

# HP MSR Router Series Fundamentals

## Configuration Guide

### **Abstract**

This document describes the software features for the HP 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 products.

**Part number: 5998-2018 Version 2**  
**Software version: CMW520-R2207P02**  
**Document version: 6PW100-20110810**  
**March 2012**



## Legal and notice information

© Copyright 2011, 2012 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 CLI .....	1
Overview .....	1
Entering the CLI .....	1
Command conventions .....	1
Undo command form .....	2
CLI views .....	2
Entering system view .....	3
Exiting the current view .....	3
Returning to user view .....	4
Using the CLI online help .....	4
Entering commands .....	5
Editing command lines .....	5
Entering incomplete keywords .....	5
Configuring command keyword aliases .....	6
Configuring CLI hotkeys .....	6
Redisplaying entered but not submitted commands .....	7
Checking command-line errors .....	8
Using command history .....	8
Accessing history commands .....	8
Setting the user interface command history buffer size .....	9
Controlling the CLI output .....	9
Multi-screen display .....	9
Filtering the output information of a display command .....	10
Configuring user privilege and command levels .....	12
Configuring a user privilege level .....	13
Switching user privilege level .....	16
Modifying a command level .....	19
Saving the current configuration .....	19
Displaying and maintaining CLI .....	20
Login methods .....	21
User interface overview .....	22
Users and user interfaces .....	23
Numbering user interfaces .....	23
CLI login .....	24
Logging in through the console port .....	24
Configuration requirements .....	24
Login procedure .....	24
Console login authentication modes .....	27
Configuring none authentication for console login .....	28
Configuring password authentication for console login .....	29
Configuring AAA authentication for console login .....	30
Configuring common settings for console login (optional) .....	33
Logging in through Telnet .....	36
Telnet login authentication modes .....	36
Configuring none authentication for Telnet login .....	37
Configuring password authentication for Telnet login .....	38
Configuring AAA authentication for Telnet login .....	39
Configuring common settings for VTY user interfaces (optional) .....	42

Configuring the device to log in to a Telnet server as a Telnet client.....	44
Logging in through SSH .....	44
Configuring the SSH server.....	45
Configuring the SSH client to log in to the SSH server .....	47
Logging in through the AUX port.....	48
AUX port login authentication modes .....	48
Configuring none authentication for AUX port login.....	49
Configuring password authentication for AUX port login .....	50
Configuring AAA authentication for AUX port login.....	51
Configuring common settings for AUX port login (optional) .....	54
Configuration requirements.....	56
Login procedure.....	57
Logging in through modems .....	59
Configuration requirements.....	59
Login procedure.....	60
Modem login authentication modes.....	63
Configuring none authentication for modem login.....	64
Configuring password authentication for modem login.....	65
Configuring AAA authentication for modem login .....	66
Configuring common settings for modem login (optional).....	68
Displaying and maintaining CLI login .....	71
Web login .....	73
Configuration requirements.....	73
Configuring HTTP login .....	73
Configuring HTTPS login .....	75
Displaying and maintaining web login .....	76
Configuration examples .....	77
HTTP login example .....	77
HTTPS login example .....	78
NMS login .....	81
Configuring NMS login.....	81
NMS login example .....	83
User login control.....	85
Configuring login control over Telnet users.....	85
Configuring source IP-based login control over Telnet users .....	85
Configuring source and destination IP-based login control over Telnet users .....	86
Configuring source MAC-based login control over Telnet users.....	87
Source MAC-based login control configuration example.....	87
Configuring source IP-based login control over NMS users.....	88
Configuration preparation .....	88
Configuration steps .....	88
Configuration example .....	89
Configuring source IP-based login control over web users .....	90
Configuration preparation .....	90
Configuration steps .....	90
Logging off online web users .....	90
Configuration example .....	91
Device management .....	92
Overview.....	92
Configuring the device name .....	92
Changing the system time .....	92
Configuration guidelines .....	93
Configuration steps .....	95

Enabling displaying the copyright statement .....	95
Configuring banners .....	96
Configuration steps .....	97
Configuring the maximum number of concurrent users .....	97
Configuring the exception handling method .....	98
Rebooting the router .....	98
Rebooting the router immediately at the CLI .....	98
Scheduling a device reboot .....	98
Scheduling jobs .....	99
Configuration guidelines .....	99
Scheduling a job in the nonmodular approach .....	100
Scheduling a job in the modular approach .....	100
Scheduled job configuration example .....	101
Configuring a detection interval .....	102
Configuring card temperature thresholds .....	103
Configuring NMS monitored interfaces .....	103
Configuring an interface card working mode .....	104
Clearing unused 16-bit interface indexes .....	105
Verifying and diagnosing transceiver modules .....	105
Verifying transceiver modules .....	106
Diagnosing transceiver modules .....	106
Displaying and maintaining device management .....	107
<b>Configuration file management .....</b>	<b>109</b>
Overview .....	109
Types of configuration .....	109
Configuration file format and content .....	110
Coexistence of multiple configuration files .....	110
Startup with the configuration file .....	110
Saving the running configuration .....	110
Encrypting a configuration file .....	111
Configuration save modes .....	111
Setting configuration rollback .....	112
Configuration task list .....	113
Configuring parameters for saving the current running configuration .....	113
Enabling running configuration automatic save .....	114
Manually saving the running configuration .....	114
Setting configuration rollback .....	115
Specifying a startup configuration file for the next startup .....	115
Backing up the startup configuration file .....	115
Deleting a startup configuration file for the next startup .....	116
Restoring a startup configuration file .....	116
Displaying and maintaining a configuration file .....	117
<b>Managing files .....</b>	<b>118</b>
Overview .....	118
Storage media naming rules .....	118
Filename formats .....	118
Managing directories .....	119
Displaying directory information .....	119
Displaying the current working directory .....	119
Changing the current working directory .....	119
Creating a directory .....	119
Removing a directory .....	119
Managing files .....	120
Displaying file information .....	120

Displaying file contents.....	120
Renaming a file .....	120
Copying a file.....	120
Moving a file.....	120
Deleting a file .....	121
Restoring a file from the recycle bin.....	121
Emptying the recycle bin .....	121
Performing batch operations.....	121
Performing storage media operations .....	122
Managing storage media space .....	122
Mounting/unmounting storage media .....	122
Displaying and maintaining the NAND flash memory .....	123
Setting prompt modes.....	124
File management examples .....	124
<b>Configuring FTP.....</b>	<b>126</b>
Operation.....	126
Configuring the FTP client .....	127
Establishing an FTP connection.....	127
Managing directories on the FTP server .....	129
Operating the files on the FTP server .....	129
Using another username to log in to the FTP server .....	130
Maintaining and debugging the FTP connection.....	130
Terminating an FTP connection.....	131
FTP client configuration example.....	131
Configuring the FTP server .....	133
Configuring authentication and authorization on the FTP server .....	133
FTP server configuration example.....	134
Displaying and maintaining FTP.....	136
<b>Configuring TFTP.....</b>	<b>137</b>
Operation.....	137
Configuring the TFTP client .....	137
Displaying and maintaining the TFTP client .....	139
TFTP client configuration example.....	139
<b>License management .....</b>	<b>141</b>
Registering the software .....	141
Displaying and maintaining licenses .....	141
<b>Configuring software upgrade.....</b>	<b>142</b>
Overview.....	142
Upgrade methods .....	142
Software upgrade through a system reboot.....	143
Upgrading the Boot ROM program through a system reboot.....	143
Upgrading the boot file through a system reboot.....	143
Software upgrade by installing hotfixes .....	144
Basic concepts .....	144
Patch status.....	144
Configuration task list .....	147
Configuration prerequisites .....	147
One-step patch installation.....	147
Step-by-step patch installation.....	148
Step-by-step patch uninstallation.....	150
Displaying and maintaining software upgrade .....	150
Configuration examples .....	150
Hotfix configuration example.....	152

Automatic configuration .....	154
Typical automatic configuration network .....	154
How automatic configuration works .....	154
Work flow .....	155
Using DHCP to obtain an IP address and other configuration information .....	156
Obtaining the configuration file from the TFTP server .....	157
Executing the configuration file .....	159
Support and other resources .....	160
Contacting HP .....	160
Subscription service .....	160
Related information .....	160
Documents .....	160
Websites .....	160
Conventions .....	160
Index .....	163

# Configuring CLI

## Overview

The CLI enables you to interact with your device by entering text commands. At the CLI, you can instruct your device to perform a given task by typing a text command and then pressing **Enter**. Compared with the 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

```
.....
* Copyright (c) 2004-2011 Hangzhou H3C Tech. Co., Ltd. All rights reserved. *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
.....

User interface con0 is available.

Please press ENTER.

<H3C>
#Jun 18 15:48:11:979 2011 H3C SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1<hh3cLogin>: login from Console
%Jun 18 15:48:11:980 2011 H3C SHELL/5/SHELL_LOGIN: Console logged in from con0.
<H3C>_
```

## Entering the CLI

HP devices provide multiple methods for entering the CLI, such as through the console port, through Telnet, and through SSH. For more information, see "[CLI login](#)."

## 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

Convention	Description
<b>Boldface</b>	The keywords of a command line are in <b>Boldface</b> . Keep keywords unchanged when entering them at the CLI.
<i>Italic</i>	Command arguments are in <i>italic</i> . Replace arguments with actual values when entering a command at the CLI.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x   y   ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.

