>
<td>rule { rule-id } { permit</td>
</tr>
<tr>
<td>4.</td>
<td>Exit the advanced ACL view.</td>
<td>quit —</td>
</tr>
<tr>
<td>5.</td>
<td>Enter user interface view.</td>
<td>user-interface [ type ] first-number [ last-number ] —</td>
</tr>
<tr>
<td>6.</td>
<td>Use the ACL to control user login by source MAC address.</td>
<td>acl acl-number inbound Required. inbound: Filters incoming Telnet packets.</td>
</tr>
</tbody>
</table>

**NOTE:**
The above configuration does not take effect if the Telnet client and server are not in the same subnet.

### Source MAC-based login control configuration example

#### Network requirements
As shown in Figure 9, configure an ACL on the Device to permit only incoming Telnet packets sourced from Host A and Host B.

**Figure 9 Network diagram for configuring source MAC-based login control**
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

Configuring source IP-based login control over NMS users

Log in to the NMS to remotely manage the devices. SNMP is used for communication between the NMS and
the agent that resides in the device. By using the ACL, control SNMP user access to the device.

Configuration preparation

Before configuration, determine the permitted or denied source IP addresses.

Configuring source IP-based login control over NMS users

Because basic ACLs match the source IP addresses of packets, use basic ACLs to implement source IP-based
login control over NMS users. Basic ACLs are numbered from 2000 to 2999. For more information about
ACL, see ACL and QoS Configuration Guide.

To configure source IP-based login control over NMS users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a basic ACL and enter its view, or enter the view of an existing basic ACL.</td>
<td>acl [ipv6</td>
</tr>
<tr>
<td></td>
<td></td>
<td>By default, no basic ACL exists.</td>
</tr>
</tbody>
</table>
| 3.    | Create rules for this ACL.       | rule [rule-id] {permit | deny} [source
|       |                                  | {source-addr source-wildcard | any} | time-range | time-name | fragment | logging] | Required. |
| 4.    | Exit the basic ACL view.         | quit                                         | —                        |
| 5.    | Associate this SNMP community with the ACL. | snmp-agent community [read | write] community-name [ad acl-number | mib-view view-name] | Required.  |
|       |                                  | Associate the ACL                            |

80
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><strong>snmp-agent group</strong> { v1</td>
<td>v2c } group-name [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl acl-number ]&lt;br&gt;<strong>snmp-agent group v3</strong> group-name [ authentication</td>
</tr>
<tr>
<td>7.</td>
<td><strong>snmp-agent usm-user</strong> { v1</td>
<td>v2c }&lt;br&gt;user-name group-name [ acl acl-number ]&lt;br&gt;<strong>snmp-agent usm-user v3</strong> user-name group-name [ [ cipher ] authentication-mode { md5</td>
</tr>
</tbody>
</table>

**Source IP-based login control over NMS users configuration example**

**Network requirements**

As shown in Figure 10, configure the device to allow only NMS users from Host A and Host B to access.

**Figure 10 Network diagram for configuring source IP-based login control over NMS users**

![Network diagram](image)

**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.<br><Sysname> system-view<br>[Sysname] acl number 2000 match-order config<br>[Sysname-acl-basic-2000] rule 1 permit source 10.110.100.52 0<br>[Sysname-acl-basic-2000] rule 2 permit source 10.110.100.46 0<br>[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 source IP-based login control over web users

Log in to the web management page of the device through HTTP/HTTPS to remotely manage the devices. By using the ACL, control web user access to the device.

Configuration preparation

Before configuration, determine the permitted or denied source IP addresses.

Configuring source IP-based login control over web users

Because basic ACLs match the source IP addresses of packets, use basic ACLs to implement source IP-based login control over web users. Basic ACLs are numbered from 2000 to 2999. For more information about ACL, see ACL and QoS Configuration Guide.

To configure source IP-based login control over web users:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td>acl [ ipv6 ] number acl-number [ match-order { config</td>
<td>auto } ]</td>
</tr>
<tr>
<td></td>
<td>rule [ rule-id ] { permit</td>
<td>deny } [ source { sour-addr sour-wildcard</td>
</tr>
<tr>
<td>3.</td>
<td>quit</td>
<td>—</td>
</tr>
<tr>
<td>4.</td>
<td>ip http acl acl-number</td>
<td>Required to use one command.</td>
</tr>
<tr>
<td>5.</td>
<td>ip https acl acl-number</td>
<td></td>
</tr>
</tbody>
</table>

82
Logging off online web users

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log off online web users.</td>
<td>Required. Execute the command in user interface view.</td>
</tr>
</tbody>
</table>

Source IP-based login control over web users configuration example

Network requirements

As shown in Figure 11, configure the device to allow only web users from Host B to access.

Figure 11 Network diagram for configuring source IP-based login control

![Network diagram for configuring source IP-based login control](image)

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 that only web users from Host B are allowed to access the device.
[Sysname] ip http acl 2030
Configuring FTP

Overview

FTP is an application layer protocol for sharing files between server and client over a TCP/IP network. FTP uses TCP ports 20 and 21 for file transfer. Port 20 is used to transmit data, and port 21 to transmit control commands. For more information about FTP basic operations, see RFC 959.

FTP transfers files in the following modes:
- **ASCII mode**—Transfers files as text, like .txt, .bat, and .cfg files.
- **Binary mode**—Transfers files as raw data, like .app, .bin, and .btm files.

Operation

⚠️ **CAUTION:**
- Make sure that the FTP server and the FTP client can reach each other before establishing the FTP connection.
- When you use IE to log in to the device serving as the FTP server, some FTP functions are not available. This is because multiple connections are established during the login process but the device supports only one connection at a time.

FTP adopts the client/server model. Your device can function either as the client or the server (as shown in Figure 12).
- When the device serves as the FTP client, use Telnet or an emulation program to log in to the device from the PC, run `ftp` to establish a connection from the device (FTP client) to the PC (FTP server), and then upload/download files to/from the server.
- When the device serves as the FTP server, run the FTP client program on the PC to establish a connection to the FTP server and upload/download files to/from the server.

![Network diagram for FTP](image)

When the device serves as the FTP client, you must perform the following configuration:

<table>
<thead>
<tr>
<th>Device (FTP client)</th>
<th>Configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use <code>ftp</code> to establish the connection to the remote FTP server.</td>
<td>If the remote FTP server supports anonymous FTP, the device can log in to it directly; if not, the device must obtain the FTP username and password first to log in to the remote FTP server.</td>
<td></td>
</tr>
</tbody>
</table>
When the device serves as the FTP server, you must perform the following configuration:

**Table 6 Configuration when the device serves as the FTP server**

<table>
<thead>
<tr>
<th>Device (FTP server)</th>
<th>Configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the FTP server function.</td>
<td>Disabled by default.</td>
<td>Use <code>display ftp-server</code> to view the FTP server configuration on the device.</td>
</tr>
<tr>
<td>Configure authentication and authorization.</td>
<td>Configure the username, password, and authorized directory for an FTP user.</td>
<td>The device does not support anonymous FTP for security reasons. You must set a valid username and password. By default, authenticated users can access the root directory of the device.</td>
</tr>
<tr>
<td>Configure the FTP server operating parameters.</td>
<td>Parameters such as the FTP connection timeout time.</td>
<td></td>
</tr>
<tr>
<td>PC (FTP client)</td>
<td>Use the FTP client program to log in to the FTP server.</td>
<td>Log in to the FTP server only after you enter the correct FTP username and password.</td>
</tr>
</tbody>
</table>

**Configuring the FTP client**

Only users with the manage level can use `ftp` to log in to an FTP server, enter FTP client view, and execute directory and file related commands. However, whether the commands can be executed successfully depends on the authorizations of the FTP server.

**Establishing an FTP connection**

Before access the FTP server, you must first establish a connection from the FTP client to the FTP server. Either use `ftp` to establish the connection directly or use `open` command in FTP client view to establish the connection.

When using `ftp`, specify the source interface (such as a loopback) or source IP address. The primary IP address of the specified source interface or the specified source IP address is used as the source IP address of sent FTP packets. The source address of the transmitted packets is selected following these rules:

- If no source address is specified, the FTP client uses the IP address of the interface determined by the matched route as the source IP address to communicate with an FTP server.
- If the source address is specified with the `ftp client source` or `ftp`, this source address is used to communicate with an FTP server.
- If you use `ftp client source` and `ftp` to specify a source address respectively, the source address specified with `ftp` is used to communicate with an FTP server.
- The source address specified with `ftp client source` is valid for all FTP connections and the source address specified with `ftp` is valid only for the current FTP connection.
To establish an IPv4 FTP connection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the source address of the FTP client.</td>
<td>ftp client source { interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Optional. A switch uses the IP address of the interface determined by the matched route as the source IP address to communicate with the FTP server by default.</td>
</tr>
<tr>
<td>3.</td>
<td>Exit to system view.</td>
<td>quit</td>
</tr>
<tr>
<td>4.</td>
<td>Log in to the remote FTP server directly in user view.</td>
<td>ftp [ server-address [ service-port ] [ vpn-instance vpn-instance-name ] [ source { interface interface-type interface-number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use either approach. The ftp command is available in user view; and open is available in FTP client view.</td>
</tr>
<tr>
<td>5.</td>
<td>Log in to the remote FTP server indirectly in FTP client view.</td>
<td>ftp open server-address [ service-port ]</td>
</tr>
</tbody>
</table>

If no primary IP address is configured on the specified source interface, you cannot establish an FTP connection.

If you use ftp client source to configure a source interface and then use it to configure a source IP address, the source IP address overwrites the source interface, and vice versa.

To establish an IPv6 FTP connection:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log in to the remote FTP server directly in user view.</td>
<td>ftp ipv6 [ server-address [ service-port ] [ vpn-instance vpn-instance-name ] [ source ipv6 source-ipv6-address ] [ -i interface-type interface-number ] ]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use either approach. The ftp ipv6 command is available in user view; and open ipv6 is available in FTP client view.</td>
</tr>
<tr>
<td>2.</td>
<td>Log in to the remote FTP server indirectly in FTP client view.</td>
<td>open ipv6 server-address [ service-port ] [ -i interface-type interface-number ]</td>
</tr>
</tbody>
</table>
Operating FTP server directories

After the switch serving as the FTP client has established a connection with an FTP server, create or delete folders under the authorized directory of the FTP server. For more information about establishing an FTP connection, see “Establishing an FTP connection.”

To operate the directories on an FTP server:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display detailed information about a directory or file on the remote FTP server.</td>
<td>dir [ remotefile [ localfile ] ]</td>
<td>Optional</td>
</tr>
<tr>
<td>Query a directory or file on the remote FTP server.</td>
<td>ls [ remotefile [ localfile ] ]</td>
<td>Optional</td>
</tr>
<tr>
<td>Change the working directory of the remote FTP server.</td>
<td>cd ( directory</td>
<td>..</td>
</tr>
<tr>
<td>Exit the current working directory and return to an upper level directory of the remote FTP server.</td>
<td>cdup</td>
<td>Optional</td>
</tr>
<tr>
<td>Display the working directory that is being accessed.</td>
<td>pwd</td>
<td>Optional</td>
</tr>
<tr>
<td>Create a directory on the remote FTP server.</td>
<td>mkdir directory</td>
<td>Optional</td>
</tr>
<tr>
<td>Remove the specified working directory on the remote FTP server.</td>
<td>rmdir directory</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Operating FTP server files

After the switch serving as the FTP client has established a connection with an FTP server, upload a file to or download a file from the FTP server under the authorized directory of the FTP server by following these steps. For information about establishing an FTP connection, see “Establishing an FTP connection.”

Use dir or ls to view the directory and the location of the file on the FTP server.

Delete useless files for effective use of the storage space.

Set the file transfer mode. FTP transmits files in two modes:

- **ASCII mode**—Transfers files as text.
- **Binary mode**—Transfers files as raw data.

Uselcd to view the local working directory of the FTP client. Upload the file under this directory, or save the downloaded file under this directory.

Upload or download the file.
To operate the files on an FTP server:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display detailed information about a directory or file on the remote FTP server.</td>
<td><code>dir [ remotefile [ localfile ] ]</code></td>
<td>Optional. The <code>ls</code> command only displays the name of a directory or file. The <code>dir</code> command displays detailed information such as the file size and creation time.</td>
</tr>
<tr>
<td>Query a directory or file on the remote FTP server.</td>
<td><code>ls [ remotefile [ localfile ] ]</code></td>
<td>Optional. The <code>ls</code> command only displays the name of a directory or file. The <code>dir</code> command displays detailed information such as the file size and creation time.</td>
</tr>
<tr>
<td>Delete the specified file on the remote FTP server permanently.</td>
<td><code>delete remotefile</code></td>
<td>Optional.</td>
</tr>
<tr>
<td>Set the file transfer mode to ASCII.</td>
<td><code>ascii</code></td>
<td>Optional. ASCII by default.</td>
</tr>
<tr>
<td>Set the file transfer mode to binary.</td>
<td><code>binary</code></td>
<td>Optional. ASCII by default.</td>
</tr>
<tr>
<td>Set the data transmission mode to passive.</td>
<td><code>passive</code></td>
<td>Optional. Passive by default.</td>
</tr>
<tr>
<td>Display the local working directory of the FTP client.</td>
<td><code>lcd</code></td>
<td>Optional.</td>
</tr>
<tr>
<td>Upload a file to the FTP server.</td>
<td><code>put localfile [ remotefile ]</code></td>
<td>Optional.</td>
</tr>
<tr>
<td>Download a file from the FTP server.</td>
<td><code>get remotefile [ localfile ]</code></td>
<td>Optional.</td>
</tr>
</tbody>
</table>

Using another username to log in to an FTP server

After the switch serving as the FTP client has established a connection with the FTP server, use another username to log in to the FTP server. For more information about establishing an FTP connection, see “Establishing an FTP connection.”

This feature allows you to switch to different user levels without affecting the current FTP connection; if you enter an incorrect username or password, the current connection is terminated, and you must log in again to access the FTP server.

Follow the step below to use another username to log in to the FTP server:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use another username to re-log in after successfully logging in to the FTP server.</td>
<td><code>user username [ password ]</code></td>
<td>Optional.</td>
</tr>
</tbody>
</table>
Maintaining and debugging an FTP connection

After a switch serving as the FTP client has established a connection with the FTP server, perform the following operations to locate and diagnose problems encountered in an FTP connection. For more information about establishing an FTP connection, see “Establishing an FTP connection.”

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the help information of FTP-related commands supported by the remote FTP server.</td>
<td><code>remotehelp [ protocol-command ]</code></td>
<td>Optional.</td>
</tr>
<tr>
<td>Enable information display in a detailed manner.</td>
<td><code>verbose</code></td>
<td>Optional. Enabled by default.</td>
</tr>
<tr>
<td>Enable FTP related debugging when the switch acts as the FTP client.</td>
<td><code>debugging</code></td>
<td>Optional. Disabled by default.</td>
</tr>
</tbody>
</table>

Terminating an FTP connection

After the switch serving as the FTP client has established a connection with the FTP server, use any of the following commands to terminate an FTP connection. For more information about establishing an FTP connection, see “Establishing an FTP connection.”

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate the connection to the FTP server without exiting FTP client view.</td>
<td><code>disconnect</code></td>
<td>Optional. Equal to the <code>close</code>.</td>
</tr>
<tr>
<td>Terminate the connection to the FTP server without exiting FTP client view.</td>
<td><code>close</code></td>
<td>Optional. Equal to <code>disconnect</code>.</td>
</tr>
<tr>
<td>Terminate the connection to the FTP server and return to user view.</td>
<td><code>bye</code></td>
<td>Optional. Equal to the <code>quit</code> command in FTP client view.</td>
</tr>
<tr>
<td>Terminate the connection to the FTP server and return to user view.</td>
<td><code>quit</code></td>
<td>Optional. Available in FTP client view, equal to the <code>bye</code>.</td>
</tr>
</tbody>
</table>

FTP client configuration example

Network requirements

- As shown in Figure 13, use Device as an FTP client and PC as the FTP server. Their IP addresses are 10.2.1.1/16 and 10.1.1.1/16 respectively. Device and PC are reachable to each other.
- Device downloads a boot file from PC for device upgrade, and uploads the configuration file to PC for backup.
- On PC, an FTP user account has been created for the FTP client, with the username being `abc` and the password being `pwd`. 
Figure 13 Network diagram for FTPing a boot file from an FTP server

![Network Diagram](image)

**Procedure**

⚠️ **CAUTION:**
- The boot file used for the next startup must be saved under the root directory of the storage medium. Copy or move a file to the root directory of the storage medium. For more information about boot-loader, see Fundamentals Command Reference.
- If the available memory space of the device is not enough, use `fixdisk` to clear the memory or use `delete` `/unreserved file-url` to delete the files not in use and then perform the following operations.

# Log in to the server through FTP.
```plaintext
<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 to transmit boot file.
```plaintext
[ftp] binary
200 Type set to I.
```

# Download the boot file `newest.bin` from PC to Device.
```plaintext
[ftp] get newest.bin
```

# Upload the configuration file `config.cfg` of Device to the server for backup.
```plaintext
[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
```

# Specify `newest.bin` as the main boot file to be used at the next startup.
```plaintext
<Sysname> boot-loader file newest.bin main
```

# Reboot the device, and the boot file is updated at the system reboot.
```plaintext
<Sysname> reboot
```
FTP client configuration example

Network requirements

- As shown in Figure 14, use Device as an FTP client and PC as the FTP server. Their IP addresses are 10.2.1.1/16 and 10.1.1.1/16 respectively. Device and PC are reachable to each other.
- Device downloads a boot file from PC for device upgrade, and uploads the configuration file to PC for backup.
- On PC, an FTP user account has been created for the FTP client, with the username being abc and the password being pwd.

Figure 14 Network diagram for FTPing a boot file from an FTP server

![Network diagram for FTPing a boot file from an FTP server](image)

Procedure

⚠️ CAUTION:
- The boot file used for the next startup must be saved under the root directory of the storage medium. Copy or move a file to the root directory of the storage medium. For more information about boot-loader, see Fundamentals Command Reference.
- If the available memory space of the device is not enough, use fixdisk to clear the memory or use delete /unreserved file-url to delete the files not in use and then perform the following operations.

# Log in to the server 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 to transmit boot file.
[ftp] binary
200 Type set to I.

# Download the boot file newest.bin from PC to the device.
- Download the boot file newest.bin from PC to the root directory of the storage medium on the master.
[ftp] get newest.bin
• Download the boot file `newest.bin` from PC to the root directory of the storage medium of a subordinate switch (with member ID of 2).

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

# Upload the configuration file `config.cfg` of the device to the server 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
```

# Specify `newest.bin` as the main boot file to be used at 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!

# Reboot the device, and the boot file is updated at the system reboot.

```
<Sysname> reboot
```

## Configuring the FTP server

### Configuring FTP server operating parameters

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

- **Fast mode**—The FTP server starts writing data to the storage medium after a file is transferred to the memory. This prevents the existing file on the FTP server from being corrupted in the event that an anomaly, power failure for example, occurs during a file transfer.