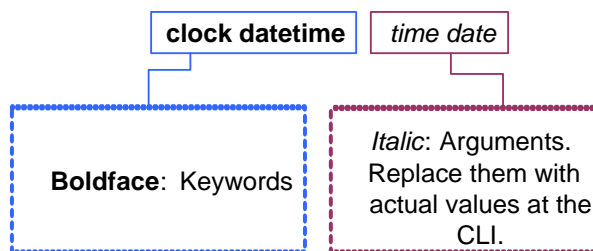


Convention	Description
[ x   y   ... ]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x   y   ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[ x   y   ... ] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.
&<1-n>	The arguments before the ampersand (&) sign can be entered 1 to n times.
#	A line starting with the # sign is comments.

The HP command lines keywords are not case sensitive.

Take the **clock datetime** *time date* command as an example to understand the meaning of the command-line parameters according to [Table 1](#).

**Figure 2 Read command-line parameters**



For example, you can type the following command line 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
```

You can read any command that is more complicated according to [Table 1](#).

## Undo command form

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, the **info-center enable** command enables the information center, and the **undo info-center enable** command disables the information center.

## CLI views

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

CLI views are organized in a hierarchical structure, as shown in [Figure 3](#).

After logging in to the switch, you are in user view. The prompt of user view is *<device name>*. In user view, you can perform display, debugging, and file management operations, set the system time, restart your device, and perform FTP and Telnet operations.

From user view, you can enter system view, where you can configure parameters such as daylight saving time, banners, and short-cut keys.

From system view, you can enter different function views. For example, you can enter interface view to configure interface parameters, enter user interface view to configure login user attributes, create a VLAN and enter its view, create a local user and enter local user view to configure the password and level of the local user, or enter OSPF view to configure OSPF parameters.

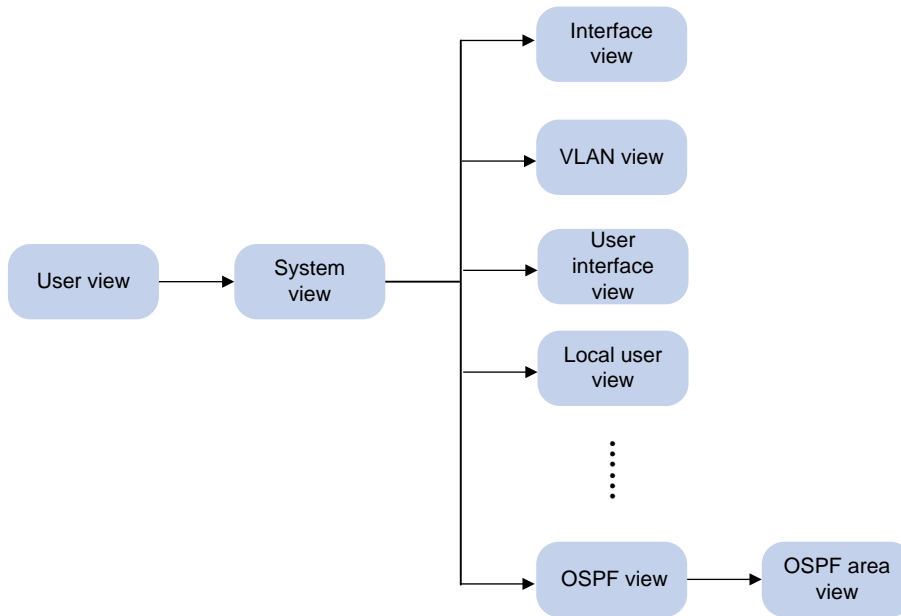
---

**NOTE:**

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

---

**Figure 3 Command-line views**



## Entering system view

When you log in to the device, you enter user view, where the prompt <device name> is displayed. You can 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.

Task	Command	Remarks
Enter system view from user view	<b>system-view</b>	Required Available in user view

## 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.

Task	Command	Remarks
Return to the upper-level view from any view	<b>quit</b>	Required Available in any view

The **quit** command in user view terminates the current connection between the terminal and the device.

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

The **return** command enables you to return to user view from any other view in one operation, instead of using the **quit** command repeatedly. Pressing **Ctrl+Z** has the same effect.

Task	Command	Remarks
Return to user view	<b>return</b>	Required Available in any view except user view

## Using the CLI 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
  clock            Specify the system clock
```

...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 number
[sysname] interface vlan-interface 1 ?
  <cr>
[sysname] interface vlan-interface 1
```

The string **<cr>** indicates that the command is a complete command, and you can execute the command by pressing **Enter**.

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

```
<sysname> c?  
cd  
clock  
cluster  
copy  
<sysname> display cl?  
clipboard  
clock  
cluster
```

## Entering commands

### Editing command lines

See [Table 2](#) and [Table 3](#) for shortcut keys to edit command lines.

**Table 2 Commonly used editing shortcut keys**

Key	Function
Common keys	If the edit buffer is not full, pressing a common key inserts the character at the position of the cursor and moves the cursor to the right.
<b>Backspace</b>	Deletes the character to the left of the cursor and moves the cursor back one character.
Left arrow key or <b>Ctrl+B</b>	The cursor moves one character space to the left.
Right arrow key or <b>Ctrl+F</b>	The cursor moves one character space to the right.
<b>Tab</b>	<p>If you press <b>Tab</b> after entering part of a keyword, the system automatically completes the keyword:</p> <ul style="list-style-type: none"><li>• If finding a unique match, the system substitutes the complete keyword for the incomplete one and displays it in the next line.</li><li>• If there is more than one match, you can press <b>Tab</b> repeatedly to display in cycles all the keywords starting with the character string you entered.</li><li>• If there is no match, the system does not modify the incomplete keyword and displays it again in the next line.</li></ul>

### Entering incomplete keywords

Enter a command comprising incomplete keywords to 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 to be used at the next startup, enter **st s**.

Press **Tab** to automatically complete an incomplete keyword.

## Configuring command keyword aliases

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

### Configuration guide

- When defining a keyword alias, you must enter the *cmdkey* and *alias* arguments in their complete form.
- When entering a keyword alias, the system displays and saves the keyword instead of its alias.
- When pressing **Tab** after typing part of an alias, the keyword is displayed.
- If you enter a string that partially matches a keyword and an alias, the command indicated by the alias is executed. To execute the command indicated by the keyword, enter the complete keyword.
- When entering a string that partially matches multiple aliases, the system gives you prompts.
- You can substitute an alias for only the first keyword of a non-undo command or the second keyword of an **undo** command.

### Configuration steps

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable the command keyword alias function.	<b>command-alias enable</b>	Required. By default, the command keyword alias function is disabled, and you cannot configure or use command keyword aliases.
3. Configure a command keyword alias.	<b>command-alias mapping</b> <i>cmdkey</i> <i>alias</i>	Required. Not configured by default.

## Configuring CLI hotkeys

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure CLI hotkeys.	<b>hotkey</b> { <b>CTRL_G</b>   <b>CTRL_L</b>   <b>CTRL_O</b>   <b>CTRL_T</b>   <b>CTRL_U</b> } <i>command</i>	Optional. <b>Ctrl+G</b> , <b>Ctrl+L</b> , and <b>Ctrl+O</b> hotkeys are specified at the CLI by default.
3. Display hotkeys.	<b>display hotkey</b>	Available in any view. See <a href="#">Table 3</a> for hotkeys reserved by the system.

By default, the **Ctrl+G**, **Ctrl+L**, and **Ctrl+O** hotkeys are associated with predefined commands; **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**.

**Table 3 Hotkeys reserved by the system**

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

The hotkeys in [Table 3](#) are defined by the switch. If the same hotkeys are defined by the terminal software used to interact with the switch, the hotkeys defined by the terminal software take effect.

## Redisplaying entered but not submitted commands

After you enable redisplaying of entered but not submitted commands:

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

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable redisplaying of entered but not submitted commands.	<b>info-center synchronous</b>	Required. Disabled by default. For more information about <b>info-center synchronous</b> , see <i>Network Management and Monitoring Configuration Guide</i> .

## Checking command-line errors

If a command line contains syntax errors, the CLI displays error messages. [Table 4](#) lists some common command-line error messages.

**Table 4 Common command-line error messages**

Error message	Cause
% Unrecognized command found at '^' position.	Command was not found.
% Incomplete command found at '^' position.	Incomplete command.
% Ambiguous command found at '^' position.	Ambiguous command.
Too many parameters.	Too many parameters.
% Wrong parameter found at '^' position.	Wrong parameters.

## Using command history

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

## Accessing history commands

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

You can 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; you can 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 incomplete.

- 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 execute **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, see *Fundamentals Command Reference*.

## Setting the user interface command history buffer size

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter user interface view.	<b>user-interface</b> { <i>first-num</i> [ <i>last-num</i> 1]   { <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> } <i>first-num</i> 2 [ <i>last-num</i> 2] }	— For more information about <b>user-interface</b> , see <i>Fundamentals Command Reference</i> .
3. Set the maximum number of commands that can be saved in the command history buffer.	<b>history-command max-size</b> <i>size-value</i>	Optional. By default, the command history buffer can save up to 10 commands. For more information about <b>history-command max-size</b> , see <i>Fundamentals Command Reference</i> .

## Controlling the CLI output

### Multi-screen display

If the output information is more than one screen, the system automatically pauses after displaying a screen. By default, up to 24 lines can be displayed on a screen. To change the screen length, use **screen-length**. For more information, see *Fundamentals Command Reference*.

**Table 5** Keys for controlling output

Key	Function
<b>Space</b>	Displays the next screen
<b>Enter</b>	Displays the next line
<b>Ctrl+C</b>	Stops the displaying and aborts the command execution
<b>&lt;PageUp&gt;</b>	Displays the previous page
<b>&lt;PageDown&gt;</b>	Displays the next page



## Disabling pause in multi-screen display

Use the following command to disable pausing between multiple screens of output. All output information is displayed at one time and the screen is refreshed continuously until the last screen is displayed.

Task	Command	Remarks
Disable pausing between screens of output for the current session	<b>screen-length disable</b>	<p>Required.</p> <p>By default, a login user uses the settings of <b>screen-length</b>. The default settings of <b>screen-length</b> are: pausing between screens of output is enabled and up to 24 lines are displayed on a screen.</p> <p>This command is executed in user view, and takes effect for the current session only. When you relog into the switch, the default configuration is restored.</p>

## Filtering the output information of a display command

To filter output information of a **display** command:

- Following **display**, enter the **begin**, **exclude**, or **include** keyword plus a regular expression.
- When the system pauses after displaying a screen of output information, use **/**, **-** or **+** plus a regular expression to filter subsequent output information. **/** equals the keyword **begin**, **-** equals the keyword **exclude**, and **+** 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, and supports some special characters.

**Table 6 Special characters supported in a regular express**

Character	Meaning	Remarks
<b>^string</b>	Starting sign. <i>string</i> appears only at the beginning of a line.	For example, regular expression <b>"^user"</b> only matches a string beginning with "user", not "Auser".
<b>string\$</b>	Ending sign. <i>string</i> appears only at the end of a line.	For example, regular expression <b>"user\$"</b> only matches a string ending with "user", not "userA".
<b>.</b>	Matches any single character, such as a single character, a special character, and a blank.	For example, <b>"s"</b> matches both <b>"as"</b> and <b>"bs"</b> .
<b>*</b>	Matches the preceding character or character group zero or multiple times.	For example, <b>"zo*"</b> matches <b>"z"</b> and <b>"zoo"</b> ; <b>"(zo)*"</b> matches <b>"zo"</b> and <b>"zozo"</b> .
<b>+</b>	Matches the preceding character or character group one or multiple times	For example, <b>"zo+"</b> matches <b>"zo"</b> and <b>"zoo"</b> , but not <b>"z"</b> .
<b> </b>	Matches the preceding or succeeding character string	For example, <b>"def int"</b> only matches a character string containing <b>"def"</b> or <b>"int"</b> .

Character	Meaning	Remarks
-	If it is at the beginning or the end of a regular expression, it equals ^ or \$. In other cases, it equals comma, space, round bracket, or curly bracket.	For example, "a_b" matches "a b" or "a(b"; "_ab" only matches a line starting with "ab"; "ab_" only matches a line ending with "ab".
-	It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means 1 to 9 (inclusive); "a-h" means a to h (inclusive).
[ ]	Matches a single character contained within the brackets.	For example, [16A] matches a string containing any character among 1, 6, and A; [1-36A] matches a string containing any character among 1, 2, 3, 6, and A (- is a hyphen). "]" can be matched as a common character only when it is put at the beginning of characters within the brackets, for example [ ]string]. There is no such limit on "[".
( )	A character group. It is usually used with "+" or "*".	For example, (123A) means a character group "123A"; "408(12)+" matches 40812 or 408121212. But it does not match 408.
\index	Repeats the character string specified by the index. A character string refers to the string within ( ) before \. index refers to the sequence number (starting from 1 from left to right) of the character group before \. If only one character group appears before \, index can only be 1; if n character groups appear before index, index can be any integer from 1 to n.	For example, (string)\1 repeats string, and a matching string must contain stringstring. (string1)(string2)\2 repeats string2, and a matching string must contain string1string2string2. (string1)(string2)\1\2 repeats string1 and string2, respectively, and a matching string must contain string1string2string1string2.
[^]	Matches a single character not contained within the brackets.	For example, [^16A] means to match a string containing any character except 1, 6 or A, and the matching string can also contain 1, 6 or A, but cannot contain these three characters only. For example, [^16A] matches "abc" and "m16", but not 1, 16, or 16A.
\<string	Matches a character string starting with string.	For example, "\<do" matches word "domain" and string "doa".
string\>	Matches a character string ending with string.	For example, "do\>" matches word "undo" and string "abcdo".
\bcharacter2	Matches character1character2. character1 can be any character except number, letter or underline, and \b equals [^A-Za-z0-9_].	For example, "\ba" matches "a" with "." being character1, and "a" being character2, but it does not match "2a" or "ba".
\Bcharacter	Matches a string containing character, and no space is allowed before character.	For example, "\Bt" matches "t" in "install", but not "t" in "big top".
character1\w	Matches character1character2. character2 must be a number, letter, or underline, and \w equals [^A-Za-z0-9_].	For example, "v\w" matches "vlan", with "v" being character1, and "l" being character2. v\w also matches "service", with "i" being character2.

Character	Meaning	Remarks
\W	Equals \b.	For example, "\Wa" matches "a", with "." being <i>character1</i> , and "a" being <i>character2</i> , but does not match "2a" or "ba".
\	Escape character. If a special character listed in this table follows \, the specific meaning of the character is removed.	For example, "\\" matches a string containing "\", "\^" matches a string containing "^", and "\\b" matches a string containing "b".

## Filtering output information examples

### 1. Example for 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 device model and the current configuration).

```
<Sysname> display current-configuration | begin user-interface
user-interface con 0
user-interface aux 0
user-interface vty 0 4
  authentication-mode none
  user privilege level 3
#
return
```

### 2. Example for using the **exclude** keyword

# Display the nondirect routes in the routing table (the output depends on the device model and the current configuration).

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

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
10.1.1.0/24	OSPF	10	2	10.1.1.2	Vlan2

### 3. Example for using the **include** keyword

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

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

Destination/Mask	Proto	Pre	Cost	NextHop	Interface
192.168.1.0/24	Direct	0	0	192.168.1.42	Vlan999

# Configuring user privilege and command levels

To avoid unauthorized access, the 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 the commands are categorized into four levels: visit, monitor, system, and manage, and are identified from low to high, respectively, by 0 through 3. [Table 7](#) describes the command levels.

**Table 7 Default command levels**

Level	Privilege	Description
0	Visit	<p>Involves commands for network diagnosis and commands for accessing an external device. Configuration of commands at this level cannot survive a device restart. Upon device restart, the commands at this level will be restored to the default settings.</p> <p>Commands at this level include <b>ping</b>, <b>tracert</b>, <b>telnet</b>, and <b>ssh2</b>.</p>
1	Monitor	<p>Involves commands for system maintenance and service fault diagnosis. Commands at this level are not saved after being configured. After the switch is restarted, the commands at this level will be restored to the default settings.</p> <p>Commands at this level include <b>debugging</b>, <b>terminal</b>, <b>refresh</b>, and <b>send</b>.</p>
2	System	<p>Provides service configuration commands, including routing configuration commands and commands for configuring services at different network levels. By default, commands at this level include all configuration commands except for those at manage level.</p>
3	Manage	<p>Involves commands that influence the basic operation of the system and commands for configuring system support modules.</p> <p>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).</p>

## 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.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter user interface view.	<b>user-interface</b> { <i>first-num</i> } [ <i>last-num</i> 1 ]   { <b>aux</b>   <b>console</b>   <b>vty</b> } <i>first-num2</i> [ <i>last-num2</i> ] }	—
3. Specify the scheme authentication mode.	<b>authentication-mode</b> <b>scheme</b>	<p>Required.</p> <p>By default, the authentication mode for VTY and AUX users is <b>password</b>, and no authentication is needed for console and TTY login users.</p>
4. Return to system view.	<b>quit</b>	—

Step	Command	Remarks
5. Configure the authentication mode for SSH users as <b>password</b> .	For more information, see <i>Security Configuration Guide</i> .	Required if users use SSH to log in, and username and password are needed at authentication.
6. Configure the user privilege level by using AAA authentication parameters.	a. Using local authentication <ul style="list-style-type: none"> <li>Use <b>local-user</b> to create a local user and enter local user view.</li> <li>Use the <b>level</b> keyword in <b>authorization-attribute</b> to configure the user privilege level.</li> </ul>	User either approach: <ul style="list-style-type: none"> <li>For local authentication, if you do not configure the user privilege level, the user privilege level is 0.</li> <li>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.</li> </ul>
	b. Using remote authentication (RADIUS, HWTACACS, and LDAP authentications) Configure the user privilege level on the authentication server.	

### Configuring a user privilege level by using AAA authentication parameters example

# 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 need to 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 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.

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

Step	Command	Remarks
1. Configure the authentication type for SSH users as <b>publickey</b> .	For more information, see <i>Security Configuration Guide</i> .	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 <b>scheme</b> .

Step	Command	Remarks
2. Enter system view.	<b>system-view</b>	—
3. Enter user interface view.	<b>user-interface</b> { <i>first-num 1</i> [ <i>last-num 1</i> ]   <b>vty</b> <i>first-num2</i> [ <i>last-num2</i> ] }	—
4. Configure the authentication mode for any user that uses the current user interface to log in to the switch.	<b>authentication-mode</b> <i>scheme</i>	Optional. By default, the authentication mode for VTY and AUX users is <b>password</b> , and no authentication is needed for AUX users.
5. Configure the privilege level for users that log in through the current user interface.	<b>user privilege level</b> <i>level</i>	Optional. By default, the user privilege level for users logged in through the console user interface is 3, and that for users logged in through the other user interfaces is 0.

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 (**none** or **password** authentication mode):

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter user interface view.	<b>user-interface</b> { <i>first-num 1</i> [ <i>last-num 1</i> ]   { <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> } <i>first-num2</i> [ <i>last-num2</i> ] }	—
3. Configure the authentication mode for any user that uses the current user interface to log in to the switch.	<b>authentication-mode</b> { <b>none</b>   <b>password</b> }	Optional. By default, the authentication mode for VTY and AUX user interfaces is <b>password</b> , and no authentication is needed for AUX login users.
4. Configure the privilege level of users logged in through the current user interface.	<b>user privilege level</b> <i>level</i>	Optional. By default, the user privilege level for users logged in through the console user interface is 3, and that for users logged in through the other user interfaces is 0.

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

# Perform no authentication on users logged in to the switch through Telnet, and specify their privilege level as 1. (Use no authentication mode in a secure network environment.)

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode none
[Sysname-ui-vty0-4] user privilege level 1
```