- **Normal mode**—The FTP server writes data to the storage medium while receiving data. This means that any anomaly, power failure for example, 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 the FTP server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the FTP server</td>
<td>ftp server enable Required. Disabled by default.</td>
</tr>
<tr>
<td>3.</td>
<td>Use an ACL to control FTP clients’ access to the switch.</td>
<td>ftp server acl acl-number Optional. By default, no ACL is used to control FTP clients’ access to the switch.</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the idle-timeout timer.</td>
<td>ftp timeout minutes Optional. 30 minutes by default. Within the idle-timeout time, if there is no information interaction between the FTP server and client, the connection between them is terminated.</td>
</tr>
<tr>
<td>5.</td>
<td>Set the file update mode for the FTP server.</td>
<td>ftp update { fast</td>
</tr>
<tr>
<td>6.</td>
<td>Quit to user view.</td>
<td>quit —</td>
</tr>
<tr>
<td>7.</td>
<td>Manually release the FTP connection established with the specified username.</td>
<td>free ftp user username Optional. Available in user view.</td>
</tr>
</tbody>
</table>

Configuring authentication and authorization on the FTP server

To allow an FTP user to access certain directories on the FTP server, you must create an account for the user, authorizing access to the directories and associating the username and password with the account.

The following configuration is used when the FTP server authenticates and authorizes a local FTP user. If the FTP server needs to authenticate a remote FTP user, you must configure authentication, authorization and accounting (AAA) policy instead of the local user. For detailed configuration, see the Security Command Reference.

In local authentication, the switch checks the entered username and password against those configured on the switch. In remote authentication, the switch sends the entered username and password to the remote authentication server, which then checks whether they are consistent with those configured on the switch.

When the switch serves as the FTP server, if the client is to perform the write operations (upload, delete, create, and delete for example) on the device’s file system, the FTP login users must be level 3 users; if the client is to perform other operations, for example, read operation, the switch has no restriction on the user level of the FTP login users.
To configure authentication and authorization for FTP server:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Create a local user and enter its view.</td>
<td>local-user user-name</td>
</tr>
<tr>
<td>3.</td>
<td>Assign a password to the user.</td>
<td>password { simple</td>
</tr>
<tr>
<td>4.</td>
<td>Assign the FTP service to the user.</td>
<td>service-type ftp</td>
</tr>
<tr>
<td>5.</td>
<td>Configure user properties.</td>
<td>authorization-attribute { acl acl-number</td>
</tr>
</tbody>
</table>

**FTP server configuration example**

**Network requirements**

- As shown in Figure 15, use Device as an FTP server, and the PC as the FTP client. Their IP addresses are 1.2.1.1/16 and 1.1.1.1/16 respectively. Device and PC are reachable to each other.
- PC keeps the updated boot file of the device. Use FTP to upgrade the device and back up the configuration file.
- Set the username to ftp and the password to pwd for the FTP client to log in to the FTP server.

**Figure 15 Upgrading using the FTP server**
Procedure

⚠️ CAUTION:

The boot file used for the next startup must be saved under the root directory of the storage medium (For a device that has been partitioned, the boot file must be saved on the first partition). Copy or move a file to the root directory of the storage medium. For more information about boot-loader, see Fundamentals Command Reference.

1. Configure Device (FTP Server)

   # Create an FTP user account ftp, set its password to pwd and the user privilege level to level 3 (the manage level). Allow user ftp to access the root directory of the flash, and specify ftp to use FTP.

   `<Sysname> system-view
   [Sysname] local-user ftp
   [Sysname-luser-ftp] password simple pwd
   [Sysname-luser-ftp] authorization-attribute level 3
   [Sysname-luser-ftp] authorization-attribute work-directory flash:/
   [Sysname-luser-ftp] service-type ftp
   [Sysname-luser-ftp] quit
   # Enable FTP server.
   [Sysname] ftp server enable
   [Sysname] quit
   # Check files on your device. Remove those redundant to ensure adequate space for the boot file to be uploaded.

   `<Sysname> dir
   Directory of flash:/

   0 drw- - Dec 07 2005 10:00:57 filename
   1 drw- - Jan 02 2006 14:27:51 logfile
   2 -rw- 1216 Jan 02 2006 14:28:59 config.cfg
   3 -rw- 1216 Jan 02 2006 16:27:26 back.cfg

   515712 KB total (2511 KB free)
   `<Sysname> delete /unreserved flash:/back.cfg

2. Configure the PC (FTP Client)

   # Log in to the FTP server through FTP.

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

   # Download the configuration file config.cfg of the device to the PC for backup.

   ftp> get config.cfg back-config.cfg

   # Upload the configuration file newest.bin to Device.
ftp> put newest.bin
ftp> bye

Take the same steps to upgrade configuration file with FTP. When upgrading the configuration file with FTP, put the new file under the root directory of the storage medium.

After you finish transferring the Boot ROM program through FTP, you must run `bootrom update` to upgrade the Boot ROM.

3. Upgrade Device

   # Specify `newest.bin` as the main boot file to be used at the next startup.
   <Sysname> boot-loader file newest.bin main

   # Reboot the device and the boot file is updated at the system reboot.
   <Sysname> reboot

FTP server configuration example

Network requirements

- As shown in Figure 2, an IRF virtual device comprises a master and a subordinate FTP server. The member ID of the master is 1 and that of the subordinate switch is 2.
- The IRF virtual device serves as an FTP server, and the PC serves as an FTP client. The IRF virtual device and the PC are reachable to each other.
- The PC keeps the updated boot file of the IRF virtual device. Use FTP to upgrade the IRF virtual device and back up the configuration file.
- Set the username to `ftp` and the password to `pwd` for the FTP client to log in to the FTP server.

Figure 2 Upgrading using the FTP server
Procedure

⚠️ **CAUTION:**

- If the available memory space of the master and subordinate switches is insufficient, use `fixdisk` to clear the memory or use `delete /unreserved file-url` to delete the files not in use and then perform the following operations.
- The boot file used for the next startup must be saved under the root directory of the storage medium (For a device that has been partitioned, the boot file must be saved on the first partition). Copy or move a file to the root directory of the storage medium. For more information about `boot-loader`, see *Fundamentals Command Reference*.

1. Configure the IRF virtual device (FTP Server)

   # Create an FTP user account `ftp`, set its password to `pwd` and the user privilege level to level 3 (the manage level). Allow user `ftp` to access the root directory of the flash on the master, and specify `ftp` to use FTP.

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

   # To access the root directory of the storage medium of a subordinate switch (with the member ID 2), replace `flash:/` with `slot2#flash:/` in `authorization-attribute work-directory flash:/`.

   ```
   [Sysname-luser-ftp] service-type ftp
   [Sysname-luser-ftp] quit
   ``

2. Configure the PC (FTP Client)

   # Log in to the FTP server through FTP.

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

   # Download the configuration file `config.cfg` of the IRF virtual device to the PC for backup.

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

   # Upload the configuration file `newest.bin` to the root directory of the storage medium on the master.

   ```
   ftp> put newest.bin
   ftp> bye
   ``

   Take the same steps to upgrade configuration file with FTP. When upgrading the configuration file with FTP, put the new file under the root directory of the storage medium.

   After you finish upgrading the Boot ROM program through FTP, you must run `bootrom update` to upgrade the Boot ROM.
3. Upgrade the IRF virtual device
   
   # Copy the boot file newest.bin to the root directory of the storage medium on a subordinate switch (with the member ID 2).
   <Sysname> copy newest.bin slot2#flash:/

   # Specify newest.bin as the main boot file to be used at 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!

   # Reboot the IRF virtual device and the boot file is updated at the system reboot.
   <Sysname> reboot

Displaying and maintaining FTP

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the configuration of the FTP client.</td>
<td>display ftp client configuration [ { begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display the configuration of the FTP server.</td>
<td>display ftp-server [ { begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display detailed information about logged-in FTP users.</td>
<td>display ftp-user [ { begin</td>
<td>exclude</td>
</tr>
</tbody>
</table>
Configuring TFTP

Overview

TFTP provides functions similar to those provided by FTP, but it is less complex than FTP in interactive access interface and authentication. It is more suitable in environments where complex interaction is not needed between client and server.

TFTP uses the UDP port 69 for data transmission. For more information about TFTP basic operation, see RFC 1350.

In TFTP, file transfer is initiated by the client.
- In a normal file downloading process, the client sends a read request to the TFTP server, receives data from the server, and then sends the acknowledgement to the server.
- In a normal file uploading process, the client sends a write request to the TFTP server, sends data to the server, and receives the acknowledgement from the server.

TFTP transfers files in the following modes:
- **Binary mode**—Transfers files as raw data, like .app, .bin, and .btm files.
- **ASCII mode**—Transfers files as text, like .txt, .bat, and .cfg files.

Operation

Only the TFTP client service is available with your device.

Figure 2 TFTP configuration diagram

Before using TFTP, the administrator needs to configure IP addresses for the TFTP client and server, and make sure that there is a reachable route between the TFTP client and server.
When the device serves as the TFTP client, you must perform the following configuration:

**Table 2 Configuration when the device serves as the TFTP client**

<table>
<thead>
<tr>
<th>Device</th>
<th>Configuration</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device (TFTP client)</td>
<td>• Configure the IP address and routing function, and ensure that the route between the device and the TFTP server is available.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use <code>tftp</code> to establish a connection to the remote TFTP server to upload/download files to/from the TFTP server</td>
<td></td>
</tr>
<tr>
<td>PC (TFTP server)</td>
<td>Enable TFTP server on the PC, and configure the TFTP working directory.</td>
<td></td>
</tr>
</tbody>
</table>

**Configuring the TFTP client**

When a device acts as a TFTP client, upload a file on the device to a TFTP server and download a file from the TFTP server to the local device. Use either of the following methods to download a file:

- **Normal download**—The device writes the obtained file to the storage medium directly. In this way, if you download a remote file using a filename `destination-filename` that exists in the directory, the device deletes the original file and then saves the new one. If file download fails due to network disconnection or other reasons, the original system file will never recover because it has been deleted.

- **Secure download**—The device saves the obtained file to its memory and does not write it to the storage medium until the whole file is obtained. If you download a remote file using a filename `destination-filename` that exists in the directory, the original file is not overwritten. If file download fails due to network disconnection or other reasons, the original file still exists. This mode is more secure but consumes more memory.

HP recommends using the secure mode or, if you use the normal mode, specify a filename not existing in the current directory as the target filename when downloading the boot file or the startup configuration file.

Before using `tftp` to establish a TFTP connection, perform source address binding. Source address binding means configuring an IP address on a stable interface such as a loopback interface, and then using this IP address as the source IP address of a TFTP connection. The source address binding function simplifies the configuration of ACL rules and security policies. You just need to specify the source or destination address argument in an ACL rule as this address to filter inbound and outbound packets on the device, ignoring the difference between interface IP addresses as well as the effect of interface statuses. Configure the source address by configuring the source interface or source IP address. The primary IP address configured on the source interface is the source address of the transmitted packets.
To configure the TFTP client:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td>tftp-server [ ipv6 ] acl acl-number</td>
<td>Optional. By default, no ACL is used to control the device’s access to TFTP servers.</td>
</tr>
<tr>
<td></td>
<td>tftp client source { interface interface-type interface-number</td>
<td>A device uses the source address determined by the matched route to communicate with the TFTP server by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If no primary IP address is configured on the source interface, no TFTP connection can be established.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you use tftp client source to first configure the source interface and then the source IP address of the packets of the TFTP client, the new source IP address will overwrite the current one, and vice versa.</td>
</tr>
<tr>
<td>3.</td>
<td>quit</td>
<td>—</td>
</tr>
<tr>
<td>4.</td>
<td>display tftp client configuration [</td>
<td>Available in any view.</td>
</tr>
<tr>
<td></td>
<td>{ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>5.</td>
<td>tftp server-address { get</td>
<td>put</td>
</tr>
</tbody>
</table>

Displaying and maintaining the TFTP client

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the configuration of the TFTP client.</td>
<td>display tftp client configuration [</td>
<td>Available in any view.</td>
</tr>
<tr>
<td></td>
<td>{ begin</td>
<td>exclude</td>
</tr>
</tbody>
</table>
TFTP client configuration example

Network requirements

- As shown in Figure 3, use a PC as the TFTP server and Device as the TFTP client. Their IP addresses are 1.2.1.1/16 and 1.1.1.1/16 respectively. Device and PC are reachable to each other.
- Device downloads a boot file from PC for upgrading and uploads a configuration file named config.cfg to PC for backup.

Figure 3 Smooth upgrading using the TFTP client function

Procedure

⚠️ CAUTION:

- The boot file used for the next startup must be saved under the root directory of the storage medium.
  Copy or move a file to the root directory of the storage medium. For more information about boot-loader, see Fundamentals Command Reference.
- If the available memory space of the device is not enough, use fixdisk to clear the memory or use delete /unreserved file-url to delete the files not in use and then perform the following operations.

1. Configure the PC (TFTP Server), the configuration procedure is omitted.
   - On the PC, enable the TFTP server.
   - Configure a TFTP working directory.
2. Configure Device (TFTP Client)
   # Enter system view.
   <Sysname> system-view

   # Download application file newest.bin from PC.
   <Sysname> tftp 1.2.1.1 get 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 boot file to be used at the next startup.
   <Sysname> boot-loader file newest.bin bbb.bin main

   # Reboot the device and the software is upgraded.
   <Sysname> reboot
TFTP client configuration (IRF mode) example

Network requirements

- As shown in Figure 2, an IRF virtual device comprises a master and a subordinate switch. The member ID of the master is 1 and that of the subordinate switch is 2.
- The PC serves as a TFTP server and the IRF virtual device as a TFTP client. Their IP addresses are 1.2.1.1/16 and 1.1.1.1/16 respectively. Device and PC are reachable to each other.
- The IRF virtual device downloads a boot file from PC for upgrading and uploads a configuration file named `config.cfg` to PC for backup.

Figure 2 Smooth upgrading using the TFTP client function

Procedure

⚠️ **CAUTION:**

- If the available memory space of the master and subordinate switches is not enough, use `fixdisk` to clear the memory or use `delete /unreserved file-url` to delete the files not in use and then perform the following operations.
- The boot file used for the next startup must be saved under the root directory of the storage medium. Copy or move a file to the root directory of the storage medium. For more information about `boot-loader`, see Fundamentals Command Reference.

1. Configure the PC (TFTP Server), the configuration procedure is omitted.
   - On the PC, enable the TFTP server.
   - Configure a TFTP working directory.

2. Configure the IRF virtual device (TFTP Client)

   # Download application file `newest.bin` from PC to the master and subordinate switches.
   - Download application file `newest.bin` from PC to the root directory of the storage medium on the master.
     ```
     <Sysname> tftp 1.2.1.1 get newest.bin
     ```
   - Download application file `newest.bin` from PC to the root directory of the storage medium on a subordinate switch (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 boot file to be used at 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!

# Reboot the IRF virtual device and the software is upgraded.

   <Sysname> reboot
File management

Files such as host software and configuration files that are necessary for the operation of the device are saved in the storage media of the device. Manage files on your device through these operations: Performing directory operations, Performing file operations, Performing batch operations, Performing storage media operations, Setting prompt modes, Setting prompt modes, Setting prompt modes, Setting prompt modes, and Setting prompt modes.

Filename formats

When you specify a file, you must enter the filename in one of the following formats.

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
<th>Length</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>file-name</td>
<td>Specifies a file in the current working directory.</td>
<td>1 to 91 characters</td>
<td>a.cfg indicates a file named a.cfg in the current working directory. If the current working directory is on the master, a.cfg represents file a.cfg on the master; if the current working directory is on a subordinate, a.cfg represents file a.cfg on the subordinate.</td>
</tr>
<tr>
<td>path/file-name</td>
<td>Specifies a file in the specified folder in the current working directory. path represents the folder name. Specify multiple folders, indicating a file under a multi-level folder.</td>
<td>1 to 135 characters</td>
<td>test/a.cfg indicates a file named a.cfg in the test folder in the current working directory.</td>
</tr>
<tr>
<td>drive:/[path]/file-name</td>
<td>Specifies a file in the specified storage medium on the device. drive represents the storage medium name. The storage medium on the master is usually flash; the storage medium on a subordinate is usually slotX#flash, where X represents the member ID of the subordinate, for example slot2#flash. To view the correspondence between a device and its member ID, use display irf.</td>
<td>1 to 135 characters</td>
<td>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 read and write the a.cfg file in the root directory of the flash on a subordinate (with the member ID 2), enter slot2#flash:/a.cfg for the filename.</td>
</tr>
</tbody>
</table>

Performing directory operations

Create or remove a directory, display the current working directory, the specified directory, file information, and so on.
Displaying directory information

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display directory or file information.</td>
<td><code>dir [ /all ] [ file-url ]</code></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

Displaying the current working directory

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current working directory.</td>
<td><code>pwd</code></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

Changing the current working directory

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the current working directory.</td>
<td>`cd { directory</td>
<td>..</td>
</tr>
</tbody>
</table>

Creating a directory

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a directory.</td>
<td><code>mkdir directory</code></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

Removing a directory

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| Remove a directory.         | `rmdir directory` | Required. Available in user view. The directory to be removed must be empty. Before removing a directory delete all files and the subdirectory in it.
  • For file deletion, see the `delete` command.
  • For subdirectory deletion, see the `rmdir`. The `rmdir` command automatically deletes the files in the recycle bin in the current directory. |
Performing file operations
Display the specified directory or file information; display file contents; rename, copy, move, remove, restore, and delete files. Create a file by copying, downloading or using **save**.

### Displaying file information

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display file or directory information.</td>
<td><strong>dir [ /all ] [ file-url]</strong></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

### Displaying file contents

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the contents of a file.</td>
<td><strong>more file-url</strong></td>
<td>Required. Only a .txt file can be displayed. Available in user view.</td>
</tr>
</tbody>
</table>

### Renaming a file

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>

### Copying a file

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>

### Moving a file

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
</table>
Deleting a file

⚠️ CAUTION:
- The files in the recycle bin still occupy storage space. To delete a file in the recycle bin, run `reset recycle-bin` in the directory to which the file originally belongs. HP recommends you to empty the recycle bin periodically with `reset recycle-bin` to save storage space.
- The `delete /unreserved file-url` command deletes a file permanently and the action cannot be undone. Execution of this command equals execution of `delete file-url` and then `reset recycle-bin` in the same directory.

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move a file to the recycle bin or delete it permanently.</td>
<td><code>delete [ /unreserved ] file-url</code></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

Restoring a file from the recycle bin

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore a file from the recycle bin.</td>
<td><code>undelete file-url</code></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

Emptying the recycle bin

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter the original working directory of the file to be deleted.</td>
<td>`cd {directory</td>
<td>..</td>
</tr>
<tr>
<td>2. Delete the file in the current directory and in the recycle bin.</td>
<td><code>reset recycle-bin [ /force ]</code></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

Performing batch operations

⚠️ CAUTION:
Running 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 running the command are not satisfied, this command fails to be executed, and the system skips the command to the next one.
A batch file is a set of executable commands. Executing a batch file is the same as executing the commands in the batch file one by one.

Before executing a batch file, edit the batch file on your PC, and then download the batch file to the device. If the suffix of the file is not `.bat`, use `rename` to change the suffix to `.bat`.

To execute a batch file:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><code>system-view</code></td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td><code>execute filename</code></td>
<td>Required.</td>
</tr>
</tbody>
</table>

Performing storage media operations

Managing storage media space

⚠️ CAUTION:

When you format storage media, all files stored on it are erased and cannot be restored. If a startup configuration file exists on the storage media, formatting results in loss of the startup configuration file.

When the space of a storage medium becomes inaccessible due to abnormal operations, use `fixdisk` to restore it. The execution of the `format` command formats the storage medium, and all data on the storage medium is deleted.

To manage the space of a storage medium:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore the space of a storage medium.</td>
<td><code>fixdisk device</code></td>
<td>Optional Available in user view</td>
</tr>
<tr>
<td>Format a storage medium.</td>
<td><code>format device</code></td>
<td>Optional Available in user view</td>
</tr>
</tbody>
</table>

Displaying and maintaining the NAND flash memory

The physical space of the NAND flash memory is divided into multiple blocks, each of which is subdivided into multiple pages. The NAND flash memory is erased on a block basis and read on a page basis; the memory spaces are allocated on a page basis.

Displaying and repairing bad blocks

Bad block ratio varies with products of different vendors. The frequently used area of the memory goes bad easily. Bad blocks cannot be used to store data, and the system has to skip the bad blocks when it allocates storage spaces to files. Get the locations of bad blocks and repair them at the command line interface.
To display and repair bad blocks:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Display the number and location of bad blocks in the NAND flash memory.</td>
<td>`display nandflash badblock-location [</td>
</tr>
<tr>
<td>2.</td>
<td>Repair bad blocks.</td>
<td><code>fixdisk device</code></td>
</tr>
</tbody>
</table>

Checking files

After files are written to the NAND flash memory, use the following commands together to check the content of these files.

To check files:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the space distribution of the specified file in the NAND flash memory.</td>
<td>`display nandflash file-location filename [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display data on the specified physical page.</td>
<td>`display nandflash page-data page-value [</td>
<td>{ begin</td>
</tr>
</tbody>
</table>

Setting prompt modes

The system provides the following prompt modes:

- **alert**—The system warns about operations that may bring undesirable consequences such as file corruption or data loss.
- **quiet**—The system does not prompt confirmation for any operation.

HP recommends using the **alert** mode.

To set the operation prompt mode:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td>2.</td>
<td>Set the operation prompt mode of the file system.</td>
<td>`file prompt { alert</td>
</tr>
</tbody>
</table>
File operation example

# Display the files and the subdirectories in the current directory.
<Sysname> dir
Directory of flash:/

0  drw-         -  Feb 16 2006 11:45:36   logfile
1  -rw-      1218  Feb 16 2006 11:46:19   config.cfg
2  drw-         -  Feb 16 2006 15:20:27   test
3  -rw-    184108  Feb 16 2006 15:30:20   aaa.bin

515712 KB total (2521 KB free)

# Create a 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-         -  Feb 16 2006 15:28:14   mytest

515712 KB total (2519 KB free)

# Return to the upper directory.
<Sysname> cd ..

# Display the current working directory.
<Sysname> pwd
flash:
Configuration file management

The device provides the configuration file management function. Manage configuration files on the user-friendly command line interface (CLI).

Overview

A configuration file contains a set of commands. Save the current configuration to a configuration file so that the configuration can take effect after a device reboot. In addition, conveniently view the configuration information, or upload/download the configuration file to/from another device to configure devices in batches.

Types of configuration

The device maintains the following types of configurations: factory defaults, startup configuration, and running configuration.

Factory default

Devices are shipped with some basic settings, which are called factory defaults. These default settings ensure that a device can start up and run normally when it has no configuration file or the configuration file is damaged.

To view the factory defaults of the device, use `display default-configuration`.

Startup configuration

Use startup configuration for initialization when the device boots. If this file does not exist, the system boots using null configuration. Null configuration is the factory default configuration, which may differ from the default settings for commands. The factory default configuration may vary with device models.

View the startup configuration using either of the following methods:

- Use `display startup` to view the currently using startup configuration file, and use `more` to view the content of the configuration file.
- After the reboot of the device and before configuring the device, use `display current-configuration` to view the startup configuration.

Running configuration

The running configuration may include the startup configuration if the startup configuration has not been modified during system operation. It also includes any new configurations added during system operation. The running configuration is stored in the temporary storage media of the device, and is removed if not saved when the device reboots.

Use `display current-configuration` to view the current validated configuration of the device.
Configuration file format and content

A configuration file is saved as a text file; the following rules apply:

- Only non-default configuration settings are saved.
- Commands in a configuration file are listed in sections by views, usually in the order of system view, interface view, routing protocol view, and user interface view. Sections are separated with one or multiple blank lines or comment lines that start with a pound sign #.
- A configuration file ends with a return.

Coexistence of multiple configuration files

The device can save multiple configuration files on its storage media. Save the configurations used in different networking environments as different configuration files. When the device moves between networking environments, specify the configuration file as the startup configuration file to be used at the next startup of the device and then restart the device. Multiple configuration files allow the device to adapt to a network rapidly, saving the configuration workload.

A device starts up using only one configuration file. However, specify two startup configuration files, main startup configuration file and backup startup configuration file to be used at the next startup of the device as needed when the device has main and backup configuration files. The device starts up using the main startup configuration file. If the main startup configuration file is corrupted or lost, the device starts up using the backup startup configuration file. Devices supporting main and backup startup configuration files are more secure and reliable.

At a moment, the switch has at most one main startup configuration file and one backup startup configuration file. Specify neither of the two files (displayed as NULL).

Specify main and backup startup configuration files to be used at the next startup of the device using one of the following methods:

- Specify them when saving the running configuration. For more information, see Saving the running configuration.
- Specify them when specifying the startup configuration file to be used at the next system startup. For more information, see
Specifying a startup configuration file to be used at the next system startup.

Startup with the configuration file

The device takes the following steps when it starts up:

1. If the main startup configuration file you specified exists, the device starts up with this configuration file.
2. If the main startup configuration file you specified does not exist but the backup startup configuration file exists, the device starts up with the backup startup configuration file.
3. If neither the main nor the backup startup configuration file exists, the device starts up with null configuration.

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.

To save the current configuration:

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling configuration file auto-save</td>
<td>Optional</td>
</tr>
<tr>
<td>Selecting save mode for the configuration</td>
<td>Required</td>
</tr>
</tbody>
</table>

Enabling configuration file auto-save

- With the configuration file auto-save function enabled, when you save the current configuration by executing `save [ safely ] [ backup | main ] [ force ]` or executing `save filename all` and then pressing `Enter`, the master and a subordinate automatically save the current configuration to the specified configuration file, and use the file as the configuration file to be used at the next startup, keeping the consistency of the configuration files on the master and the subordinate.

- If the configuration file auto-save function is not enabled, when you save the current configuration by executing `save [ safely ] [ backup | main ]` or executing `save filename all` and then pressing `Enter`:
  - Only the master will automatically save the current configuration to the specified configuration file.
  - Using the file as the configuration file for the next startup; the subordinate switches will neither save the configuration file nor configure the file for the next startup.

To configure the configuration file auto-save function:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enter system view.</td>
<td><code>system-view</code></td>
<td>—</td>
</tr>
</tbody>
</table>

Selecting save mode for the configuration file

- **Fast saving mode**—This is the mode when using `save` without the `safely` keyword. The file saves more quickly but is likely to lose the existing configuration file if the device reboots or the power fails during the process.
• **Safe mode**—This is the mode when using `save` with the `safely` keyword. The file saves more slowly but can retain the configuration file in the device even if the device reboots or the power fails during the process.

The fast saving mode is suitable for environments where the power supply is stable. The safe mode is preferred in environments where a stable power supply is unavailable or remote maintenance is involved.
To save the current configuration:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Save the current configuration to the specified file, but the configuration file is not set as the file to be used at the next startup.</td>
<td>save file-url [ all</td>
</tr>
<tr>
<td>2.</td>
<td>Save the current configuration to the root directories of the storage media of all member devices and specify the file as the startup configuration file to be used at the next system startup.</td>
<td>save [ safely ] [ backup</td>
</tr>
</tbody>
</table>

The configuration file must be with extension .cfg.

Whether save [ safely ] [ backup | main ] [ force ] or save filename all command+Enter takes effect on all member devices or on the master only depends on whether the configuration file auto-save function is enabled. For the configuration file auto-save function, see Enabling configuration file auto-save.

Executing save [ safely ] and save [ safely ] main has the same effect: The system will save the current configuration and specify the configuration file as the main startup configuration file to be used at the next system startup.

During the execution of save [ backup | main ], the startup configuration file to be used at the next system startup may be lost if the device reboots or the power supply fails. In this case, the device will boot with the null configuration, and after the device reboots, you will need to re-specify a startup configuration file for the next system startup (see
Specifying a startup configuration file to be used at the next system startup.

Setting configuration rollback

Configuration rollback allows you to revert to a previous configuration state based on a specified configuration file. The specified configuration file must be a valid .cfg file generated by using either the backup function (manually or automatically) or save.

If a configuration file is generated by another device, the configuration file must comply with the format of the configuration file on the current device. HP recommends using the configuration file that is generated by using the backup function (manually or automatically).

Configuration rollback can be applied in the following situations:
- Running configuration error. Rolling back the running configuration to a correct one is needed.
- The application environment has changed and the device has to run in a configuration state based on a previous configuration file without being rebooted.

Before setting configuration rollback, perform the following steps:
1. Specify the filename prefix and path for saving the running configuration.
2. Save the running configuration with the specified filename (filename prefix + serial number) to the specified path. The running configuration can be saved automatically or manually.

When you enter configuration replace file the system compares the running configuration and the specified replacement configuration file. The configuration replace file command performs the following actions:
- Preserves all commands present in both the replacement configuration file and the running configuration.
- Removes commands from the running configuration that are not present in the replacement configuration file.
- Applies the commands from the replacement configuration file that are not present in the running configuration.
- Applies the commands from the replacement configuration file that have different configurations in the running configuration.

The running configuration is only saved to the master, and only the configuration on the master can be rolled back. However, the related configuration is synchronized to the subordinate switches to ensure the rollback of the configuration after the master is changed.

Configuration task list

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring parameters for saving the running configuration</td>
<td>Required</td>
</tr>
<tr>
<td>Enabling automatic saving of the running configuration</td>
<td>Required</td>
</tr>
<tr>
<td>Manually saving the running configuration</td>
<td>Use either approach</td>
</tr>
<tr>
<td>Setting configuration rollback</td>
<td>Required</td>
</tr>
</tbody>
</table>
Configuring parameters for saving the running configuration

Before the running configuration is saved manually or automatically, the file path and filename prefix must be configured. After that, the system saves the running configuration with the specified filename (filename prefix_serial number.cfg) to the specified path. The filename of a saved configuration file is like 20080620archive_1.cfg, or 20080620archive_2.cfg. The saved configuration files are numbered automatically, from 1 to 1,000 (with an increment of 1). If the serial number reaches 1,000, it restarts from 1. If you change the path or filename prefix, or reboot the device, the saved file serial number restarts from 1, and the system recounts the saved configuration files. If you change the path of the saved configuration files, the files in the original path become common configuration files, and are not processed as saved configuration files, and are not displayed when you view saved configuration files.

The number of saved configuration files has an upper limit. After the maximum number of files is saved, the system deletes the oldest files when the next configuration file is saved.
To configure parameters for saving the running configuration:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the path and filename prefix for saving configuration files.</td>
<td>archive configuration location directory filename-prefix filename-prefix Required. By default, the path and filename for saving configuration files are not configured, and the system does not save the configuration file at a specified interval.</td>
</tr>
<tr>
<td>3.</td>
<td>Set the maximum number of configuration files that can be saved.</td>
<td>archive configuration max file-number Optional. The default number is 5.</td>
</tr>
</tbody>
</table>

Only execute saving and rollback operations on the master. To make the configuration rollback take effect on the new master after an active/standby switchover, execute `archive configuration location` to specify the path and filename prefix of the saved configuration file on both the master and subordinate switches. Before the execution of this command, ensure that the specified path is available on both the master and the subordinate switches, and that the path does not include any member ID.

If `undo archive configuration location` is executed, the running configuration cannot be saved either manually or automatically, and the configuration is restored to the default by executing `archive configuration interval` and `archive configuration max`, meanwhile, the saved configuration files are cleared.

The value of the `file-number` argument is determined by memory space. Set a comparatively small value for the `file-number` argument if the available memory space is small.

**Enabling automatic saving of the running configuration**

Configure the system to save the running configuration at a specified interval, and use `display archive configuration` to view the filenames and save time of the saved configuration files. This enables you to easily roll back the current configuration to a previous configuration state.

Configure an automatic save interval based on the storage media’s performance and the frequency of configuration modification using the following guidelines:

If the configuration of the device does not change frequently, manually save the running configuration as needed.

To enable automatic saving of the running configuration:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the automatic saving of the running configuration, and set the interval.</td>
<td>archive configuration interval minutes Optional. Disabled by default. The path and filename prefix for saving configuration files must be specified before you configure the automatic saving period.</td>
</tr>
</tbody>
</table>
Manually saving the running configuration

Automatic saving of the running configuration occupies system resources, and frequent can saving greatly affect system performance. If the system configuration does not change frequently, disable the automatic saving of the running configuration and save it manually.

In addition, automatic saving of the running configuration is performed periodically, while manual saving can immediately save the running configuration. Before performing complicated configuration, manually save the running configuration so that the device can revert to the previous state if and when the configuration fails.

To manually save the running configuration:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually save the running configuration.</td>
<td>archive configuration</td>
<td>Required Available in user view. Specify the path and filename prefix of a save configuration file before you manually save the running configuration; otherwise, the operation fails.</td>
</tr>
</tbody>
</table>

Setting configuration rollback

⚠️ CAUTION:
Do not reboot an IRF member device during configuration rollback. Configuration rollback may fail if one of the following situations is present (if a command cannot be rolled back, the system skips it and processes the next one):

- The complete undo form of a command is not supported. You cannot get the actual undo form of the command by simply putting the keyword undo in front of the command, so the complete undo form of the command cannot be recognized by the device.
- The configuration cannot be removed, such as hardware-related commands
- Commands in different views are dependent on each other
- If the replacement configuration file is not a complete file generated by using save or archive configuration, or the file is copied from a different type of device, the configuration cannot be rolled back. Ensure that the replacement configuration file is correct and compatible with the current device.
- The configuration file specified with configuration replace file filename can only be a configuration file in simple text. Otherwise, errors may occur in configuration rollback.

To set configuration rollback:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Set configuration rollback.</td>
<td>configuration replace file filename Required.</td>
</tr>
</tbody>
</table>
Specifying a startup configuration file to be used at the next system startup

⚠️ CAUTION:
A configuration file must use .cfg as its extension name and the startup configuration file must be saved in the root directory of the storage media.

To specify a startup configuration file to be used at the next system startup, use the following guidelines:

- Use `save`. If you save the running configuration to the specified configuration file in the interactive mode, the system automatically sets the file as the main startup configuration file to be used at the next system startup.
- Use the command dedicated to specify a startup configuration file to be used at the next startup, which is described in the following table:

To specify a startup configuration file to be used at the next startup:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify a startup configuration file to be used at the next system startup of all member devices.</td>
<td><code>startup saved-configuration cfgfile [backup main]</code></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

Backing up the startup configuration file

The backup function allows you to copy the startup configuration file to be used at the next startup from the device to the TFTP server.

The backup operation backs up the main startup configuration file to the TFTP server for devices supporting main and backup startup configuration files.