# 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 4
[Sysname-ui-vty1] authentication-mode password
[Sysname-ui-vty0-4] set authentication password cipher 12345678
[Sysname-ui-vty0-4] user privilege level 2
```

By default, users logged in through Telnet use the commands of level 0 after passing the authentication. After the configuration, when users log in to the switch through Telnet, they must enter password **12345678**, and then they can use commands of levels 0, 1, and 2.

For more information about user interfaces, see "[Login methods](#)." For more information about **user-interface**, **authentication-mode**, and **user privilege level**, see *Fundamentals Command Reference*.

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 switching, users can continue to configure the switch without needing to relog in, but the commands 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 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 must 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

- 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 categories:

Authentication mode	Meaning	Description
local	Local password authentication	The switch authenticates a user by using the privilege level switching password entered by the user. When this mode is applied, set the password for privilege level switching with <b>super password</b> .

Authentication mode	Meaning	Description
<b>scheme</b>	Remote AAA authentication through HWTACACS or RADIUS	<p>The switch sends the username and password for privilege level switching to the HWTACACS or RADIUS server for remote authentication.</p> <p>When this mode is applied, perform the following configurations:</p> <ul style="list-style-type: none"> <li>Configure HWTACACS or RADIUS scheme and reference the created scheme in the ISP domain. For more information, see <i>Security Configuration Guide</i>.</li> <li>Create the corresponding user and configure password on the HWTACACS or RADIUS server.</li> </ul>
<b>local scheme</b>	Performs the local password authentication first and then the remote AAA authentication	The switch authenticates a user by using the local password first, and if no password for privilege level switching is set, for the user logged in from the console port, the privilege level is switched directly; for the user logged in from any of the AUX, TTY, or VTY user interfaces, the AAA authentication is performed.
<b>scheme local</b>	Performs remote AAA authentication first and then the local password authentication	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.



#### CAUTION:

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.

To set the authentication mode for user privilege level switching:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Set the authentication mode for user privilege level switching.	<b>super authentication-mode</b> <b>{ local   scheme } *</b>	Optional. <b>local</b> by default.
3. Configure the password for user privilege level switching.	<b>super password</b> [ <b>level</b> <i>user-level</i> ] { <b>simple</b>   <b>cipher</b> } <i>password</i>	<p>Required if the authentication mode is set to <b>local</b> (specify the <b>local</b> keyword when setting the authentication mode).</p> <p>By default, no privilege level switching password is configured.</p> <p>If no user privilege level is specified when you configure the password for switching the user privilege level with the <b>super password</b> command, the user privilege level defaults to 3.</p>

If the user logs in from the console user interface (the console port or the AUX port used as the console port), the privilege level can be switched to a higher level, although the authentication mode is **local**, and no user privilege level password is configured.



## Switching the user privilege level



### CAUTION:

The privilege level switching fails after three consecutive unsuccessful password attempts.

Task	Command	Remarks
Switch the user privilege level.	<b>super</b> [ <i>level</i> ]	Required. When logging in to the switch, a user has a user privilege level, which depends on user interface or authentication user level. Available in user view.

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 8 Information entered for user privilege level switching**

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

User interface authentication mode	User privilege level switching authentication mode	Information entered for the first authentication mode	Information entered after the authentication mode changes
	<b>scheme local</b>	Password for privilege level switching (configured on the AAA server). The system uses the username used for logging in as the privilege level switching username.	Local user privilege level switching password.

- 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.
- For more information about user interface authentication, see "[CLI login](#)."

## Modifying a command level

All the 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.



### CAUTION:

HP recommends using the default command level or modifying 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.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure the command level in a specified view.	<b>command-privilege level level</b> <b>view view command</b>	Required. See <a href="#">Table 7</a> for the default settings.

## Saving the current configuration

On the device, you can enter the **save** command in any view to save all the 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 the **reset** commands, which clear specified information. The one-time commands executed are never saved.

## Displaying and maintaining CLI

Task	Command	Remarks
Display defined command keyword aliases and the corresponding keywords.	<b>display command-alias</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.
Display the clipboard information.	<b>display clipboard</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.

# Login methods

You can log in to a device in a variety of ways, as shown in [Table 9](#).

**Table 9 Login methods**

Login method	Default state
Logging in through the console port	By default, you can 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.
Logging in through Telnet	To log in to a device through Telnet, log in to the device through the console port and complete the following configuration: <ul style="list-style-type: none"><li>• Enable the Telnet function.</li><li>• Configure the IP address of the device interface, and ensure your device and the Telnet client can reach each other.</li><li>• Configure the authentication mode of VTY login users.</li><li>• Configure the user privilege level of VTY login users.</li></ul>
CLI login	To log in to a device through SSH, log in to the device through the console port and complete the following configuration: <ul style="list-style-type: none"><li>• Enable the SSH function and configure SSH attributes.</li><li>• Configure the IP address of the device interface, and ensure your device and the SSH client can reach each other.</li><li>• Configure the authentication mode of VTY login users as <b>scheme</b>.</li><li>• Configure the user privilege level of VTY login users.</li></ul>
Logging in through the AUX port	To log in to a device through the AUX port, log in to the device through the console port and configure the password for the password authentication mode, or change the authentication mode and configure parameters for the new authentication mode.
Logging in through modems	To log in to a device through modems, log in to the device through the console port and configure the password for the password authentication mode, or change the authentication mode and configure parameters for the new authentication mode.

Login method	Default state
Web login	<p>To log in to a device through web, log in to the device through the console port and complete the following configuration:</p> <ul style="list-style-type: none"> <li>• Configure the IP address of the device interface.</li> <li>• Configure a username and password for a web user.</li> <li>• Configure the user privilege level for the web user.</li> <li>• Configure a service type for the web user.</li> </ul>
NMS login	<p>To log in to a device through a NMS, log in to the device through the console port and complete the following configuration:</p> <ul style="list-style-type: none"> <li>• Configure the IP address of the device interface, and ensure the device and the NMS can reach each other.</li> <li>• Configure SNMP basic parameters.</li> </ul>

## User interface overview

User interfaces, or lines allow you to manage and monitor sessions between the terminal and device when you log in to the device through the console port, AUX port, or an asynchronous serial interface directly, or through Telnet or SSH.

Asynchronous serial interfaces include the following types:

- Synchronous/asynchronous serial interface operating in asynchronous mode, whose interface index begins with **Serial**.
- Dedicated asynchronous serial interface, whose interface index begins with **Async**.

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 device supports the following CLI configuration methods:

- Local configuration through the console port
- Local/remote configuration through the AUX port
- Local/remote configuration through the asynchronous serial port
- Local/remote configuration through Telnet or SSH

The methods correspond to the following user interfaces:

- **Console 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.
- **AUX user interface**—Used to manage and monitor users that log in via the AUX port. The type of the AUX port is EIA/TIA-232 DTE. The port is usually used for modem dialup access.
- **TTY user interface**—Used to manage and monitor users that log in via TTY, or, via an asynchronous serial port.
- **VTY user interface**—Used to manage and monitor users that log in via VTY. A VTY port is a logical terminal line used for Telnet or SSH access.

## Users and user interfaces

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 console port 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 multiple console ports, AUX ports, asynchronous serial interfaces, and Ethernet interfaces, so multiple user interfaces of the same port type are supported. 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 0 with a step of 1 and in the sequence of console, TTY, AUX, and VTY user interfaces. Use **display user-interface** 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:

- Console ports are numbered from 0 in the ascending order, with a step of 1
- AUX ports are numbered from 0 in the ascending order, with a step of 1
- TTYs are numbered from 1 in the ascending order, with a step of 1
- VTYs are numbered from 0 in the ascending order, with a step of 1

# CLI login

The CLI enables you to interact with a device by entering text commands. At the CLI, you can 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 GUI, where you can use a mouse to perform configuration, the CLI allows you to enter more information in one command line.

You can log in to the CLI of the device through the console port, Telnet, SSH, or modem.

## Logging in through the console port

Logging in through the console port is the most fundamental login method. To log in through other methods, you must log in through the console port and perform the required configurations.

## Configuration requirements

To log in the device through the console port, you only need to run a hyper terminal program on your host and configure the hyper terminal attributes. No configuration is needed on the device.

The hyper terminal attributes must match the default settings of the console port on the device.

**Table 10 Default settings of the console port on the device**

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

## Login procedure

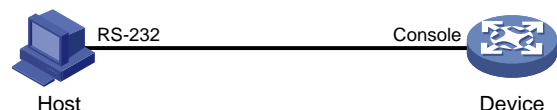
1. Turn off the device and PC.

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

To disconnect the PC from the device, first unplug the RJ-45 connector and then the DB-9 connector.

2. Use the console cable shipped with the device to connect the PC to 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 4 Connect the PC to the device through a console cable**





#### CAUTION:

Identify interfaces correctly to avoid connection errors.

3. Launch a terminal emulation program (such as HyperTerminal in Windows XP/Windows 2000). The following uses the HyperTerminal of Windows XP as an example. Select a serial port to be connected to the device, and set terminal parameters as follows (see [Figure 5](#) through [Figure 7](#)):
  - **Bits per second—9600**
  - **Data bits—8**
  - **Parity—None**
  - **Stop bits—1**
  - **Flow control—None**

On Windows 2003 Server operating system, 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, 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 5 Connection description**

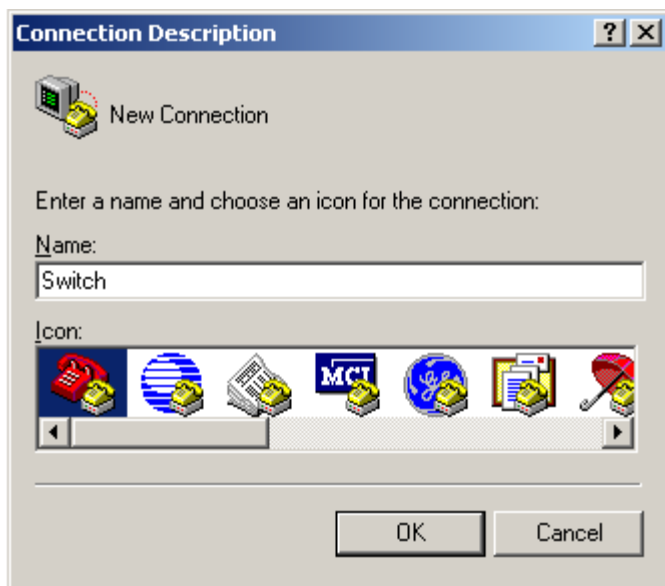
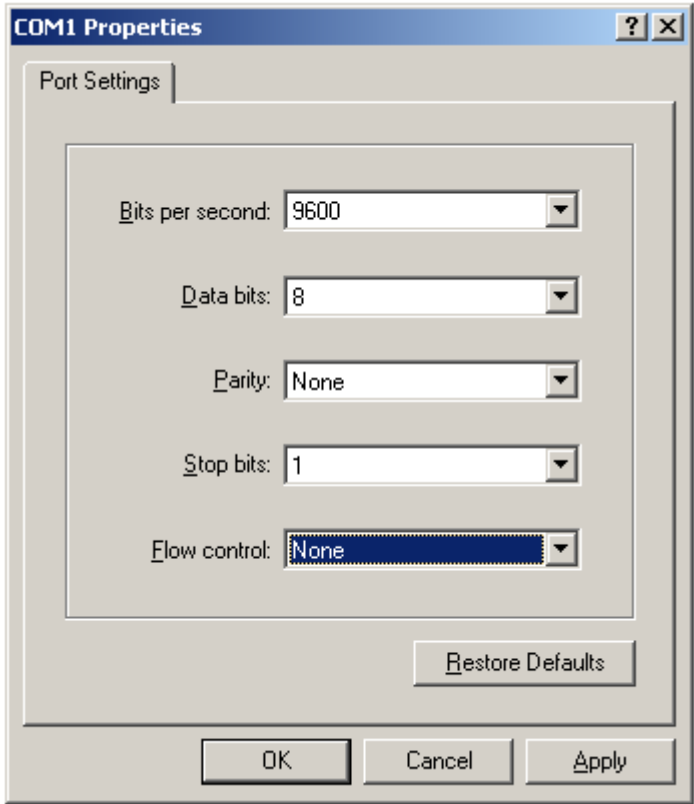




Figure 6 Specify the serial port used to establish the connection



Figure 7 Set the properties of the serial port



4. Turn on the device. You are prompted to press **Enter** if the device successfully completes the POST. A prompt, such as <HP>, appears after you press **Enter**, as shown in [Figure 8](#).

**Figure 8 Configuration page**

```
id=0x19003fff,proc=0xa834e8
id=0x19003fff,proc=0xa7110c
id=0x19004fff,proc=0xa6b60c
id=0x19500fff,proc=0x507c4c
id=0x19500fff,proc=0x505fc4
id=0x19510fff,proc=0x353df2c
id=0x19518fff,proc=0x366c6c0
id=0x19700100,proc=0x508a88
id=0x19700fff,proc=0xa4e2b4
id=0x19703fff,proc=0xa48ec4
id=0x1a000fff,proc=0x2182b10
id=0x1cfff000,proc=0x20a6ccc
id=0x26000fff,proc=0x191f450
id=0x27607100,proc=0x5074a8
User interface con0 is available.

Press ENTER to get started.
<HP>
%Aug  9 14:11:02:740 2011 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console
%Aug  9 14:11:02:740 2011 HP SHELL/5/SHELL_LOGIN: Console logged in from con0.
<HP>
```

5. 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 login:

- **none**—Requires no username or password at login. This mode is insecure.
- **password**—Requires password authentication at login.
- **scheme**—Uses AAA for user authentication, authorization, and accounting at login. AAA is a uniform framework for implementing network access management. This document describes only how to use AAA for local authentication and remote authentication. For more information, see *Security Configuration Guide*.

---

### ⓘ **IMPORTANT:**

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

**Table 11 Configuration required for different console login authentication modes**

Authentication mode	Configuration	Remarks
None	Configure the device not to authenticate users.	See "Configuring none authentication for console login."
Password	Configure the device to authenticate users by using the local password.	See "Configuring password authentication for console login."
	Set the local password.	
AAA	Configure the device to use AAA for users.	See "Configuring AAA authentication for console login."
	Configure AAA.	
	To configure local authentication:	
	<ol style="list-style-type: none"> <li>1. Configure a local user and specify the password.</li> <li>2. Configure the device to use local authentication.</li> </ol>	
AAA	To configure remote RADIUS or HWTACACS authentication:	See "Configuring AAA authentication for console login."
	<ol style="list-style-type: none"> <li>1. Configure the RADIUS or HWTACACS scheme on the device.</li> <li>2. Configure the username and password on the AAA server.</li> <li>3. Configure the device to use the scheme for user authentication.</li> </ol>	

## Configuring none authentication for console login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter console user interface view.	<b>user-interface console</b> <i>first-number</i> [ <i>last-number</i> ]	—
3. Specify the none authentication mode.	<b>authentication-mode none</b>	Required. By default, you can log in to the device through the console port without authentication, and have user privilege level 3 after login.
4. Configure common settings for console login.	—	Optional. See "Configuring common settings for console login (optional)."

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 9](#).

**Figure 9 Configuration page**

```
*****
* 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.                 *
*****

User interface con0 is available.

Please press ENTER.

<HP>
%Aug 9 14:12:04:780 2011 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console
%Aug 9 14:12:04:780 2011 HP SHELL/5/SHELL_LOGIN: Console logged in from con0.
<HP>
```

## Configuring password authentication for console login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter console user interface view.	<b>user-interface console</b> <i>first-number</i> [ <i>last-number</i> ]	—
3. Configure the authentication mode as local password authentication.	<b>authentication-mode password</b>	Required. By default, you can log in to the device through the console port without authentication and have user privilege level 3 after login.
4. Set the local password.	<b>set authentication password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required. By default, no local password is set.
5. Configure common settings for console login.	—	Optional. See " <a href="#">Configuring common settings for console login (optional)</a> ."

When you log in to the device through the console port after 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 10](#).

Figure 10 Configuration page

```

*****
* 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.                 *
*****

User interface con0 is available.

Please press ENTER.