Before the backup operation:

- Ensure that the server is reachable and enabled with TFTP service, and the client has the read and write permission.
- Use `display startup` command (in user view) to check whether you have specified a startup configuration file to be used at the next startup. If the file is set as NULL or does not exist, the backup operation fails.

To back up the startup configuration file to be used at the next startup:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up the startup configuration file to be used at the next startup to the specified TFTP server.</td>
<td><code>backup startup-configuration to dest-addr [dest-filename ]</code></td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>
Deleting a startup configuration file to be used at the next startup

⚠️ CAUTION:

This command permanently deletes startup configuration files to be used at the next startup from all member devices. Use it with caution.

Delete a startup configuration file to be used at the next startup at the CLI. On a device that has main and backup startup configuration files, you can choose to delete the main, the backup, or both. If the device has only one startup configuration to be used at the next startup, the system only sets the startup configuration file to NULL.

You may need to delete a startup configuration file to be used at the next startup for one of the following reasons:

- After you upgrade system software, the existing startup configuration files do not match the new system software.
- Startup configuration files are corrupted (often caused by loading a wrong configuration file).

With startup configuration files deleted, the devices uses null configuration at the next startup.

To delete a startup configuration file to be used at the next startup:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete a startup configuration file to be</td>
<td>reset saved-configuration</td>
<td>Required.</td>
</tr>
<tr>
<td>used at the next startup from the storage</td>
<td>[ backup</td>
<td>main ]</td>
</tr>
<tr>
<td>media.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Restoring a startup configuration file

The restore function allows you to copy a configuration file from a TFTP server to the root directory of the storage media of all member devices and specify the file as the startup configuration file to be used at the next startup.

Before restoring a configuration file, ensure that the server is reachable, the server is enabled with TFTP service, and the client has read and write permission.

To restore a startup configuration file to be used at the next startup:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore a startup configuration file to be</td>
<td>restore startup-</td>
<td>Required.</td>
</tr>
<tr>
<td>used at the next startup.</td>
<td>configuration from src-addr src-filename</td>
<td>Available in user view.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>After execution of the command, use display startup to verify that the filename of the configuration file to be used at the next system startup is the same with that specified by the filename argument.</td>
</tr>
</tbody>
</table>
## Displaying and maintaining a configuration file

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the information about configuration rollback.</td>
<td>display archive configuration [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display the factory defaults of the device.</td>
<td>display default-configuration [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display the current validated configurations of the device.</td>
<td>display current-configuration [ [ configuration</td>
<td>configuration ]</td>
</tr>
<tr>
<td>Display the running configuration file saved on the storage media of the device.</td>
<td>display saved-configuration [ by-linenum ] [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display the configuration files used at this and the next system startup.</td>
<td>display startup [</td>
<td>{ begin</td>
</tr>
<tr>
<td>Display the valid configuration under the current view.</td>
<td>display this [ by-linenum ] [</td>
<td>{ begin</td>
</tr>
</tbody>
</table>
Configuring software upgrade

Overview

Device software includes the Boot ROM program and the system boot file. After powered on, the device runs the Boot ROM program, initializes the hardware, and displays the hardware information. Then the device runs the boot file. The boot file provides drivers and adaption for hardware, and implements service features. The Boot ROM program and system boot file are required for the startup and running of a device.

Figure 2 Relationship between the Boot ROM program and the system boot file

1. Start
2. Boot ROM runs
3. Press Ctrl+B
4. Yes
   - Enter Boot ROM menu to upgrade the Boot ROM program or boot file
5. No
   - Run boot file
6. Enter CLI
7. Finish
8. Select the Reboot option to reboot the device
Software upgrade methods

The Boot ROM program and system boot file can both be upgraded at the Boot ROM menu or at the CLI. The following sections describe upgrading through command lines. For instructions about how to upgrade through the Boot ROM menu, see the release notes of your switch.

Upgrading at the CLI falls into the following categories:

<table>
<thead>
<tr>
<th>Upgrade method</th>
<th>Upgrade object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrading the boot ROM program through a system reboot</td>
<td>Boot ROM program</td>
<td>• You must reboot the whole system to upgrade the software of a device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• This causes running service interruption during the upgrade process, and is not recommended.</td>
</tr>
<tr>
<td>Upgrading the boot file through a system reboot</td>
<td>System boot file</td>
<td></td>
</tr>
<tr>
<td>Upgrading IRF member switch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software upgrade by installing hotfixes</td>
<td>System boot file</td>
<td>• Hotfix is a fast, cost-effective method to repair software defects of a device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Compared with software version upgrade, hotfix can upgrade the software without interrupting the running services of the device. It can repair the software defects of the current version without rebooting the device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The patch files match the device model and software version. If they are not matched, the hotfixing operation fails.</td>
</tr>
<tr>
<td>ISSU</td>
<td>System boot file</td>
<td>• In-Service Software Upgrade (ISSU) enables software upgrade and ensures continues packet forwarding.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For more information, see ISSU configuration in the <em>Fundamentals Configuration Guide</em></td>
</tr>
</tbody>
</table>
## Upgrading the boot ROM program through a system reboot

### CAUTION:

To execute the **bootrom** command successfully, save the Boot ROM file in the root directory of the storage media on a member device.

To upgrade the Boot ROM program:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong> —&lt;br&gt;Optional. By default, the validity check function is enabled at the time of upgrading Boot ROM. The Boot ROM programs of member devices vary with devices, so users are easily confused when upgrading the Boot ROM. With the validity check function enabled, the device can strictly check the Boot ROM upgrade files for correctness and the version configuration information to ensure a successful upgrade.</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the validity check function when upgrading the Boot ROM.</td>
<td><strong>bootrom-update security-check enable</strong> —&lt;br&gt;The Boot ROM programs of member devices vary with devices, so users are easily confused when upgrading the Boot ROM. With the validity check function enabled, the device can strictly check the Boot ROM upgrade files for correctness and the version configuration information to ensure a successful upgrade.</td>
</tr>
<tr>
<td>3.</td>
<td>Return to user view.</td>
<td><strong>quit</strong> —&lt;br&gt;Required. For more information about FTP or TFTP, see Fundamentals Configuration Guide.</td>
</tr>
<tr>
<td>4.</td>
<td>Save the Boot ROM program to the root directory of the Flash of the master device by using FTP, TFTP, or other approaches.</td>
<td>—&lt;br&gt;Required. For more information about FTP or TFTP, see Fundamentals Configuration Guide.</td>
</tr>
<tr>
<td>5.</td>
<td>Upgrade the Boot ROM program on member devices.</td>
<td><strong>bootrom update file file-url slot slot-number-list</strong> Required.&lt;br&gt;Available in user view.</td>
</tr>
<tr>
<td>6.</td>
<td>Reboot a specified member switch or the IRF virtual device.</td>
<td><strong>reboot [ slot slot-number ]</strong> The <strong>slot</strong> keyword specifies a switch by its member ID of the IRF virtual device. If the keyword is not provided, the IRF virtual device will reboot. Available in user view.</td>
</tr>
</tbody>
</table>
Upgrading the boot file through a system reboot

⚠️ CAUTION:

- You must save the file to be used at the next device boot in the root directory of the device. Copy or move a file to change the path of it to the root directory.
- To run `boot-loader` successfully, save the file to be used at the next device boot in the root directory of the storage media on a member device.
- You cannot specify the boot file to be used at the next boot of the USB device.
- The names of the files to be used at the next boot of the master and subordinate switches may be different, but the versions of the files must be the same; otherwise, a subordinate switch reboots by using the master’s boot file and joins the IRF virtual device again.

To upgrade the boot file through a system reboot:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Save the boot file to the root directory of the Flash of the master device by using FTP, TFTP, or other approaches.</td>
<td>Required. For more information about FTP or TFTP, see Fundamentals Configuration Guide.</td>
</tr>
<tr>
<td>2.</td>
<td>Copy the new boot file to the root directory of the storage media of the subordinate switch.</td>
<td>Required. Available in user view.</td>
</tr>
<tr>
<td>3.</td>
<td>Specify a boot file to be used at the next boot of a member device.</td>
<td>Required. Available in user view.</td>
</tr>
<tr>
<td>4.</td>
<td>Reboot a specified member switch or the IRF virtual device.</td>
<td>Available in user view.</td>
</tr>
</tbody>
</table>
Upgrading IRF member switch boot file

⚠️ CAUTION:

If the free Flash space on the member switch is not enough when you upgrade the boot file of an IRF member switch, the system automatically compares the sum of the space occupied by the current boot file and the remaining space with the size of the new boot file:

- If the sum is greater than the size of the new boot file, the member switch automatically deletes the current boot file to release the space.
- If the sum is smaller than the size of the new boot file, the member switch prompts you that the upgrade fails.

Before upgrading the boot file of IRF member switches, be sure that the free Flash space of the member switch is enough to store the new boot file.

The system can automatically copy a boot file saved on the Flash of the master of an IRF virtual device to a specified member switch or all member switches, and specify the boot file as the boot file to be used at the next boot of the member switches. This feature simplifies the upgrade steps and improves management efficiency.

To upgrade the boot file:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Save the boot file to the root directory of the Flash of the master device by using FTP, TFTP, or other approaches.</td>
<td>Required. For more information about FTP or TFTP, see Fundamentals Configuration Guide.</td>
</tr>
<tr>
<td>2.</td>
<td>Specify a boot file to be used at the next boot of a member device or all member devices of an IRF virtual device</td>
<td>Required. Available in user view.</td>
</tr>
<tr>
<td>3.</td>
<td>Reboot a member switch or all member switches</td>
<td>Required. The slot keyword specifies a switch by its member ID of the IRF virtual device. If the keyword is not provided, all member switches will reboot. Available in user view.</td>
</tr>
</tbody>
</table>
Software upgrade by installing hotfixes

A hotfix is a fast, cost-effective method to repair the software defects of a device. Compared with other methods of software version upgrade, a hotfix can upgrade the software without interrupting the running services of the device. It can repair software defects of the current version without rebooting the device.

Patch and patch file

A patch, also called "patch unit," is a package to fix software defects. Patches are usually released as patch files.

A patch file may contain one or more patches for different defects. After loaded from the storage media to the memory patch area, each patch is assigned a unique number, which starts from 1, for identification, management and operation. For example, if a patch file has three patch units, they are numbered as 1, 2, and 3 respectively.

Patch types

The patch type only affects the patch loading process.

- **Common patches**—Those formally released through the version release flow. Common patches always include the functions of the previous temporary patches so as to replace them.
- **Temporary patches**—Those not formally released through the version release flow, but temporarily provided to solve the emergent problems. The system deletes all temporary patches before it loads the common patch.
- **Incremental patch**—Those dependent on the previous patch units. For example, if a patch file has three patch units, patch 3 can be run only after patch 1 and 2 take effect. You cannot run patch 3 separately. Currently released patches are all incremental patches.

Patch status

Each patch has its status, which can be switched only by commands. The relationship between patch state changes and command actions is shown in Figure 3.

The patch can be in the state of IDLE, DEACTIVE, ACTIVE, and RUNNING.

Load, run temporarily, confirm running, stop running, delete, install, and uninstall represent operations, corresponding to commands of **patch load**, **patch active**, **patch run**, **patch deactive**, **patch delete**, **patch install**, and **undo patch install**. For example, if you run **patch active** command for the patches in the DEACTIVE state, the patches turn to the ACTIVE state.

Information about patch states is saved in the file patchstate on the Flash. Do not to operate this file.
**IDLE state**

Patches in the IDLE state are not loaded. You cannot install or run the patches, as shown in Figure 4 (suppose the memory patch area can load up to eight patches). The memory patch area supports up to 200 patches.

**Figure 4 Patches are not loaded to the memory patch area**
**DEACTIVE state**

Patches in the DEACTIVE state have been loaded to the memory patch area but have not run in the system yet. Suppose that the patch file to be loaded has seven patches. After the seven patches successfully pass the version check and CRC check, they are loaded to the memory patch area and are in the DEACTIVE state. At this time, the patch states in the system are as shown in Figure 5.

Figure 5 A patch file is loaded to the memory patch area

![Figure 5](image)

**ACTIVE state**

Patches in the ACTIVE state are those that have run temporarily in the system and become DEACTIVE after system reboot. For the seven patches in Figure 5, if you activate the first five patches, their states change from DEACTIVE to ACTIVE. At this time, the patch states in the system are as shown in Figure 6.

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

Figure 6 Patches are activated

![Figure 6](image)
RUNNING state

After you confirm the running of the ACTIVE patches, the patch state becomes RUNNING and they are placed in the RUNNING state after system reboot. For the five patches in Figure 6, if you confirm running the first three patches, their states change from ACTIVE to RUNNING. At this time, the patch states of the system are as shown in Figure 7.

The patches that are in the RUNNING state are still in the RUNNING state after system reboot.

Figure 7 Patches are running

---

Configuration prerequisites

Patches are released per device model. Before patching the system, you must save the appropriate patch files to the storage media of the device using FTP or TFTP. When saving the patch files, the following rules apply:

- The patch files match the device model and software version. If they are not matched, the hotfixing operation fails.
- Name a patch file properly. Otherwise, the system cannot locate the patch file and the hotfixing operation fails. The name is in the format of “patch_PATCH-FLAG suffix.bin.” The PATCH-FLAG is pre-defined and support for the PATCH-FLAG depends on device model. The first three characters of the version item (using display patch information) represent the PATCH-FLAG suffix. The system searches the root directory of the storage medium (Flash by default) for patch files based on the PATCH-FLAG. If there is a match, the system loads patches to or install them on the memory patch area.

Loading and installation are performed on all member devices of an IRF virtual device. Before performing these operations, save the same patch files to the root directories in the storage media of all member devices.

The following table describes the default patch name for 5820X&5800 Switch Series.

<table>
<thead>
<tr>
<th>Device</th>
<th>PATCH-FLAG</th>
<th>Default patch name</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP 5820X&amp;5800 Switch Series</td>
<td>PATCH-MPU</td>
<td>patch_mpu.bin</td>
</tr>
<tr>
<td></td>
<td>PATCH-LPU</td>
<td>patch_lpu.bin</td>
</tr>
</tbody>
</table>
One-step patch installation

To install patches in one step, use `patch install`. After you execute the command, the system displays the message “Do you want to continue running patches after reboot? [Y/N]:”

- Entering Y: All specified patches are installed, and turn to the RUNNING state from IDLE. This equals execution of the commands `patch location`, `patch load`, `patch active`, and `patch run`. The patches remain RUNNING after system reboot.

- Entering N: All specified patches are installed and turn to the ACTIVE state from IDLE. This equals execution of the commands `patch location`, `patch load` and `patch active`. The patches turn to the DEACTIVE state after system reboot.

The patch matches the device type and software version.

To install the patches in one step:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Install the patches in one step.</td>
<td><code>patch install patch-location</code></td>
</tr>
</tbody>
</table>

Step-by-step patch installation

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the patch file location.</td>
<td><code>patch location patch-location</code></td>
</tr>
<tr>
<td>3.</td>
<td>Load the patch file on from the storage medium to the specified memory patch area.</td>
<td><code>patch load slot slot-number</code></td>
</tr>
</tbody>
</table>
| 4.   | Activate the specified patches. | `patch active patch-number slot slot-number` | Required.  
- After activation, the patch takes effect and is in the test-run stage. After the device is reset or rebooted, the patch becomes invalid.  
- If an ACTIVE patch has a problem, reboot the device to deactivate the patch and avoid a series of running faults resulting from patch error. |
| 5.   | Confirm the running of the specified patches. | `patch run patch-number [ slot slot-number ]` | Required. After you confirm the running of a patch, the patch state becomes RUNNING, and the patch is in the normal running stage. After the device is reset or rebooted, the patch is still valid. |

Set the file transfer mode to binary mode before using FTP or TFTP to upload/download patch files to/from the Flash of the device. Otherwise, patch file cannot be parsed properly.
This operation applies to patches in the ACTIVE state only.

**Step-by-step patch uninstallation**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Stop running the specified patches.</td>
<td>patch deactive patch-number slot slot-number Required. When you stop running a patch, the patch state becomes DEACTIVE, and the system runs in the way before it is installed with the patch.</td>
</tr>
<tr>
<td>3.</td>
<td>Delete the specified patches from the memory patch area.</td>
<td>patch delete patch-number slot slot-number Required. Deleting patches only removes the patches from the memory patch area, and does not delete them from the storage medium. The patches turn to IDLE state after this operation. After a patch is deleted, the system runs in the way before it is installed with the patch.</td>
</tr>
</tbody>
</table>

**Displaying and maintaining the software upgrade**

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about the boot file.</td>
<td>display boot-loader [ slot slot-number ] [ ] { begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display the patch information.</td>
<td>display patch information [ ] { begin</td>
<td>exclude</td>
</tr>
</tbody>
</table>

**Software upgrade configuration examples**

**Immediate upgrade configuration example**

**Network requirement**

- As shown in Figure 8, the IRF virtual device comprises two member devices, the master with the member ID of 1 and the subordinate switch with the member ID of 2.
- The current software version is **soft-version1** for the IRF virtual device. Upgrade the software version of the IRF virtual device to **soft-version2** and configuration file to **new-config**.
- The latest application **soft-version2.bin** and the latest configuration file **new-config.cfg** are both saved on the TFTP server.
- The IP address of the IRF virtual device is 1.1.1.1/24, the IP address of the TFTP server is 2.2.2.2/24, and the TFTP server and IRF virtual device can reach each other.
Figure 8 Network diagram for immediate upgrade

The line in orange represents the IRF link.

Procedure

1. Configuration on the TFTP server (Configurations may vary with different types of servers)
   Obtain the boot file and configuration file through legitimate channels, such as the official HP website, agents, and technical staff. Save these files under the working path of the TFTP server for the TFTP client access.

2. Configuration on the members of the IRF virtual device
   # Download file new-config.cfg on the TFTP server to the master (Configurations may vary with different types of servers).
   ```
   <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 file 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 file soft-version2.bin on the TFTP server to the master and 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 file `new-config.cfg` as the configuration file to be used at the next boot of all members of the IRF virtual device.