Login authentication

Password:
<HP>
#Aug  9 14:16:34:207 2011 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console
%Aug  9 14:16:34:208 2011 HP SHELL/5/SHELL_LOGIN: Console logged in from con0.
<HP>_

```

## Configuring AAA authentication for console login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter console user interface view.	<b>user-interface console</b> <i>first-number</i> [ <i>last-number</i> ]	—
3. Specify AAA authentication mode.	<b>authentication-mode</b> <b>scheme</b>	<p>Required.</p> <p>Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme.</p> <p>By default, users that log in through the console port are not authenticated.</p>

Step	Command		Remarks
4. Enable command authorization.	<b>command authorization</b>		<p>Optional.</p> <ul style="list-style-type: none"> <li>By default, command authorization is not enabled.</li> <li>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 yes, the command can be executed.</li> </ul>
5. Enable command accounting.	<b>command accounting</b>		<p>Optional.</p> <ul style="list-style-type: none"> <li>By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li> <li>Command accounting allows the HWTACACS server to record all the 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.</li> </ul>
6. Return to system view.	<b>quit</b>		—
7. Configure authentication mode.	a. Enter ISP domain view	<b>domain</b> <i>domain-name</i>	<p>Optional.</p> <p>By default, the AAA</p>

Step		Command	Remarks
	<b>b.</b> Apply specified AAA scheme to domain <hr/> <b>c.</b> Exit to system view	<b>authentication default</b> <b>{ hwtacacs-scheme</b> <i>hwtacacs-scheme-name [ local ]</i> <b>  local   none   radius-scheme</b> <i>radius-scheme-name [ local ] }</i> <hr/> <b>quit</b>	scheme is <b>local</b> . If you specify the local AAA scheme, you must perform local user configuration. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well: <ul style="list-style-type: none"> <li>For RADIUS and HWTACACS configuration, see <i>Security Configuration Guide</i>.</li> <li>Configure the username and password on the AAA server. (For more information, see <i>Security Configuration Guide</i>.)</li> </ul>
<b>8.</b>	Create local user and enter local user view.	<b>local-user</b> <i>user-name</i>	Required.
<b>9.</b>	Set authentication password for local user.	<b>password { cipher   simple }</b> <i>password</i>	Required.
<b>10.</b>	Specifies command level of local user.	<b>authorization-attribute level</b> <i>level</i>	Optional. By default, the command level is 0.
<b>11.</b>	Specify service type for local user.	<b>service-type terminal</b>	Required. By default, no service type is specified.
<b>12.</b>	Configure common settings for console login.	—	Optional. See " <a href="#">Configuring common settings for console login (optional)</a> ."

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 **authorization-attribute level** *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*.

After the configuration, when you log in to the device through the console port, 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 11](#).

**Figure 11 Configuration page**

```
*****
* 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.                 *
*****

User interface con0 is available.

Please press ENTER.

Login authentication

Username:abcd
Password:
<HP>
#Aug  9 14:18:47:814 2011 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:abcd login from Console
%Aug  9 14:18:47:815 2011 HP SHELL/5/SHELL_LOGIN: abcd logged in from con0.
<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 use another login method. After configuring common settings for console login, you must modify the settings on the terminal to make them consistent with those on the device.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable display of copyright information.	<b>copyright-info enable</b>	Optional. Enabled by default.
3. Enter console user interface view.	<b>user-interface console</b> <i>first-number [ last-number ]</i>	—
4. Configure console port properties.	a. Configure baud rate. <b>speed</b> <i>speed-value</i>	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.



Step		Command	Remarks
<b>b.</b>	Configure parity check mode.	<b>parity</b> { <b>even</b>   <b>mark</b>   <b>none</b>   <b>odd</b>   <b>space</b> }	Optional. <b>none</b> by default.
<b>c.</b>	Configure stop bits.	<b>stopbits</b> { <b>1</b>   <b>1.5</b>   <b>2</b> }	Optional. By default, the stop bits setting 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.
<b>d.</b>	Configure data bits.	<b>databits</b> { <b>5</b>   <b>6</b>   <b>7</b>   <b>8</b> }	Optional. By default, the data bits setting of the console port is 8. Data bits is the number of bits representing one character. The setting depends on the contexts to be transmitted. For example, you can set it to 7 if standard ASCII characters are to be sent, and set it to 8 if extended ASCII characters are to be sent.
<b>e.</b>	Define a shortcut key for enabling a terminal session.	<b>activation-key</b> <i>character</i>	Optional. By default, you can press <b>Enter</b> to enable a terminal session.
<b>f.</b>	Define shortcut key for terminating tasks.	<b>escape-key</b> { <b>default</b>   <i>character</i> }	Optional. By default, you can press <b>Ctrl+C</b> to terminate a task.
<b>g.</b>	Configure stop bits detection.	<b>stopbit-error intolerance</b>	Optional. By default, no stop bits are detected.
<b>h.</b>	Configure flow control mode	<b>flow-control</b> { <b>hardware</b>   <b>none</b>   <b>software</b> } <b>flow-control hardware</b> <i>flow-control-type1</i> [ <b>software</b> <i>flow-control-type2</i> ] <b>flow-control software</b> <i>flow-control-type1</i> [ <b>hardware</b> <i>flow-control-type2</i> ]	Optional. By default, no flow control is performed.

Step	Command	Remarks
i. Configure type of terminal display	<b>terminal type</b> { <b>ansi</b>   <b>vt100</b> }	<p>Optional.</p> <p>By default, the terminal display type is ANSI.</p> <p>The device supports two types of terminal display: ANSI and VT100. HP recommends you to set 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.</p>
j. Configure user privilege level for login users	<b>user privilege level</b> <i>level</i>	<p>Optional.</p> <p>By default, the default command level is 3 for the console user interface.</p>
k. Set maximum number of lines on next screen.	<b>screen-length</b> <i>screen-length</i>	<p>Optional.</p> <p>By default, the next screen displays 24 lines.</p> <p>A value of 0 disables the function.</p>
l. Set size of history command buffer.	<b>history-command max-size</b> <i>value</i>	<p>Optional.</p> <p>By default, the buffer saves 10 history commands at most.</p>
m. Set idle-timeout timer.	<b>idle-timeout</b> <i>minutes</i> [ <i>seconds</i> ]	<p>Optional.</p> <p>The default idle-timeout is 10 minutes. The system automatically terminates the user's connection if there is no information interaction between the device and the user within the idle-timeout time.</p> <p>Setting idle-timeout to 0 disables the timer.</p>

# Logging in through Telnet

The device supports Telnet. You can telnet to the device to remotely manage and maintain the device.

**Figure 12 Telnet login**



**Table 12 Configuration requirements for Telnet login**

Object	Requirements
Telnet server	Configure the IP address of the device interface, and make sure the Telnet server and client can reach each other.
	Configure the authentication mode and other settings.
Telnet client	Run the Telnet client program.
	Obtain the IP address of the device interface on the server.

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

- On a device that serves as the Telnet client, you can log in to a Telnet server to perform operations on the server.
- On a device that serves as the Telnet server, you can configure the authentication mode and user privilege level for Telnet users. By default, password authentication is adopted for Telnet login, but no login password is configured. Before you can telnet to the device, you must log in to the device through the console port and configure the authentication mode, user privilege level, and common settings.

## Telnet login authentication modes

The following authentication modes are available for Telnet login: **none**, **password**, and AAA (**scheme**).

- **none**—Requires no username and password at login. This mode is insecure.
- **password**—Requires password authentication at login. Keep your password. If you lose your password, log in to the device through the console port to view or modify the password.
- **scheme**—Uses AAA for user authentication, authorization, and accounting at login. AAA is a uniform framework for implementing network access management. This document describes only how to use AAA for local authentication and remote authentication. For more information about AAA configuration, see *Security Configuration Guide*. Keep your username and password. If you lose your local password, log in to the device through the console port to view or modify the Telnet password. If you lose your remote authentication password, contact the administrator.

**Table 13 Configuration required for different Telnet login authentication modes**

Authentication mode	Configuration	Remarks
None	Configure the device not to authenticate users.	See " <a href="#">Configuring none authentication for Telnet login.</a> "

Authentication mode	Configuration	Remarks
Password	Configure the device to authenticate users by using the local password.	See <a href="#">"Configuring password authentication for Telnet login."</a>
	Set the local password.	
Scheme	Configure the device to use AAA for users.	See <a href="#">"Configuring AAA authentication for Telnet login."</a>
	Configure AAA on the device.	
	To configure local authentication:	
	1. Configure a local user and specify the password.	
	2. Configure the device to use local authentication.	
	To configure remote RADIUS or HWTACACS authentication:	
	1. Configure the RADIUS or HWTACACS scheme on the device.	
	2. Configure the username and password on the AAA server.	
	3. Configure the device to use the scheme for user authentication.	

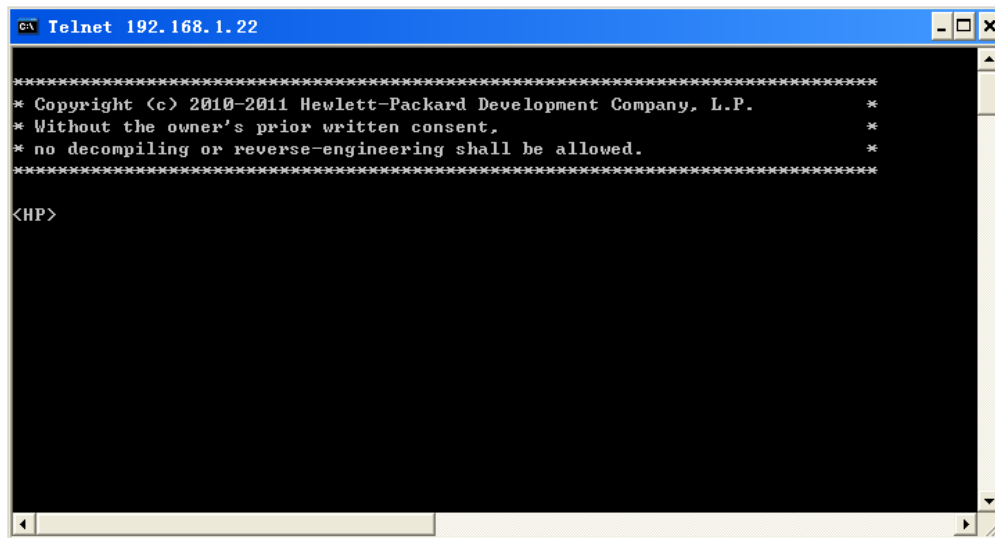
## Configuring none authentication for Telnet login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable Telnet.	<b>telnet server enable</b>	Required.
3. Enter one or multiple VTY user interface views.	<b>user-interface vty</b> <i>first-number</i> [ <i>last-number</i> ]	—
4. Specify the none authentication mode.	<b>authentication-mode none</b>	Required.
5. Configure the command level for login users on the current user interfaces.	<b>user privilege level</b> <i>level</i>	Required. By default, the default command level is 0 for VTY user interfaces.
6. Configure common settings for VTY user interfaces.	—	Optional. See <a href="#">"Configuring common settings for VTY user interfaces (optional)."</a>

When you log in to the device through Telnet again, perform the following steps:

- You enter the VTY user interface, as shown in [Figure 13](#).
- If "All user interfaces are used, please try later!" is displayed, then the current login users exceed the maximum number. You must try later.

Figure 13 Configuration page



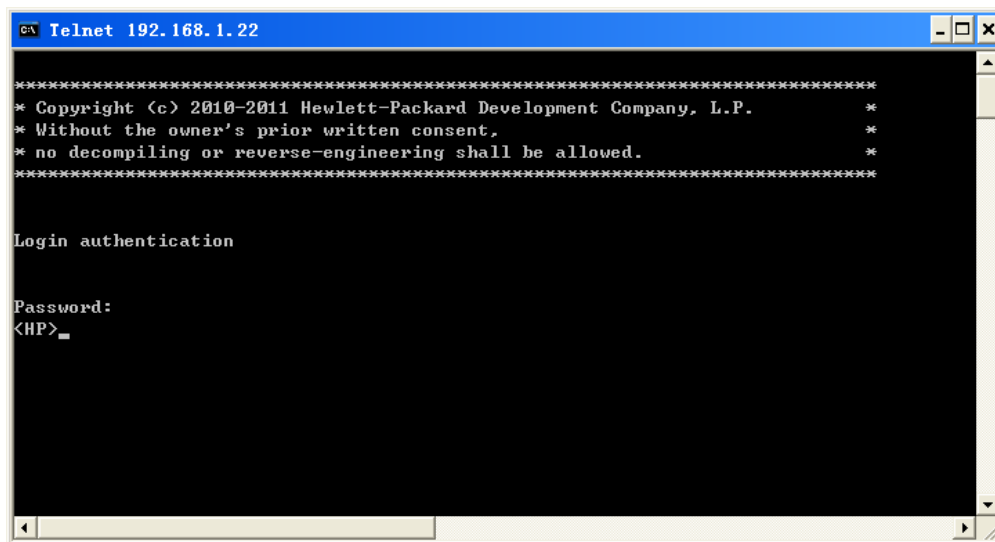
## Configuring password authentication for Telnet login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable Telnet.	<b>telnet server enable</b>	Required.
3. Enter one or multiple VTY user interface views.	<b>user-interface vty</b> <i>first-number</i> [ <i>last-number</i> ]	—
4. Specify the password authentication mode.	<b>authentication-mode password</b>	Required.
5. Set the local password.	<b>set authentication password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required. By default, no local password is set.
6. Configure the user privilege level for login users.	<b>user privilege level</b> <i>level</i>	Required. 0 by default.
7. Configure common settings for VTY user interfaces.	—	Optional. See " <a href="#">Configuring common settings for VTY user interfaces (optional)</a> ."

When you log in to the device through Telnet again, perform the following steps:

- 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 14](#).
- If "All user interfaces are used, please try later!" is displayed, then the number of current concurrent login users exceed the maximum. You must try later.

Figure 14 Configuration page



## Configuring AAA authentication for Telnet login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable Telnet.	<b>telnet server enable</b>	Required.
3. Enter one or multiple VTY user interface views.	<b>user-interface vty</b> <i>first-number [ last-number ]</i>	—
4. Specify the AAA authentication mode.	<b>authentication-mode scheme</b>	Required. Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme. By default, local authentication is adopted.
5. Enable command authorization.	<b>command authorization</b>	Optional. By default, command authorization is not enabled. <ul style="list-style-type: none"> <li>Create a HWTACACS scheme, and specify the IP address of the authorization server and other authorization parameters. For more information, see <i>Security Configuration Guide</i>.</li> <li>Reference the created HWTACACS scheme in the ISP domain. For more information, see <i>Security Configuration Guide</i>.</li> </ul>

Step	Command	Remarks
6. Enable command accounting.	<b>command accounting</b>	<p>Optional.</p> <ul style="list-style-type: none"> <li>By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li> <li>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.</li> </ul>
7. Exit to system view.	<b>quit</b>	—
8. Configure authentication mode.	<p>a. Enter default ISP domain view.</p>	<p>Optional.</p> <p>By default, the AAA scheme is <b>local</b>.</p>
	<p>b. Specify domain's AAA scheme.</p>	<p>If you specify the local AAA scheme, perform the configuration concerning local user as well. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well:</p> <ul style="list-style-type: none"> <li>For RADIUS and HWTACACS configuration, see <i>Security Configuration Guide</i>.</li> <li>Configure the username and password on the AAA server. (For more information, see <i>Security Configuration Guide</i>.)</li> </ul>
	<p>c. Exit to system view.</p>	<b>quit</b>
9. Create local user and enter local user view.	<b>local-user</b> <i>user-name</i>	Required.
10. Set local password.	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	<p>Required.</p> <p>By default, no local password is set.</p>

Step	Command	Remarks
11. Specifies command level of local user.	<b>authorization-attribute level</b> <i>level</i>	Optional. By default, the command level is 0.
12. Specify service type for local user.	<b>service-type telnet</b>	Required. By default, no service type is specified.
13. Exit to system view.	<b>quit</b>	—
14. Configure common settings for VTY user interfaces.	—	Optional. See " <a href="#">Configuring common settings for VTY user interfaces (optional)</a> ."

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

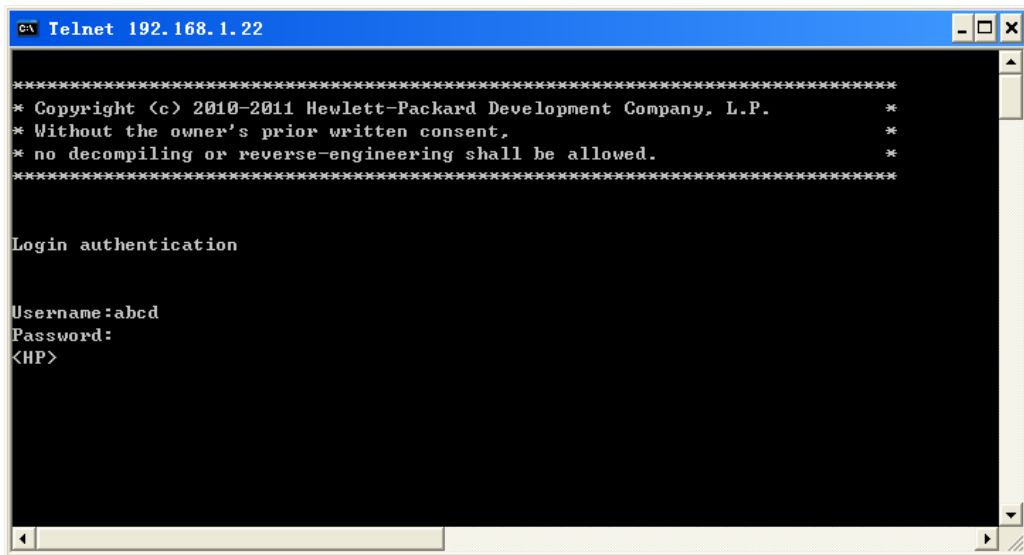
For more information about AAA, RADIUS, and HWTACACS, see *Security Configuration Guide*.

When you log in to the device through Telnet again:

- You must 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 15](#).
- 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. You must try again later.



Figure 15 Configuration page



## Configuring common settings for VTY user interfaces (optional)



### CAUTION:

Using **auto-execute command** may disable your ability to configure the system through the user interface to which the command is applied. Before configuring the command and saving the configuration (by using **save**), ensure you can access the device through VTY, TTY, console, or AUX interfaces to remove the configuration when a problem occurs.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter interface view.	<b>interface</b> <i>interface-type</i> { <i>interface-number</i>   <i>interface-number.subnumber</i> }	Required.
3. Specify an IP address for an interface.	<b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> }	Required.
4. Return to system view.	<b>quit</b>	—
5. Enable display of copyright information.	<b>copyright-info enable</b>	Optional. Enabled by default.
6. Enter one or multiple VTY user interface views.	<b>user-interface vty</b> <i>first-number</i> [ <i>last-number</i> ]	—
7. User interface configuration.	a. Enable terminal service.	Optional. Enabled by default.
	b. Enable current user interfaces support for pad, SSH, Telnet, or all of them.	Optional. By default, all protocols are supported.