```plaintext
<IRF> startup saved-configuration new-config.cfg main
Please wait ...
Setting the master board ...
... Done!
Setting the slave board ...
Slot 1:
  Set next configuration file successfully.
Slot 0:
  Set next configuration file successfully.
Slot 1:
  Set next configuration file successfully.
```

# Specify file `soft-version2.bin` as the boot file to be used at the next boot of all members of the IRF virtual device.

```plaintext
<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 device. The software version is upgraded now.

```plaintext
<IRF> reboot
```

To check if the upgrade is successful after the device reboots, use `display version`.

**Hotfix configuration example**

**Network requirements**

- The IRF virtual device in this example comprises two member devices, the master and subordinate switch. The software running on the member devices are of some problem, and hotfixing is needed.
- The patch file `patch_mpu.bin` and `patch_lpu.bin` is saved on the TFTP server.
- The IP address of the IRF virtual device is 1.1.1.1/24, and IP address of the TFTP server is 2.2.2.2/24. The IRF virtual device and TFTP server can reach each other.

**Figure 2 Network diagram for configuring hotfix**

![Network diagram](image)

*Note: The orange line indicates the IRF link.*
Procedure

⚠️ CAUTION:
Make sure the free Flash space of the device is big enough to store the patch files.

1. Configure the TFTP server. The configuration varies depending on server type, and the configuration procedure is omitted.
   - Enable the TFTP server function.
   - Save the patch file patch_mpu.bin and patch_lpu.bin to the directory of TFTP server.
2. Configure the device.
   # Before upgrading the software, use save command to save the current system configuration. The configuration procedure is omitted.
   # Load the patch file patch_mpu.bin and patch_lpu.bin from the TFTP server to the root directory of the master’s storage medium.
     <Device> tftp 2.2.2.2 get patch_mpu.bin
     <Device> tftp 2.2.2.2 get patch_lpu.bin
   # Load the patch file patch_mpu.bin and patch_lpu.bin from the TFTP server to the root directory of the subordinate switch’s storage medium.
     <Device> tftp 2.2.2.2 get patch_mpu.bin slot2#flash:/patch_mpu.bin
     <Device> tftp 2.2.2.2 get patch_lpu.bin slot2#flash:/patch_lpu.bin
   # Install the patch.
     <Device> system-view
     [Device] 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........
     Installation completed, and patches will continue to run after reboot.
ISSU enables software upgrade and ensures continuous packet forwarding.

As shown in Figure 2, to ensure high availability for user networks, cross-device link aggregation is configured on the IRF member switches at the distribution layer so that 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, use ISSU to upgrade the boot file 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 2 IRF network diagram*
ISSU process

ISSU follows a strict procedure, as shown in Figure 2.

**Figure 3 ISSU flow chart**

Do not modify the current configuration, plug or unplug cables connected to IRF ports, or delete or modify the boot file during ISSU. Otherwise, an upgrade failure may occur.

To upgrade the boot files of IRF member switches through ISSU, the member switches must form a ring topology.
ISSU states

During the ISSU process, use display issu state to view the ISSU state of the IRF virtual device, including whether the new boot file is compatible with the current boot file, and the adopted ISSU method.

Table 2 ISSU state description

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

Boot file version rollback

The HP 5820X & 5800 switch series support version rollback during ISSU. When ISSU fails to proceed on an IRF member switch (for example, the new boot file is broken), use this feature to revert the boot file to the previous version.

The HP 5820X & 5800 switch series support the following version rollback methods.

Automatic rollback

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

- **Compatible ISSU method**—If you do not run issu accept on the specified subordinate switch or you do not run issu commit on any other member switch before the rollback timer expires, the system automatically stops the ISSU upgrade and rolls back the boot file of the upgraded IRF member switches to the previous version.

- **Incompatible ISSU method**—If you do not run issu run switchover to upgrade all IRF member switches that have not been upgraded in one operation before the rollback timer expires, the system automatically rolls back the boot file of all upgraded IRF member switches to the previous version.

For information about compatible and incompatible ISSU methods, see Enabling version compatibility check.

Manual rollback

Use issu rollback to roll back the boot file of an IRF member switch to the previous version. Whether manual rollback can be configured for an IRF member switch depends on the ISSU state. For more information, see Table 1.
Configuring ISSU

Configuration task list

<table>
<thead>
<tr>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Download the new boot file to the Flash of all IRF member switches.</td>
<td>Required</td>
</tr>
<tr>
<td>Prerequisites for performing ISSU.</td>
<td>Required</td>
</tr>
<tr>
<td>Enabling version compatibility check.</td>
<td>Required</td>
</tr>
<tr>
<td>Configuring ISSU.</td>
<td>Required</td>
</tr>
<tr>
<td>Use either approach</td>
<td>Use either approach</td>
</tr>
<tr>
<td>Configuring the ISSU version rollback timer.</td>
<td>Optional</td>
</tr>
<tr>
<td>Displaying and maintaining ISSU.</td>
<td>Optional</td>
</tr>
</tbody>
</table>

Prerequisites for performing ISSU

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Save the current configuration.</td>
<td>save</td>
<td>Required. Before performing ISSU, make sure that the current configuration of the IRF virtual device has been saved to the configuration file.</td>
</tr>
<tr>
<td>Display the running status of each IRF member switch.</td>
<td>display device</td>
<td>Required. Before performing ISSU, make sure that all member switches of the IRF virtual device are in the normal state.</td>
</tr>
<tr>
<td>Display the boot file information.</td>
<td>display boot-loader</td>
<td>Required. Before performing an ISSU upgrade, make sure that the boot file of all IRF member switches is identical, which means the boot file version, name, and directory are the same.</td>
</tr>
<tr>
<td>Display the roles of IRF member switches.</td>
<td>display irf</td>
<td>Required.</td>
</tr>
<tr>
<td>Display information about the files in the Flash.</td>
<td>dir</td>
<td>Required. Before performing an ISSU upgrade, make sure that the new and current boot files exist in the Flash of each IRF member switch, and they are saved in the same directory.</td>
</tr>
</tbody>
</table>
Enabling version compatibility check

Before performing an ISSU upgrade, you must check the version compatibility between the new and current boot files, to determine whether ISSU can be performed, and which ISSU method is adopted.

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

- **Compatible**—The running boot file is compatible with the new boot file. Use the compatible ISSU method to upgrade the boot file of the IRF virtual device. For more information, see Configuring compatible ISSU.

- **Incompatible**—The current running boot file is incompatible with the new boot file. Use the incompatible ISSU method to upgrade the boot file of the IRF virtual device. For more information, see
Configuring incompatible ISSU.

- **Unknown**—The current and new boot files have big differences, or the current boot file does not support ISSU. You cannot upgrade the boot file through ISSU.

To enable version compatibility check:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enters system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Check whether the new boot file is compatible with the current boot file.</td>
<td>display version comp-matrix file upgrading-filename</td>
</tr>
</tbody>
</table>

**Configuring ISSU**

**Configuring compatible ISSU**

⚠️ **CAUTION:**

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

Use `display version comp-matrix file upgrading-filename` to view the versions of the new and current boot files. If the new boot file is compatible with the current boot file, perform a compatible ISSU.

The roles of some IRF member switches change after an ISSU upgrade.
To configure compatible ISSU:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Upgrade the specified subordinate switch (the new master after the upgrade).</td>
<td>issu load file upgrading-filename slot slot-number</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>slot-number is the member ID of the subordinate switch.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The specified subordinate switch reboots with the new boot file when this command is executed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perform the next operation after the subordinate switch is rebooted.</td>
</tr>
<tr>
<td>3.</td>
<td>Reboot the master current manually.</td>
<td>issu run switchover slot slot-number</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>With this command executed:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The master reboots with the current boot file, and becomes a subordinate switch after reboot.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The subordinate switches of the IRF virtual device perform master election. The winner (the subordinate switch specified with issu load) becomes the new master.</td>
</tr>
<tr>
<td></td>
<td>IMPORTANT:</td>
<td>• The slot-number provided in this command must be the same as that specified in the issu load.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Perform the next operation after the reboot process is completed.</td>
</tr>
<tr>
<td>4.</td>
<td>Accept the ISSU.</td>
<td>issu accept slot slot-number</td>
</tr>
<tr>
<td></td>
<td>Optional</td>
<td>By default, the rollback timer is 45 minutes. If you do not run issu accept on the specified subordinate switch or you do not run 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.</td>
</tr>
<tr>
<td></td>
<td>IMPORTANT:</td>
<td>• The slot-number argument provided in this command must be the same as that specified in the issu load.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When this command is executed, the rollback timer becomes invalid, which means the boot file cannot be automatically rolled back.</td>
</tr>
<tr>
<td>5.</td>
<td>Upgrade an IRF member switch that has not been upgraded.</td>
<td>issu commit slot slot-number</td>
</tr>
<tr>
<td></td>
<td>Required</td>
<td>• This command upgrades one IRF member switch at a time. If the IRF virtual device has three or more than three member switches, repeat this command to upgrade them one by one.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When all IRF member switches reboot with the new boot file, the ISSU process completes.</td>
</tr>
<tr>
<td></td>
<td>After executing issu commit, you cannot roll back the current boot file version BB to former version AA. To do so, use the AA version boot file as the new boot file version to perform another ISSU for the IRF virtual device.</td>
<td></td>
</tr>
</tbody>
</table>
## Configuring incompatible ISSU

Use `display version comp-matrix file upgrading-filename` to view the versions of the new and current boot files. If they are incompatible, perform an incompatible ISSU.

To configure incompatible ISSU:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enters system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Upgrade the specified subordinate switch (the new master after the upgrade).</td>
<td><code>issu load file upgrading-filename slot slot-number force</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Upgrade all IRF member switches that have not been upgraded in one operation.</td>
<td><code>issu run switchover slot slot-number</code></td>
</tr>
</tbody>
</table>

## Configuring the ISSU version rollback timer

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enters system view.</td>
<td><code>system-view</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Configure the rollback timer.</td>
<td><code>issu rollback-timer minutes</code></td>
</tr>
</tbody>
</table>
Performing manual version rollback

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enters system view.</td>
<td>system-view —</td>
</tr>
<tr>
<td>2.</td>
<td>Perform a manual version rollback.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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

Displaying and maintaining ISSU

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information about the rollback timer.</td>
<td>display issu rollback-timer</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display the ISSU state.</td>
<td>display issu state</td>
<td>Available in any view</td>
</tr>
<tr>
<td>Display version compatibility information.</td>
<td>display version comp-matrix [ file upgrading-filename ]</td>
<td>Available in any view</td>
</tr>
</tbody>
</table>

ISSU configuration example

Current network status and requirements analysis

Current network status

1. As shown in Figure 2, access layer switches Switch A, Switch B, and Switch C connect to user networks.
2. Distribution layer switches Switch D, Switch E, and Switch form an IRF virtual switch. The member ID of the master is 1, and those of the subordinate switches are 2 and 3 respectively.
3. To ensure high availability, configure cross-device link aggregation using the following guidelines so that 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 virtual switch, 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 virtual switch.
   - On Switch B, create aggregation group 2 that corresponds to aggregation group 2 on the IRF virtual switch.
• On Switch C, create aggregation group 3 that corresponds to aggregation group 3 on the IRF virtual switch.

Network requirements

You must upgrade the boot files of the IRF member switches and ensure packet forwarding for user network using the following guidelines:

• The current boot file on each IRF member switch is **soft-version1.bin**. The new boot file **soft-version2.bin** is saved on the TFTP server. You must perform remote ISSU for the IRF virtual switch.

• The IP address of the IRF virtual switch is 1.1.1.1/24, and that of the TFTP server is 2.2.2.2/24. The IRF virtual switch and the TFTP server can reach each other.

Network diagram

**Figure 2 Network diagram**
1. Configuration on the IRF virtual switch

  # 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
2. **Configuration on 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. **Configuration on 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. **Configuration on Switch C**

   # Create dynamic aggregate interface 3.

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

```plaintext
[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
```

**Configuration on the TFTP server**

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

**ISSU upgrade preparation**

**Download boot file 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:/
```

**Check all IRF member switches before the ISSU upgrade**

⚠️ **CAUTION:**

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

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      Ver.B   NULL    003     201        IVL    MAIN       Normal
Slot 2
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      28      Ver.B   NULL    003     201        IVL    MAIN       Normal
Slot 3
SubSNo PortNum PCBVer FPGAVer CPLDVer BootRomVer AddrLM Type       State
0      28      Ver.B   NULL    003     201        IVL    MAIN       Normal
```

The output shows that the state of all IRF member switches is normal.
2. Check whether the current boot files 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 boot 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 that the following information:
   - The member ID and the priority of the master is 1 and 10 respectively
   - The member ID and the priority of one subordinate switch is 2 and 9 respectively
   - The member ID and the priority of the other subordinate switch is 3 and 1 respectively

   During the ISSU upgrade process, you must select subordinate switch 2 as the specified subordinate switch.
4. Check whether the new boot file has been saved in the Flash of each IRF member switch. If not, the ISSU upgrade cannot be performed.

# Verify that the new boot file `soft-version2.bin` has been saved to the Flash of the master.

<IRF> dir flash:

```
Directory of flash:

0  -rw-  6085  May 29 2010 11:38:45  config.cfg
1  -rw-  10518 Apr 26 2000 12:45:05  logfile.log
2  -rw-  43836748 Apr 26 2000 14:24:11 soft-version1.bin
3  -rw-  43836956 Apr 26 2000 14:13:46 soft-version2.bin
4  drw-         -  Apr 26 2000 12:00:33  seclog
5  -rw-       287  Apr 26 2000 12:19:52  system.xml
```

515712 KB total (425956 KB free)

The output shows that the new boot file has been saved to the Flash of the master.

# Verify that the new boot file `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 2000 12:45:05  logfile.log
2  -rw-  43836748 Apr 26 2000 14:24:11 soft-version1.bin
3  -rw-  43836956 Apr 26 2000 14:13:46 soft-version2.bin
4  drw-         -  Apr 26 2000 12:00:33  seclog
5  -rw-       287  Apr 26 2000 12:19:52  system.xml
```

515712 KB total (425956 KB free)

The output shows that the new boot file has been saved to the Flash of subordinate switch 2.

# Verify that the new boot file `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 2000 12:45:05  logfile.log
2  -rw-  43836748 Apr 26 2000 14:24:11 soft-version1.bin
3  -rw-  43836956 Apr 26 2000 14:13:46 soft-version2.bin
4  drw-         -  Apr 26 2000 12:00:33  seclog
5  -rw-       287  Apr 26 2000 12:19:52  system.xml
```

515712 KB total (425956 KB free)

The output shows that the new boot file 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.

View the compatibility information between the new and current boot files

# Check whether the current and new boot files are compatible.
<IRF> display version comp-matrix file soft-version2.bin

1. If they are compatible, the following output is displayed (The output of this command varies with devices.):
   Number of Matrices in Table = 1
   Matrix for HP A5800-24G-PoE+ Switch

   Running Version: R1211
   Version Compatibility List:
   A1210 (Compatible)

   The output shows that the new and current versions are fully compatible. Use the compatible ISSU upgrade method. For more information, see “Performing compatible ISSU upgrade.”

2. If the two versions are incompatible, the following output is displayed (The output of this command varies with devices.):
   Number of Matrices in Table = 1
   Matrix for HP A5800-24G-PoE+ Switch

   Running Version: R1211
   Version Compatibility List:
   A1202 (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.

```bash
<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 boot file of salve switch 2 is `soft-version2.bin`.

```bash
[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 boot file of subordinate switch 2 is `soft-version2.bin`.

# Reboot the master manually.

```bash
[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 virtual switch. 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.

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

# Upgrade switches 1 and 3 respectively.

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

```bash
[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 boot files of all IRF member switches have been upgraded to the new version.
# Verify that the current boot files 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 chassis to master. Continue? [Y/N]: y
  
  Then, the ISSU upgrade process completes and the boot files of all IRF member switches have been upgraded to the new version.
# Verify that the current boot files 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:
```
Configuring device management

The configuration tasks in this document are independent. Perform these tasks as needed in any order.

Overview

The device management function allows you to view the current working state of a device, configure running parameters, and perform daily device maintenance and management.

Configuring the device name

The device name is used to identify a device in a network. In the system, the device name is the same as the prompt of the CLI. For example, if the device name is **Sysname**, the prompt of user view is `<Sysname>`.

To configure the device name:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the device name.</td>
<td>sysname sysname</td>
</tr>
</tbody>
</table>

Configuring the system clock

The system clock, displayed by the system timestamp, is determined by configured relative time, time zone, and daylight saving time. To view the system clock, use `display clock`.

To configure the system clock:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Set time and date.</td>
<td>clock datetime time date</td>
</tr>
<tr>
<td>2.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>3.</td>
<td>Set the time zone.</td>
<td>clock timezone zone-name { add</td>
</tr>
<tr>
<td>4.</td>
<td>Set a daylight saving time scheme.</td>
<td>clock summer-time zone-name one-off start-time start-date end-time end-date add-time</td>
</tr>
</tbody>
</table>
Displaying the system clock

The system clock is determined by `clock datetime`, `clock timezone` and `clock summer-time`. If these three commands are not configured, `display clock` displays the original system clock. If you combine these three commands in different ways, the system clock is displayed in the ways as shown in Table 2. The following describes the meanings of the parameters in the configuration column:

- 1 indicates date-time has been configured with `clock datetime`.
- 2 indicates time-zone has been configured with `clock timezone` and the offset time is `zone-offset`.
- 3 indicates daylight saving time has been configured with `clock summer-time` and the offset time is `summer-offset`.
- [1] indicates `clock datetime` is an optional configuration.
- The default system clock is 2005/1/1 1:00:00 in the example.

**Table 2 System clock configuration**

<table>
<thead>
<tr>
<th>Configuration</th>
<th>System clock configured</th>
<th>Example</th>
</tr>
</thead>
</table>
| 1             | `date-time`             | Configure: `clock datetime` 1:00 2007/1/1
|               |                         | System clock configured: 01:00:00
|               |                         | UTC Mon 01/01/2007 |
| 2             | The original system clock ± “zone-offset” | Configure: `clock timezone` zone-time add 1
|               |                         | System clock configured: 02:00:00
|               |                         | zone-time Sat 01/01/2005 |
| 1 and 2       | `date-time ± zone-offset` | Configure: `clock datetime` 2:00 2007/2/2 and `clock timezone` zone-time add 1
|               |                         | System clock configured: 03:00:00
|               |                         | zone-time Fri 02/02/2007 |
| [1], 2 and 1  | `date-time`             | Configure: `clock timezone` zone-time add 1 and `clock datetime` 3:00 2007/3/3
|               |                         | System clock configured: 03:00:00
|               |                         | zone-time Sat 03/03/2007 |
| 3             | If the original system clock is not in the daylight saving time range, the system clock configured is the original system clock. | Configure: `clock summer-time` ss one-off 1:00 2006/1/1 1:00 2006/8/8 2
|               |                         | System clock configured: 01:00:00
<p>|               |                         | UTC Sat 01/01/2005 |</p>
<table>
<thead>
<tr>
<th>Configuration</th>
<th>System clock configured</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the original system clock is in the daylight saving time range, the system clock configured is the original system clock + “summer-offset.”</td>
<td>Configure: clock summer-time ss one-off 00:30 2005/1/1 1:00 2005/8/8 2</td>
<td>System clock configured:: 03:00:00 ss Sat 01/01/2005</td>
</tr>
<tr>
<td>If &quot;date-time&quot; is not in the daylight saving time range, the system clock configured is &quot;date-time.&quot;</td>
<td>Configure: clock datetime 1:00 2007/1/1 and clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2</td>
<td>System clock configured:: 01:00:00 UTC Mon 01/01/2007</td>
</tr>
<tr>
<td>If “date-time” is in the daylight saving time range, the system clock configured is “date-time” + “summer-offset.”</td>
<td>Configure: clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 and clock datetime 1:00 2007/1/1</td>
<td>System clock configured:: 03:00:00 ss Mon 01/01/2007</td>
</tr>
<tr>
<td>If “date-time” is not in the daylight saving time range, the system clock configured is “date-time.”</td>
<td>Configure: clock datetime 8:00 2007/1/1 and clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2</td>
<td>System clock configured:: 10:00:00 ss Mon 01/01/2007</td>
</tr>
<tr>
<td>If “date-time” is in the daylight saving time range, the system clock configured is “date-time.”</td>
<td>Configure: clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 and clock datetime 1:00 2007/1/1</td>
<td>System clock configured:: 01:00:00 UTC Tue 01/01/2008</td>
</tr>
<tr>
<td>“date-time” is in the daylight saving time range: If the value of “date-time” - “summer-offset” is not in the summer-time range, the system clock configured is “date-time” - “summer-offset”; If the value of “date-time” - “summer-offset” is in the summer-time range, the system clock configured is “date-time.”</td>
<td>Configure: clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 and clock datetime 1:30 2007/1/1</td>
<td>System clock configured:: 23:30:00 UTC Sun 12/31/2006</td>
</tr>
<tr>
<td>[1], 3 and 1</td>
<td>Configure: clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 and clock datetime 3:00 2007/1/1</td>
<td>System clock configured:: 03:00:00 ss Mon 01/01/2007</td>
</tr>
<tr>
<td>Configuration</td>
<td>System clock configured</td>
<td>Example</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>2 and 3 or 3 and 2</td>
<td>If the value of the original system clock ± “zone-offset” is not in the summer-time range, the system clock configured is the original system clock ± “zone-offset.”</td>
<td>Configure: clock timezone zone-time add 1 and clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 System clock configured: 02:00:00 zone-time Sat 01/01/2005</td>
</tr>
<tr>
<td></td>
<td>If the value of the original system clock ± “zone-offset” is in the summer-time range, the system clock configured is the original system clock ± “zone-offset” + “summer-offset.”</td>
<td>Configure: clock timezone zone-time add 1 and 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</td>
</tr>
<tr>
<td>1, 2 and 3 or 1, 3 and 2</td>
<td>If the value of “date-time” ± “zone-offset” is not in the summer-time range, the system clock configured is “date-time” ± “zone-offset.”</td>
<td>Configure: clock datetime 1:00 2007/1/1, clock timezone zone-time add 1 and clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 System clock configured: 02:00:00 zone-time Mon 01/01/2007</td>
</tr>
<tr>
<td></td>
<td>If the value of “date-time” ± “zone-offset” is in the summer-time range, the system clock configured is “date-time” ± “zone-offset” + “summer-offset.”</td>
<td>Configure: clock datetime 1:00 2007/1/1, clock timezone zone-time add 1 and clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 System clock configured: 04:00:00 ss Mon 01/01/2007</td>
</tr>
<tr>
<td></td>
<td>If “date-time” is not in the daylight saving time range, the system clock configured is “date-time.”</td>
<td>Configure: clock timezone zone-time add 1, clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 and clock datetime 1:00 2007/1/1 System clock configured: 01:00:00 zone-time Mon 01/01/2007</td>
</tr>
<tr>
<td>[1], 2, 3 and 1 or [1], 3, 2 and 1</td>
<td>“date-time” is in the daylight saving time range: If the value of “date-time” ± “summer-offset” is not in the summer-time range, the system clock configured is “date-time” ± “summer-offset”; If the value of “date-time” ± “summer-offset” is in the summer-time range, the system clock configured is “date-time.”</td>
<td>Configure: clock timezone zone-time add 1, clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 and clock datetime 1:30 2008/1/1 System clock configured: 23:30:00 zone-time Mon 12/31/2007</td>
</tr>
<tr>
<td></td>
<td>“date-time” is in the daylight saving time range:</td>
<td>Configure: clock timezone zone-time add 1, clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 and clock datetime 3:00 2008/1/1 System clock configured: 03:00:00 ss Tue 01/01/2008</td>
</tr>
</tbody>
</table>

160
Enabling the display of copyright information

With the display of copyright information enabled, the copyright information is displayed when a user logs in through Telnet or SSH, or when a user quits user view after logging in to the device through the console port. The copyright information is not displayed under other circumstances. The display format of copyright information is shown below:

******************************************************************************
* Copyright (c) 2010-2011 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                 *
* no decompiling or reverse-engineering shall be allowed.                    *
******************************************************************************

With the display of copyright information disabled, the copyright information is never displayed.

To enable the display of copyright information:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Enable the display of copyright information.</td>
<td>copyright-info enable</td>
</tr>
</tbody>
</table>

Configuring banners

Banners are prompt information displayed by the system when users are connected to the device, perform login authentication, and start interactive configuration. The administrator can set corresponding banners as needed.

The system supports the following types of banners.

- **shell**—Also called “session banner,” displayed when a non TTY Modem user enters user view.
- **incoming**—Also called “user interface banner,” displayed when a user interface is activated by a Modem user.
- **login**—Welcome information displayed when password or scheme authentication is configured.
- **motd**—Welcome information displayed before authentication.
- **legal**—Also called “license information.” The system displays some copyright or license information, and then displays the **legal** banner before a user logs in, waiting for the user to confirm whether to continue the authentication or login. If entering **Y** or pressing the **Enter** key, the user enters the authentication or login process. If entering **N**, the user quits the authentication or login process. **Y** and **N** are case insensitive.
Input modes

The system supports single-line input mode and multiple-line input mode for configuration a banner.

Single-line input

In single-line input mode, all banner information comes after the command keywords in the same line. The start and end characters of the entered text must be the same but are not part of the banner information. In this case, the entered text, together with the command keywords, cannot exceed 510 characters.

Multiple-line input

In multiple-line input mode, all banner information is entered in multiple lines by pressing the Enter key. In this case, up to 2000 characters can be entered.

Multi-line input mode can be achieved in the following methods:

- **Method I**—Press the Enter key directly after the command keywords, enter the banner information, and finish your setting with the % character. The Enter and % characters are not part of the banner information.

- **Method II**—Enter a character after the command keywords at the first line, and then press the Enter key. Enter the banner information, and finish your setting with the character you enter at the first line. The character at the first line and the end character are not part of the banner information.

- **Method III**—Enter multiple characters after the command keywords at the first line—with the first and last characters being different, and then press the Enter key. Enter the banner information, and finish your setting with the first character you enter at the first line. The first entered character at the first line and the end character are not part of the banner information.

To configure a banner:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the banner to be displayed at login—available for Modem login users.</td>
<td>header incoming text</td>
</tr>
<tr>
<td>3.</td>
<td>Configure the banner to be displayed at login authentication.</td>
<td>header login text</td>
</tr>
<tr>
<td>4.</td>
<td>Configure the authorization information before login.</td>
<td>header legal text</td>
</tr>
<tr>
<td>5.</td>
<td>Configure the banner to be displayed when a user enters user view—available for non Modem login users.</td>
<td>header shell text</td>
</tr>
<tr>
<td>6.</td>
<td>Configure the banner to be displayed before login.</td>
<td>header motd text</td>
</tr>
</tbody>
</table>

Banner configuration example

# Configure the banner to be displayed when a user enters user view as Welcome to HP!

- Single-line input mode:

  ```
  <System> system-view
  [System] header shell %Welcome to HP!%
  ```
• Multiple-line input mode (method I):
  <System> system-view
  [System] header shell
  Please input banner content, and quit with the character '%'.
  Welcome to HP!
  %

• Multiple-line input mode (method II):
  <System> system-view
  [System] header shell W
  Please input banner content, and quit with the character 'W'.
  Welcome to HP!
  W

Configuring the exception handling method

When the system detects any software abnormality, it handles the situation with one of the following methods:

• **reboot**—The system recovers itself through automatic reboot.
• **maintain**—The system stays in the current state. Therefore, you must manually recover the system, such as reboot the system. Sometimes, it is difficult for the system to recover, or some prompts that are printed during the failure are lost after the reboot. In this case, use this method to keep the abnormal state and troubleshoot the problem.

To configure exception handling method:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td>system-view</td>
</tr>
<tr>
<td>2.</td>
<td>Configure exception handling method on all member devices.</td>
<td>system-failure { maintain</td>
</tr>
</tbody>
</table>

Optional:
By default, all member devices adopt the reboot method to handle exceptions.
With this command configured, all member devices adopt the same method to handle exceptions.

Rebooting the device

⚠️ CAUTION:

• Device reboot can result in interruption of ongoing services. Use these commands with caution.
• Before rebooting the device, use save to save the current configurations. For more information, see Fundamentals Command Reference.

When a fault occurs to a running device, reboot the device with any of the following methods to remove the fault:

• **Method I**—Power on the device after powering it off, which is also called hard reboot or cold start. This method impacts the device a lot. Powering off a running device will cause data loss and hardware damages. It is not recommended.
- **Method II**—Trigger the immediate reboot at the CLI.
- **Method III**—Enable the scheduled reboot function at the CLI. Set a time at which the device can automatically reboot, or set a delay so that the device can automatically reboot within the delay.

The last two methods are command line operations. Reboot through command lines is also called hot start, which is mainly used to reboot a device in remote maintenance without performing hardware reboot of the device.

To reboot a device:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot a member device, or all member</td>
<td><code>reboot [ slot slot-number ]</code></td>
<td>Required.</td>
</tr>
<tr>
<td>devices immediately.</td>
<td></td>
<td>The <code>slot</code> keyword specifies a member device.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If no slot is specified, the command</td>
</tr>
<tr>
<td></td>
<td></td>
<td>reboots all member devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available in user view.</td>
</tr>
</tbody>
</table>

Before rebooting the device, use `display startup` and `display boot-loader` (see Fundamentals Command Reference).

The precision of the rebooting timer is 1 minute. One minute before the rebooting time, the device prompts “REBOOT IN ONE MINUTE” and reboots in one minute.

- When you run `reboot` on the master of an IRF virtual device:
  - If you specify the `slot` keyword, the member device with the specified number reboots.
  - If you do not specify the `slot` keyword, all member devices of the IRF virtual device reboot.

If a main boot file fails or does not exist, the device cannot be rebooted with `reboot`. In this case, re-specify a main boot file to reboot the device, or power off the device, and then power it on. The system automatically uses the backup boot file to restart the device.

If you are performing file operations when the device is rebooted, the system does not execute the command for the sake of security.

To enable the scheduled reboot function:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the scheduled reboot function of</td>
<td>`schedule reboot at hh:mm [</td>
<td>Required.</td>
</tr>
<tr>
<td>all member devices and specify a</td>
<td>date ]`</td>
<td>Use either approach.</td>
</tr>
<tr>
<td>specific reboot time and date.</td>
<td></td>
<td>The scheduled reboot function is disabled by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Available in user view.</td>
</tr>
<tr>
<td>Enable the scheduled reboot function of</td>
<td>`schedule reboot delay {</td>
<td></td>
</tr>
<tr>
<td>all member devices and specify a</td>
<td>hh:mm</td>
<td>mm }</td>
</tr>
<tr>
<td>reboot waiting time.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Configuring scheduled tasks

A scheduled task defines a command or a group of commands and when such commands are to be executed. It allows a device to execute specified commands at a time when no person is available to maintain the device.

With a scheduled task configured, the device checks the configured task list every minute. If the device detects that the time to execute a command is reached, it automatically executes the command.

There are two approaches to configure a scheduled task. The following table compares the two approaches.

<table>
<thead>
<tr>
<th>Comparison item</th>
<th>Configuring a scheduled task—Approach 1</th>
<th>Configuring a scheduled task—Approach 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applicable range</td>
<td>Small</td>
<td>Large</td>
</tr>
<tr>
<td>Configuration</td>
<td>Simple</td>
<td>Complex</td>
</tr>
<tr>
<td></td>
<td>Only <strong>schedule job</strong> is involved.</td>
<td>The <strong>job</strong>, <strong>view</strong>, and <strong>time</strong> commands are involved.</td>
</tr>
<tr>
<td>Can multiple scheduled tasks be configured?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can a task contain multiple commands?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>If you use <strong>schedule job</strong> repeatedly, only the last configuration takes effect.</td>
<td>Use <strong>time</strong> in <strong>job view</strong> to configure commands to be executed at different time points.</td>
</tr>
<tr>
<td>Supported views</td>
<td>User view and system view. In the <strong>schedule job</strong>, shell represents user view, and system represents system view.</td>
<td>All views. In <strong>time</strong>, <strong>monitor</strong> represents user view.</td>
</tr>
<tr>
<td>Supported commands</td>
<td>Commands in user view and system view</td>
<td>Commands in all views</td>
</tr>
<tr>
<td>Can a task be repeatedly executed?</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Can a task be saved?</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The system does not check whether entered view and command arguments are correct. You must ensure their correctness. Otherwise, the commands cannot be executed.

The system does not require your confirmation when it is executing a scheduled task. If there is information for you to confirm, the system automatically enters Y or Yes. If characters are required, the system automatically enters a default character string, or enters an empty character string when there is no default character string.

Execution of any command that changes the user interface (such as **telnet**, **ftp**, or **ssh2**), the view (such as **system-view** or **quit**), or the user status (such as **super**) in a scheduled task does not change, the configuration interface, view, and current user status.

When the specified time is reached, the system executes the specified command in the background without displaying any prompt information except system information such as log, trap and debugging information.

Configuring a scheduled task—Approach 1
### Configuring a scheduled task—Approach 2

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view.</td>
<td><strong>system-view</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Create a scheduled task and enter job view.</td>
<td><strong>job job-name</strong> Required.</td>
</tr>
<tr>
<td>3.</td>
<td>Specify the view in which the task is executed.</td>
<td><strong>view view-name</strong> Required. Specify only one view for a task.</td>
</tr>
<tr>
<td>4.</td>
<td>Configure a command to be executed at a specific time.</td>
<td><strong>time time-id at time command</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>**time time-id { one-off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>date month-day</td>
</tr>
<tr>
<td></td>
<td></td>
<td>week-daylist</td>
</tr>
<tr>
<td></td>
<td></td>
<td>command</td>
</tr>
<tr>
<td>5.</td>
<td>Configure a command to be executed after a delay time.</td>
<td>**time time-id { one-off</td>
</tr>
</tbody>
</table>

Only one view can be specified for a task, which means all commands in the task are executed in the same specified view. If different views are specified by executing **view view-name** repeatedly, only the last configuration takes effect.

The view must be supported by the system and the view name must be complete instead of an abbreviation. Most commonly used view names include: **monitor** (user view), **system** (system view), **GigabitEthernetx/x/x** (Ethernet interface view), and **Vlan-interfacex** (VLAN interface view).

A scheduled task can contain up to 10 commands. If you want more than 10 commands to be executed, configure them in different tasks.

A **time-id** uniquely identifies the binding between a command and its execution time. If two time-ids are the same, the one configured later is effective.
Configuring the fan ventilation direction

Some switch models accommodate two fan trays to provide good ventilation. The two fan trays must be the same model. Two fan models are available for the switch. One model has air flow from the port side to the PSU side. The other model has air flow from the PSU side to the port side.

Manually configure the fan ventilation direction for the switch (the default direction is **power-to-port**). The two fan trays must have the same ventilation direction as the switch.

If one fan tray or both the two fan trays have a different ventilation direction from the switch, the system outputs trap and log information for you to replace the wrong ones.

To configure the fan ventilation direction:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. system-view</td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the fan ventilation direction for the switch. fan prefer-direction slot slot-number { power-to-port</td>
<td>port-to-power }</td>
</tr>
</tbody>
</table>

Configuring the 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 down before the detection timer times out, the device automatically brings up the port.

To configure the detection timer:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enter system view. system-view</td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td>Configure the detection timer. shutdown-interval time</td>
<td>Optional. The detection interval is 30 seconds by default.</td>
</tr>
</tbody>
</table>

Configuring temperature alarm thresholds for a member device

The switch sends traps when the temperature of a sensor crosses the lower or upper temperature threshold. Change the temperature threshold settings for the switch as needed so remove the alarm condition in time.

- If the temperature is lower than the lower limit, the device logs the event and outputs the log information and trap information for users.
- If the temperature reaches the warning threshold, the device logs the event and outputs the log information and trap information for users.
If the temperature reaches the alarming threshold, the device not only repeatedly outputs the log information and trap information in the terminal display, but also alerts users through the LED on the device panel.

To configure temperature alarm thresholds for a member device:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>system-view</td>
<td>—</td>
</tr>
<tr>
<td>2.</td>
<td>temperature-limit slot slot-number hotspot sensor- number lowerlimit warninglimit [alarmlimit]</td>
<td>Optional. By default, the temperature alarm thresholds follow the specifications listed in Table 2. The warning and alarming thresholds must be higher than the lower temperature limit. The alarming threshold must be higher than the warning threshold.</td>
</tr>
</tbody>
</table>

Table 3 Temperature alarm thresholds for a device

<table>
<thead>
<tr>
<th>Device</th>
<th>Sensor</th>
<th>Lower limit</th>
<th>Warning limit</th>
<th>Alarm limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>5820X-14XG-SFP+ Switch with 2 Interface Slots(JC106A)/5820X-14XG-SFP+ TAA Switch with 2 Interface Slots(JG259A)</td>
<td>1 2</td>
<td>5 10</td>
<td>70 90</td>
<td>80 100</td>
</tr>
<tr>
<td>5820X-24XG-SFP+ Switch(JC102A)/5820X-24XG-SFP+ TAA-compliant Switch (JG243A)</td>
<td>1 2 3</td>
<td>10 -10 10</td>
<td>80 125 90</td>
<td>87 135 100</td>
</tr>
<tr>
<td>5820AF-24XG Switch(JG219A)</td>
<td>1 4</td>
<td>0 0</td>
<td>67 61</td>
<td>72 66</td>
</tr>
<tr>
<td>5800-48G-PoE+ Switch with 2 Interface Slots(JC101A)/5800-48G-PoE+ TAA Switch with 2 Interface Slots(JG242A)</td>
<td>1 2 3</td>
<td>5 -10 10</td>
<td>70 125 90</td>
<td>80 135 100</td>
</tr>
<tr>
<td>5800-24G-PoE+ Switch(JC099A)/5800-24G-PoE+ TAA Switch(JG254A)</td>
<td>1 2</td>
<td>5 -10</td>
<td>70 125</td>
<td>80 135</td>
</tr>
<tr>
<td>5800-24G Switch(JC100A)/5800-24G TAA Switch(JG255A)</td>
<td>1 2</td>
<td>5 -10</td>
<td>70 125</td>
<td>80 135</td>
</tr>
<tr>
<td>5800-24G-SFP Switch with 1 Interface Slot(JC103A)/5800-24G-SFP TAA Switch with 1 Interface Slot(JG256A)</td>
<td>1 2</td>
<td>5 -10</td>
<td>65 125</td>
<td>75 135</td>
</tr>
</tbody>
</table>
Clearing the 16-bit interface indexes not used in the current system

△ **CAUTION:**

A confirmation is required when you execute this command. If you fail to make a confirmation within 30 seconds or enter N to cancel the operation, the command will not be executed.

The network management software requires devices to provide uniform and stable 16-bit interface indexes. That is, a one-to-one relationship should be kept between an interface’s name and the interface’s index on the same device.

For this purpose, the system will save the 16-bit index for an interface after the card where the interface resides or the logical interface is removed.

If you repeatedly insert and remove different subcards/interface cards or create/delete a large number of logical interfaces, the interface indexes are used up, and new interfaces cannot be created. To solve this problem, clear all 16-bit interface indexes saved but not used in the current system in user view.

After the clearing operation,

- A re-created interface’s index might not be consistent with the original index.
- Existing interfaces’ indexes remain unchanged.

To clear the 16-bit interface indexes not used in the current system:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear the 16-bit interface indexes saved but not in use in the current systems of all member devices.</td>
<td>reset unused porttag</td>
<td>Required. Available in user view.</td>
</tr>
</tbody>
</table>

Identifying and diagnosing pluggable transceivers

**Table 3** lists the available pluggable transceivers. They can be further divided into optical transceivers and electrical transceivers based on transmission medium.

**Table 4 Commonly used pluggable transceivers**

<table>
<thead>
<tr>
<th>Transceiver type</th>
<th>Application environment</th>
<th>Whether can be an optical transceiver</th>
<th>Whether can be an electrical transceiver</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP (Small Form-factor Pluggable)</td>
<td>Generally used for 100M/1000M Ethernet interfaces or POS 155M/622M/2.5G interfaces</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Identifying pluggable transceivers

Pluggable transceivers might be of various types and from different vendors. Use the following commands to view the key parameters of the pluggable transceivers, including transceiver type, connector type, central wavelength of the laser sent, transfer distance and vendor name to identify the pluggable transceivers.

To identify pluggable transceivers:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display key parameters of the pluggable transceivers.</td>
<td><code>display transceiver interface [interface-type interface-number]</code></td>
<td></td>
</tr>
<tr>
<td>Display the electrical label information of the pluggable transceivers.</td>
<td><code>display transceiver manuinfo interface [interface-type interface-number]</code></td>
<td>Electrical label information is also called permanent configuration data or archive information, which is written to the storage component of a transceiver during debugging or testing. The information includes transceiver name, device serial number, and vendor name.</td>
</tr>
</tbody>
</table>

### Diagnosing pluggable transceivers

The system outputs alarm information for diagnosing and troubleshooting pluggable transceivers faults. The digital diagnosis function monitors the key parameters of a transceiver, such as temperature, voltage, laser bias current, TX power, and RX power. When these parameters are abnormal, take measures to prevent transceiver faults.

To diagnose pluggable transceivers:

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the current alarm information of the pluggable transceivers.</td>
<td><code>display transceiver alarm interface [interface-type interface-number]</code></td>
<td></td>
</tr>
<tr>
<td>Display the currently measured value of the digital diagnosis parameters of the pluggable transceivers.</td>
<td><code>display transceiver diagnosis interface [interface-type interface-number]</code></td>
<td></td>
</tr>
</tbody>
</table>
## Displaying and maintaining device management configuration

<table>
<thead>
<tr>
<th>Task</th>
<th>Command</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the system version information.</td>
<td>display version</td>
<td>begin</td>
</tr>
<tr>
<td>Display the system clock information.</td>
<td>display clock</td>
<td>begin</td>
</tr>
<tr>
<td>Display or save the operation statistics of multiple functional modules.</td>
<td>display diagnostic-information</td>
<td>begin</td>
</tr>
<tr>
<td>Display CPU usage statistics.</td>
<td>display cpu-usage</td>
<td>slot</td>
</tr>
<tr>
<td>Display CPU usage history statistics in a chart.</td>
<td>display cpu-usage history</td>
<td>task</td>
</tr>
<tr>
<td>Display information about subcard, USB or hardware on the device.</td>
<td>display device</td>
<td>usb</td>
</tr>
<tr>
<td>Display device electrical label information.</td>
<td>display device manuinfo</td>
<td>slot</td>
</tr>
<tr>
<td>Display device temperature information.</td>
<td>display environment</td>
<td>slot</td>
</tr>
<tr>
<td>Display device fan operating state.</td>
<td>display fan</td>
<td>slot</td>
</tr>
<tr>
<td>Display device memory usage.</td>
<td>display memory</td>
<td>slot</td>
</tr>
<tr>
<td>Display device power state.</td>
<td>display power</td>
<td>slot</td>
</tr>
<tr>
<td>Task</td>
<td>Command</td>
<td>Remarks</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>--------------------------------</td>
</tr>
<tr>
<td>Display RPS state.</td>
<td>`display rps [ slot slot-number { rps-id } ] [</td>
<td>Available in any view</td>
</tr>
<tr>
<td></td>
<td>{ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display device reboot mode.</td>
<td>`display reboot-type [ slot slot-number ] [</td>
<td>Available in any view</td>
</tr>
<tr>
<td></td>
<td>{ begin</td>
<td>exclude</td>
</tr>
<tr>
<td>Display scheduled task configuration</td>
<td>`display schedule job [ [ begin</td>
<td>Available in any view</td>
</tr>
<tr>
<td>(configured by <code>schedule job</code>)</td>
<td>exclude</td>
<td>include } regular-expression ]</td>
</tr>
<tr>
<td>Display device reboot time.</td>
<td>`display schedule reboot [ [ begin</td>
<td>Available in any view</td>
</tr>
<tr>
<td></td>
<td>exclude</td>
<td>include } regular-expression ]</td>
</tr>
<tr>
<td>Display schedule task configuration</td>
<td>`display job [ job-name ] [ [ begin</td>
<td>Available in any view</td>
</tr>
<tr>
<td>(configured by <code>job</code>)</td>
<td>exclude</td>
<td>include } regular-expression ]</td>
</tr>
<tr>
<td>Display the exception handling methods.</td>
<td>`display system-failure [ [ begin</td>
<td>Available in any view</td>
</tr>
<tr>
<td></td>
<td>exclude</td>
<td>include } regular-expression ]</td>
</tr>
<tr>
<td>Display device software version update</td>
<td>`display version-update-record [ [ begin</td>
<td>Available in any view</td>
</tr>
<tr>
<td>records (boot file).</td>
<td>exclude</td>
<td>include } regular-expression ]</td>
</tr>
<tr>
<td>Clear the records of updating the device</td>
<td>`reset version-update-record [ [ begin</td>
<td>Available in system view</td>
</tr>
<tr>
<td>software.</td>
<td>exclude</td>
<td>include } regular-expression ]</td>
</tr>
</tbody>
</table>
Automatic configuration

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 automatic configuration network

As shown in Figure 1, the device implements automatic configuration with the cooperation of the following servers: a DHCP server, TFTP server, and DNS server:

- **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 such as the host name file and the configuration file.
- **DNS server**—IP addresses-host name resolution. In some cases, the device resolves its IP address to the 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 must configure the DHCP relay agent on the gateway.
How automatic configuration works

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. The configuration of these servers varies with device models and is omitted.

Before starting the device, connect only the interface needed in automatic configuration to the network.

Automatic configuration works in the following manner:

- During startup, the device sets the first up interface (if up Layer 2 Ethernet interfaces are available, the VLAN interface of the default VLAN of the Ethernet interfaces 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.
- 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 factory default configuration.

Work flow

Figure 2 shows the work flow of automatic configuration.

Figure 3 Work flow of automatic configuration
Using DHCP to obtain an IP address and other configuration information

Address acquisition process

As mentioned before, 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 6**—Specifies the DNS server IP address.
- **Option 66**—Specifies the TFTP server domain name.
- **Option 67** (or the file field that specifies the configuration file name)—If Option 67 contains the configuration file name, the device does not resolve the file field. If not, the device resolves the file field. The configuration file name is saved in the Option 67 or file field of the DHCP response. The device first resolves the Option 67 field. If this field contains the configuration file name, the device does not resolve the file field. If not, it resolves the file field.
- **Option 150**—Specifies the TFTP server IP address.

If no response is received from the DHCP server, the device removes the temporary configuration and starts up with factory defaults.

The temporary configuration contains two parts: the configuration made on the interface through which automatic configuration is performed, and the configuration made by executing the `ip host` commands in the host name file. The temporary configuration is removed by executing the `undo` commands. For more information about DHCP and `ip host`, see Layer 3—IP Services Configuration Guide.

Selection principles for the DHCP server address pool

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**—Contains a range of IP addresses and other parameters that the DHCP server dynamically assigns to clients.
- **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.

- **Method I**—If devices use the same configuration file, 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. The configuration file can only contain common configurations of the devices, and the specific configurations of each device must be performed in other ways. For example, the configuration file can enable Telnet and create a local user on devices so that the administrator can Telnet to each device to perform specific configurations (for example, configure the IP address of each interface).
- **Method II**—If devices use different configuration files, you must configure static address pools to ensure that each device can get a fixed IP address and a specific configuration file. With this method, the administrator does not need to perform any other configuration for the devices. To configure static
address pools, you must obtain client IDs. To obtain a device’s client ID, use `display dhcp server ip-in-use` to view address binding information on the DHCP server after the device obtains its IP address through DHCP.

### Obtaining the configuration file from the TFTP server

#### File types

⚠️ **CAUTION:**
- 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.

A device can obtain the following files from the TFTP server during automatic configuration:

- The configuration file specified by the Option 67 or file field in the DHCP response
- The host name file named `network.cfg`, which 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
```

- The configuration file of a device is named `hostname.cfg`, where `hostname` is the host name of the device. For example, if the host name of a device is `aaa`, the configuration file of the device is named `aaa.cfg`.
- The default configuration file is named `device.cfg`.
Obtaining the configuration file

Figure 4 Obtain 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 the DHCP response does not contain the configuration file name, 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 operations fail, the device requests the default configuration file from the TFTP server.

TFTP request sending mode

The device selects to unicast or broadcast a TFTP request by using the following workflow:

- If a legitimate TFTP server IP address is contained in the DHCP response, the device uncasts a TFTP request to the TFTP server.
- If no legitimate TFTP server IP address is contained in the DHCP response, the device resolves the TFTP server domain name contained in the DHCP response to the IP address through the DNS server. If successful, the device uncasts 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 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 factory defaults.

The configuration file is deleted after executed. Save the configuration by using `save`. Otherwise, the device has to perform automatic configuration again after reboot. For more information about `save`, 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 A-Series 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
Conventions

This section describes the conventions used in this documentation set.

**Command conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Bold text represents commands and keywords that you enter literally as shown.</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
<td>Italic text represents arguments that you replace with actual values.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Square brackets enclose syntax choices (keywords or arguments) that are optional.</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>{ x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>&amp;&lt;1-n&gt;</td>
<td>The argument or keyword and argument combination before the ampersand (&amp;) sign can be entered 1 to n times.</td>
</tr>
<tr>
<td>#</td>
<td>A line that starts with a pound (#) sign is comments.</td>
</tr>
</tbody>
</table>

**GUI conventions**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Window names, button names, field names, and menu items are in bold text. For example, the <strong>New User</strong> window appears; click <strong>OK</strong>.</td>
</tr>
<tr>
<td>&gt;</td>
<td>Multi-level menus are separated by angle brackets. For example, <strong>File &gt; Create &gt; Folder</strong>.</td>
</tr>
</tbody>
</table>

**Symbols**

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![WARNING]</td>
<td>An alert that calls attention to important information that if not understood or followed can result in personal injury.</td>
</tr>
<tr>
<td>![CAUTION]</td>
<td>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.</td>
</tr>
<tr>
<td>![IMPORTANT]</td>
<td>An alert that calls attention to essential information.</td>
</tr>
<tr>
<td><strong>NOTE</strong></td>
<td>An alert that contains additional or supplementary information.</td>
</tr>
<tr>
<td>![TIP]</td>
<td>An alert that provides helpful information.</td>
</tr>
</tbody>
</table>
Network topology icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Icon 1" /></td>
<td>Represents a generic network device, such as a router, switch, or firewall.</td>
</tr>
<tr>
<td><img src="image2.png" alt="Icon 2" /></td>
<td>Represents a routing-capable device, such as a router or Layer 3 switch.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Icon 3" /></td>
<td>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.</td>
</tr>
</tbody>
</table>

Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.
16-bit interface indexes, 170
ACTIVE state (patch status), 132
address
acquisition process (DHCP), 176
selection principles for DHCP server address pool, 176
alarm threshold (temperature), 168
authentication
configuring console login none authentication, 29
configuring console login password authentication, 30
configuring console login scheme authentication, 32
configuring FTP server, 93
configuring modem login none authentication, 55
configuring modem login password authentication, 56
configuring modem login scheme authentication, 58
configuring Telnet login none authentication, 38
configuring Telnet login password authentication, 40
configuring Telnet login scheme authentication, 41
console login modes, 28
modem login modes, 54
Telnet login modes, 37
authorization (FTP server), 93
automatic
rollback (ISSU boot file), 141
save (running configuration), 120
automatic configuration
address acquisition process, 176
executing configuration file from TFTP server, 179
how it works, 175
network, 174
obtaining configuration file from TFTP server, 177, 178
overview, 174
selection principles for DHCP server address pool, 176
TFTP server file types, 177
using DHCP to obtain an IP address, 176
using DHCP to obtain configuration information, 176
work flow, 175
auto-save (configuration file), 116
backing up (startup configuration file), 122
banner
configuration, 162, 163
message input mode, 163
multiple-line input mode, 163
single-line input mode, 163
types, 162
batch
operations, 108
setting prompt modes, 110
boot
ISSU boot file version automatic rollback, 141
ISSU boot file version manual rollback, 141
ISSU boot file version rollback, 141
rebooting device, 164
upgrading boot file through system reboot, 128
upgrading boot ROM through system reboot, 127
upgrading IRF member switch boot file, 129
changing current working directory, 106
checking NAND flash memory files, 110
clearing unused 16-bit interface indexes, 170
CLI
establishing FTP connection, 85
maintaining FTP connection, 89
terminating FTP connection, 89
console
configuring console port login, 26
configuring login none authentication, 29
configuring login optional common settings, 35
configuring login password authentication, 30
configuring login scheme authentication, 32
logging in through console port, 25
login authentication modes, 28
contacting HP, 180
content (configuration file), 113
copying file, 107
copyright information display, 162
creating directory, 106
current
network status (ISSU), 147
working directory change, 106
working directory display, 106
DEACTIVE state (patch status), 132
debugging FTP connection, 89
deleting
file, 108
startup configuration file, 123
detection timer, 168
device
automatic configuration, 174
clearing unused 16-bit interface indexes, 170
configuring detection timer, 168
configuring exception handling method, 164
configuring fan ventilation direction, 168
configuring login as Telnet client, 46
configuring management, 158
modem login none authentication, 55
modem login optional common settings, 61
modem login password authentication, 56
modem login scheme authentication, 58
NMS login, 72, 74
NMS SNMPv1 login settings, 73
NMS SNMPv2c login settings, 73
NMS SNMPv3 login settings, 74
scheduled task, 166
scheduled task with schedule command, 166
scheduled task with time command, 167
software upgrade, 125, 135
source and destination IP-based Telnet user login control, 78
source IP-based NMS user login control, 80, 81
source IP-based Telnet user login control, 77
source IP-based web user login control, 82, 83
source MAC-based Telnet user login control, 78, 79
SSH client, 50
SSH login, 47
SSH server, 47
system clock, 158
Telnet login, 36
Telnet login none authentication, 38
Telnet login optional common settings (VTY user interfaces), 44
Telnet login password authentication, 40
Telnet login scheme authentication, 41
Telnet user login control, 77
TFTP, 99
TFTP client, 100, 102
TFTP client (IRF mode), 103
user login control, 77
web login, 68
connecting
debugging FTP connection, 89
configuring member device temperature alarm threshold, 168
configuring name, 158
configuring scheduled task, 166
configuring system clock, 158
displaying management configuration, 172
displaying system clock, 159
enabling copyright information display, 162
maintaining management configuration, 172
rebooting, 164

DHCP
address acquisition process, 176
selection principles for DHCP server address pool, 176
using to obtain an IP address, 176
using to obtain configuration information, 176
diagnosing pluggable transceivers, 170
directory
changing current working directory, 106
creating, 106
displaying current working directory, 106
displaying information, 106
FTP server operation, 87
performing operations, 105
removing, 106
displaying
bad NAND flash memory blocks, 109
CLI login, 63
configuration file, 124
current working directory, 106
device management configuration, 172
directory information, 106
file contents, 107
file information, 107
FTP, 98
ISSU, 147
NAND flash memory, 109
software upgrade, 135
system clock, 159
TFTP client, 101
web login, 68
documentation
conventions used, 181
website, 180
emptying recycle bin, 108
enabling
configuration file auto-save, 116
copyright information display, 162
running configuration automatic save, 120
establishing FTP connection, 85
exception handling (software), 164
executing configuration file from TFTP server, 179
factory default configuration, 112
fan ventilation direction, 168
file
backing up startup configuration file, 122
checking NAND flash memory files, 110
configuration file content, 113
configuration file format, 113
configuration file overview, 112
configuration file save mode, 116
configuration files, 112
copying, 107
deleting, 108
deleting startup configuration file, 123
displaying contents, 107
displaying information, 107
emptying recycle bin, 108
enabling running configuration automatic save, 120
ISSU boot file version automatic rollback, 141
ISSU boot file version manual rollback, 141
ISSU boot file version rollback, 141
management, 105
management configuration, 112
moving, 107
name format, 105
operating FTP server files, 87
patch file, 130
performing batch operations, 108
performing operations, 107, 111
renaming, 107
restoring from recycle bin, 108
restoring startup configuration file, 123
running configuration manual save, 121
setting configuration rollback, 118
specifying startup configuration file, 122
TFTP server file types, 177
file transfer protocol. See FTP
filename format, 105
format
  configuration file, 113
  filename, 105
FTP
  client configuration, 89, 91
  configuration, 84
  configuring client, 85
  configuring server authentication, 93
  configuring server authorization, 93
  debugging connection, 89
  displaying, 98
  establishing connection, 85
  maintaining connection, 89
  operating server directories, 87
  operating server files, 87
  server configuration, 92, 94, 96
  server operating parameter configuration, 92
terminating connection, 89
  using another username for server login, 88
hotfix
  ACTIVE state patch, 132
  DEACTIVE state patch, 132
  IDLE state patch, 131
  one-step patch installation, 134
  patch, 130
  patch file, 130
  patch status, 130
  patch types, 130
  RUNNING state patch, 133
  software upgrade configuration, 137
  step-by-step patch installation, 134
  step-by-step patch uninstallation, 135
  hotfix installation (software upgrade), 130
HP
  customer support and resources, 180
  document conventions, 181
  documents and manuals, 180
  icons used, 181
  subscription service, 180
  support contact information, 180
  symbols used, 181
  websites, 180
HTTP (login configuration), 65, 68
HTTPS (login configuration), 66, 69
icons, 181
identifying pluggable transceivers, 170
IDLE state (patch status), 131
incompatible ISSU upgrade, 156
incremental patch (hotfix), 130
installing
  patch (one-step installation), 134
  patch (step-by-step installation), 134
software upgrade by hotfix installation, 130
software upgrade by patch installation, 130
uninstalling patch (step-by-step), 135

IP
configuring source and destination IP-based Telnet login control, 78
configuring source IP-based Telnet login control, 77
IRF member switch, 129

ISSU
boot file version automatic rollback, 141
boot file version manual rollback, 141
boot file version rollback, 141
compatible configuration, 144
configuration, 139, 144, 147, 149
configuring ISSU version rollback timer, 146
current network status, 147
displaying, 147
incompatible configuration, 146
performing compatible ISSU upgrade, 155
performing incompatible ISSU upgrade, 156
performing manual version rollback, 147
process, 140
requirements analysis, 147
state, 141
TFTP server configuration, 151
upgrade preparation, 151

logging in
configuring NMS login, 72
configuring NMS SNMPv1 settings, 73
configuring NMS SNMPv2c settings, 73
configuring NMS SNMPv3 settings, 74
console login authentication modes, 28
cable port configuration, 25
cable port login configuration, 26
HTTP login configuration, 65, 68
HTTPS login configuration, 66, 69
logging off online web users, 83
modem, 51
modem login authentication modes, 54
NMS login configuration, 72, 74
SSH, 47
SSH client configuration, 50
SSH server configuration, 47
Telnet, 36
Telnet authentication modes, 37
user login control configuration, 77
web login, 64
web login configuration, 68
logging off online web users, 83

MAC
configuring source IP-based NMS login control, 80, 81
configuring source MAC-based Telnet login control, 78, 79
maintaining
CLI login, 63
device management configuration, 172
FTP connection, 89
NAND flash memory, 109
managing
configuration file, 112
device management, 158
files, 105
storage media space, 109
manual rollback (ISSU boot file), 141
manuals, 180
memory
displaying NAND flash memory, 109
maintaining NAND flash memory, 109
message
configuring banner, 162
input mode (banner), 163
multiple-line input mode (banner), 163
single-line input mode (banner), 163
method (software upgrade), 126
mode
banner message input mode, 163
console login authentication, 28
FTP configuration, 84
modem login authentication, 54
multiple-line input mode (banner), 163
selecting configuration file save mode, 116
setting prompt modes, 110
single-line input mode (banner), 163
Telnet authentication, 37
TFTP request sending mode, 178
modem
configuring login none authentication, 55
configuring login optional common settings, 61
configuring login password authentication, 56
configuring login scheme authentication, 58
login, 51
login authentication modes, 54
moving a file, 107
multiple-line input mode (banner), 163
name (configuring device name), 158
NAND flash memory
checking files, 110
displaying, 109
displaying bad blocks, 109
maintaining, 109
repairing bad blocks, 109
NMS
configuring login, 72
configuring SNMPv1 login settings, 73
configuring SNMPv2c login settings, 73
configuring SNMPv3 login settings, 74
configuring source IP-based user login control, 80, 81
configuring source IP-based web user login control, 82, 83
logging off online web users, 83
login configuration, 72, 74
obtaining configuration file from TFTP server, 177, 178
one-step patch installation (hotfix), 134
operating
FTP server directories, 87
FTP server files, 87
FTP server parameter configuration, 92
Option 150 (DHCP address acquisition), 176
Option 6 (DHCP address acquisition), 176
Option 66 (DHCP address acquisition), 176
Option 67 (DHCP address acquisition), 176
optional common settings
configuring modem login, 61
console, 35
telnet (VTY user interfaces), 44
packet
upgrading software with compatible ISSU, 144
upgrading software with incompatible ISSU, 146
upgrading software with ISSU, 139, 144, 147, 149
parameter
configuring for saving running configuration, 119
FTP server operation, 92
password
configuring console login password authentication, 30
configuring modem login password authentication, 56
configuring Telnet login password authentication, 40
patch
defined, 130
file, 130
one-step installation, 134
software upgrade by installing patches, 130
status, 130
step-by-step installation, 134
step-by-step uninstallation, 135
types, 130
performing
batch operations, 108
compatible ISSU upgrade, 155
directory operations, 105
file operations, 107, 111
incompatible ISSU upgrade, 156
manual ISSU version rollback, 147
storage media operations, 109
pluggable transceiver
diagnosing, 170
identifying, 170
port
configuring console port login, 26
logging in through console port, 25
procedure
backing up startup configuration file, 122
changing current working directory, 106
clearing unused 16-bit interface indexes, 170
configuring automatic device configuration, 174
configuring banner, 162, 163
configuring compatible ISSU, 144
configuring console login none authentication, 29
configuring console login optional common settings, 35
configuring console login password authentication, 30
configuring console login scheme authentication, 32
configuring console port login, 25, 26
configuring detection timer, 168
configuring device login as Telnet client, 46
configuring device management, 158
configuring device name, 158
configuring exception handling method, 164
configuring fan ventilation direction, 168
configuring FTP, 84
configuring FTP client, 85, 89, 91
configuring FTP server, 92, 94, 96
configuring FTP server authentication, 93
configuring FTP server authorization, 93
configuring FTP server operating parameters, 92
configuring hotfix software upgrade, 137
configuring HTTP login, 65, 68
configuring HTTPS login, 66, 69
configuring immediate software upgrade, 135
configuring incompatible ISSU, 146
configuring ISSU, 139, 144, 147, 149
configuring ISSU version rollback timer, 146
configuring member device temperature alarm threshold, 168
configuring modem login, 51
configuring modem login none authentication, 55
configuring modem login optional common settings, 61
configuring modem login password authentication, 56
configuring modem login scheme authentication, 58
configuring NMS login, 72, 74
configuring NMS SNMPv1 login settings, 73
configuring NMS SNMPv2c login settings, 73
configuring NMS SNMPv3 login settings, 74
configuring parameters (saving running configuration), 119
configuring scheduled task, 166
configuring scheduled task with schedule command, 166
configuring scheduled task with time command, 167
configuring software upgrade, 125, 135
classifying source and destination IP-based Telnet user login control, 78
classifying source IP-based NMS user login control, 80, 81
classifying source IP-based Telnet user login control, 77
classifying source IP-based web user login control, 82, 83
classifying source MAC-based Telnet user login control, 78, 79
classifying SSH client, 50
classifying SSH login, 47
classifying SSH server, 47
classifying system clock, 158
classifying Telnet login, 36
classifying Telnet login none authentication, 38
classifying Telnet login optional common settings (VTY user interfaces), 44
classifying Telnet login password authentication, 40
classifying Telnet login scheme authentication, 41
classifying Telnet user login control, 77
classifying TFTP, 99
classifying TFTP client, 100, 102
classifying TFTP client (IRF mode), 103
classifying user login control, 77
classifying web login, 68
creating directory, 106
copying file, 107
creating directory, 106
classifying FTP connection, 89
deleting a file, 108
classifying startup configuration file, 123
diagnosing pluggable transceivers, 170
displaying CLI login, 63
displaying configuration file, 124
displaying current working directory, 106
displaying device management configuration, 172
displaying directory information, 106
displaying file contents, 107
displaying file information, 107
displaying FTP, 98
displaying ISSU, 147
displaying software upgrade, 135
displaying system clock, 159
displaying TFTP client, 101
displaying web login, 68
emptying recycle bin, 108
enabling configuration file auto-save, 116
enabling copyright information display, 162
enabling running configuration automatic save, 120
establishing FTP connection, 85
executing configuration file from TFTP server, 179
identifying pluggable transceivers, 170
installing patch (one-step installation), 134
installing patch (step-by-step installation), 134
logging off online web users, 83
maintaining CLI login, 63
maintaining device management configuration, 172
maintaining FTP connection, 89
managing files, 105
managing storage media space, 109
manually saving the running configuration, 121
moving file, 107
obtaining configuration file from TFTP server, 177, 178
operating FTP server directories, 87
operating FTP server files, 87
performing batch operations, 108
performing compatible ISSU upgrade, 155
performing directory operations, 105
performing file operations, 107, 111
performing incompatible ISSU upgrade, 156
performing manual ISSU version rollback, 147
performing storage media operations, 109
rebooting device, 164
removing directory, 106
renaming file, 107
restoring file from recycle bin, 108
restoring startup configuration file, 123
saving configuration file, 116
saving running configuration, 116
setting configuration rollback, 118
setting prompt modes, 110
specifying startup configuration file, 122
terminating FTP connection, 89
uninstalling patch (step-by-step), 135
upgrading IRF member switch boot file, 129
upgrading software through system reboot, 127, 128
upgrading software upgrade by installing hotfixes, 130
upgrading software upgrade by installing patches, 130
using another username for FTP server login, 88
process (DHCP address acquisition), 176
prompt modes, 110
rebooting
device, 164
software upgrade through system reboot, 127, 128
recycle bin
emptying, 108
restoring file, 108
removing directory, 106
renaming file, 107
 repairing bad NAND flash memory blocks, 109
request sending (TFTP mode), 178
requirements analysis (ISSU), 147
restoring
file from recycle bin, 108
startup configuration file, 123
rollback
setting configuration rollback, 118
running configuration, 112
RUNNING state (patch status), 133
saving
configuration file save mode, 116
configuring parameters (running configuration), 119
running configuration, 116
running configuration manual save, 121
scheduled task configuration, 166
scheme
configuring console login scheme authentication, 32
configuring modem login scheme authentication, 58
configuring Telnet login password authentication, 41
selecting configuration file save mode, 116
server
configuring authentication (FTP), 93
configuring authorization (FTP), 93
configuring SSH client, 50
configuring SSH server, 47
executing configuration file from TFTP server, 179
FTP configuration, 92
FTP operating parameters configuration, 92
FTP server configuration, 94, 96
obtaining configuration file from TFTP server, 177, 178
operating FTP directories, 87
operating FTP files, 87
selection principles for DHCP server address pool, 176
using another username for FTP login, 88
setting
configuration rollback, 118
prompt modes, 110
single-line input mode (banner), 163
SNMPv1 (NMS login configuration), 73  
SNMPv2c (NMS login configuration), 73  
SNMPv3 (NMS login configuration), 74  
software upgrade  
  configuration, 125, 135  
  displaying, 135  
  hotfix installation, 130  
  hotfix upgrade configuration, 137  
  immediate upgrade configuration, 135  
  IRF member switch boot file, 129  
  ISSU compatible configuration, 144  
  ISSU configuration, 139, 144, 147, 149  
  ISSU incompatible configuration, 146  
  ISSU preparation, 151  
  methods, 126  
  patch installation, 130  
  performing compatible ISSU upgrade, 155  
  performing incompatible ISSU upgrade, 156  
  system reboot, 127, 128  
specifying startup configuration file, 122  
SSH  
  configuring client, 50  
  configuring server, 47  
  logging in, 47  
startup  
  configuration, 112  
  configuration file, 115, 122  
  deleting startup configuration file, 123  
  restoring startup configuration file, 123  
state  
  ACTIVE hotfix patch, 132  
  DEACTIVE hotfix patch, 132  
  IDLE hotfix patch, 131  
  ISSU, 141  
  RUNNING hotfix patch, 133  
status (hotfix patch), 130  
step-by-step patch installation (hotfix), 134, 135  
storage media  
  displaying NAND flash memory, 109  
  maintaining NAND flash memory, 109  
  managing space, 109  
  performing operations, 109  
subscription service, 180  
support and other resources, 180  
switch (IRF member), 129  
symbols, 181  
system clock  
  configuring, 158  
  displaying, 159  
Telnet  
  configuring device login as Telnet client, 46  
  configuring login none authentication, 38  
  configuring login password authentication, 40  
  configuring login scheme authentication, 41  
  configuring optional common settings (VTY user interfaces), 44  
  configuring source and destination IP-based user login control, 78  
  configuring source IP-based user login control, 77  
  configuring source MAC-based user login control, 78, 79  
  configuring user login control, 77  
  logging in, 36  
  login authentication modes, 37  
temperature alarm threshold, 168  
temporary patch (hotfix), 130  
terminating FTP connection, 89  
TFTP  
  configuration, 99  
  configuring client, 100, 102  
  configuring client (IRF mode), 103
displaying client, 101
executing configuration file from TFTP server, 179
ISSU configuration on TFTP server, 151
obtaining configuration file from TFTP server, 177, 178
request sending mode, 178
server file types, 177
TFTP request sending mode, 178
time
configuring system clock, 158
displaying system clock, 159
timer
configuring detection timer, 168
configuring ISSU version rollback timer, 146
trivial file transfer protocol. See TFTP
type
banner, 162
device configuration, 112
factory default configuration, 112
patch, 130
running configuration, 112
startup configuration, 112
TFTP server file types, 177
uninstalling patch (step-by-step), 135
upgrading
IRF member switch boot file, 129
software, 125, 135
software (hotfix configuration), 137
software (immediate configuration), 135
software upgrade by installing hotfixes, 130
software upgrade by installing patches, 130
software upgrade methods, 126
software upgrade through system reboot, 127, 128
software upgrade with compatible ISSU, 144
software upgrade with incompatible ISSU, 146
software upgrade with ISSU, 139, 144, 147, 149
user
configuring source and destination IP-based Telnet login control, 78
configuring source IP-based NMS login control, 80, 81
configuring source IP-based Telnet login control, 77
configuring source IP-based web login control, 82, 83
configuring source MAC-based Telnet login control, 78, 79
configuring Telnet login control, 77
logging off online web users, 83
login control configuration, 77
message (configuring banner), 162
using
DHCP to obtain an IP address, 176
DHCP to obtain configuration information, 176
FTP server login with different username, 88
version
configuring ISSU version rollback timer, 146
ISSU boot file version automatic rollback, 141
ISSU boot file version manual rollback, 141
ISSU boot file version rollback, 141
performing manual ISSU version rollback, 147
VTY user interface (Telnet login), 44
web
configuring source IP-based user login control, 82, 83
displaying login, 68
logging off online web users, 83
login configuration, 64, 68
websites, 180