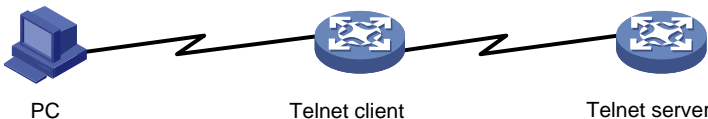
Step		Command	Remarks
c.	Define task termination shortcut key.	<b>escape-key</b> { <b>default</b>   character }	Optional. By default, you can press <b>Ctrl+C</b> to terminate a task.
d.	Configure terminal display type.	<b>terminal type</b> { <b>ansi</b>   <b>vt100</b> }	Optional. By default, the terminal display type is ANSI.
e.	Set maximum number of lines on next screen.	<b>screen-length</b> <i>screen-length</i>	Optional. By default, the next screen displays 24 lines. A value of 0 disables the function.
f.	Set history command buffer size.	<b>history-command</b> <b>max-size</b> <i>value</i>	Optional By default, the buffer saves 10 history commands.
g.	Set idle-timeout timer.	<b>idle-timeout</b> <i>minutes</i> [ <i>seconds</i> ]	Optional. The default idle-timeout is 10 minutes for all user interfaces. The system automatically terminates the user's connection if there is no information interaction between the device and the user in timeout time. Setting idle-timeout to 0 disables the timer.
h.	Specify command to be automatically executed when user logs in to current user interface.	<b>auto-execute</b> <b>command</b> <i>command</i>	Optional. By default, command auto-execution is disabled. The system automatically executes the specified command when a user logs in to the user interface, and tears down the user connection after the command is executed. If the command triggers another task, the system does not tear down the user connection until the task is completed. A Telnet command is usually specified to enable the user to automatically telnet to the specified device.

# Configuring the device to log in to a Telnet server as a Telnet client

## Configuration prerequisites

You have logged in to the device.

Figure 16 Telnet from the router (Telnet client) to another device (Telnet server)



If the Telnet client port and the Telnet server port connecting them are not in the same subnet, ensure the two devices can reach each other.

## Configuration steps

Step	Command	Remarks
1. Configure the device to log in to a Telnet server as a Telnet client.	<pre>telnet remote-host [ service-port ] [ [ vpn-instance vpn-instance-name ]   [ source { interface interface-type interface-number   ip ip-address } ] ]</pre> <pre>telnet ipv6 remote-host [ -i interface-type interface-number ] [ port-number ] [ vpn-instance vpn-instance-name ]</pre>	Required. Use either command. Available in user view.
2. Specify the source IPv4 address or source interface for sending Telnet packets.	<pre>telnet client source { interface interface-type interface-number   ip ip-address }</pre>	Optional. No source IPv4 address or source interface is specified. The source IPv4 address is selected by routing.

# Logging in through SSH

SSH offers an approach to log in to 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 17.

Figure 17 SSH login diagram



Configuration requirements of SSH login:

Object	Requirements
SSH server	Configure the IP address of the device interface, and ensure the SSH server and client can reach each other.
	Configure the authentication mode and other settings.
SSH client	If the host operates as an SSH client, run the SSH client program on the host.
	Obtain the IP address of the device interface on the server.

## Configuring the SSH server

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Create local key pairs.	<b>public-key local create { dsa   rsa }</b>	Required. By default, no local key pairs are created.
3. Enable SSH server.	<b>ssh server enable</b>	Required By default, SSH server is disabled.
4. Exit to system view.	<b>quit</b>	—
5. Enter one or more VTY user interface views.	<b>user-interface vty first-number [ last-number ]</b>	—
6. Specify the AAA authentication mode.	<b>authentication-mode e scheme</b>	Required.
7. Enable the current user interface to support either Telnet, SSH, or both of them.	<b>protocol inbound { all   pad   ssh   telnet }</b>	Optional. By default, all protocols are supported.
8. Enable command authorization.	<b>command authorization</b>	Optional. <ul style="list-style-type: none"> <li>By default, command authorization is not enabled.</li> <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 yes, the command can be executed.</li> </ul>

Step	Command	Remarks
9. Enable command accounting.	<b>command accounting</b>	Optional. <ul style="list-style-type: none"> <li>By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li> <li>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.</li> </ul>
10. Exit to system view.	<b>quit</b>	—
11. Configure authentication mode.	a. Enter default ISP domain view.	<b>domain</b> <i>domain-name</i>
	b. Apply specified AAA scheme to domain.	<b>authentication default { hwtacacs-scheme hwtacacs-scheme-name [ local ]   local   none   radius-scheme radius-scheme-name [ local ] }</b>
	c. Exit to system view.	<b>quit</b>
12. Create local user and enter local user view.	<b>local-user</b> <i>user-name</i>	Optional. By default, the AAA scheme is <b>local</b> . If you specify the local AAA scheme, perform the configuration concerning local user as well. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well: <ul style="list-style-type: none"> <li>For RADIUS and HWTACACS configuration, see <i>Security Configuration Guide</i>.</li> <li>Configure the username and password on the AAA server. (For more information, see <i>Security Configuration Guide</i>.)</li> </ul>
13. Set local password.	<b>password { cipher   simple }</b> <i>password</i>	Required. By default, no local password is set.
14. Specify command level of local user.	<b>authorization-attribute level</b> <i>level</i>	Optional. By default, the command level is 0.
15. Specify service type for local user.	<b>service-type</b> <i>ssh</i>	Required. By default, no service type is specified.
16. Return to system view.	<b>quit</b>	—

Step	Command	Remarks
17. Create SSH user, and specify authentication mode for SSH user.	<pre>ssh user username service-type stelnet authentication-type { password   { any   password- publickey   publickey } assign publickey keyname }</pre>	Optional. By default, no SSH user exists, and no authentication mode is specified.
18. Configure common settings for VTY user interfaces.	—	Optional. See <a href="#">"Configuring common settings for VTY user interfaces (optional)."</a>

This chapter describes how to configure an SSH client by using **password** authentication. For more information, see *Security Configuration Guide*.

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

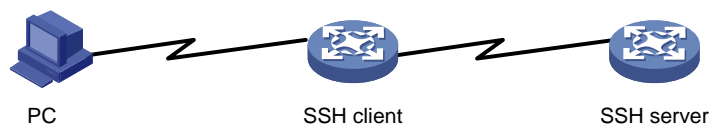
For more information about AAA, RADIUS, and HWTACACS, see *Security Configuration Guide*.

## Configuring the SSH client to log in to the SSH server

### Configuration prerequisites

You have logged in to the device.

**Figure 18 Log in to another device from the router**



If the SSH client and the SSH server are not in the same subnet, ensure the two devices can reach each other.

## Configuration steps

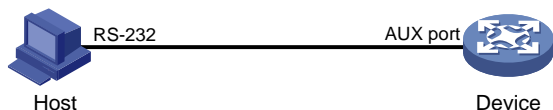
Step	Command	Remarks
1. Log in to an IPv4 SSH server.	<b>ssh2 server</b>	Required. server is the IPv4 address or host name of the server. Available in user view.
2. Log in to an IPv6 SSH server.	<b>ssh2 ipv6 server</b>	Required. server is the IPv6 address or host name of the server. Available in user view.

You can configure other settings for the SSH client to work with the SSH server. For more information, see SSH2.0 configuration commands in the *Security Command Reference*.

## Logging in through the AUX port

For a device that has separate console and AUX ports, you can use both to log in to the device. As shown in Figure 19, the console cable used in AUX port login is the same as that in console login.

Figure 19 AUX port login diagram



By default, AUX port login adopts password authentication. To log in through the AUX port, log in to the device through the console port or another method, configure the password for AUX password authentication or change the authentication mode, and configure related parameters.

## AUX port login authentication modes

By default, password authentication is adopted for AUX port login.

The following authentication modes are available for AUX port login: **none**, **password**, and AAA (**scheme**).

- **none**—Requires no username and password at login. This mode is insecure.
- **password**—Requires password authentication at login. Keep your password.
- **scheme**—Uses AAA for user authentication, authorization, and accounting at login. AAA is a uniform framework for implementing network access management. This document describes only how to use AAA for local authentication and remote authentication. For more information about AAA configuration, see *Security Configuration Guide*. Keep your username and password.

**Table 14 Configuration required for different AUX login authentication modes**

Authentication mode	Configuration	Remarks
None	Configure the device not to authenticate users.	See " <a href="#">Configuring none authentication for AUX port login.</a> "
Password	Configure the device to authenticate users by using the local password. Set the local password.	See " <a href="#">Configuring password authentication for AUX port login.</a> "
AAA	Configure the device to use AAA for users.  Configure AAA on the device. To configure local authentication: <ol style="list-style-type: none"> <li>1. Configure a local user and specify the password.</li> <li>2. Configure the device to use local authentication.</li> </ol> To configure remote RADIUS or HWTACACS authentication: <ol style="list-style-type: none"> <li>1. Configure the RADIUS or HWTACACS scheme on the device.</li> <li>2. Configure the username and password on the AAA server.</li> <li>3. Configure the device to use the scheme for user authentication.</li> </ol>	See " <a href="#">Configuring AAA authentication for AUX port login.</a> "

AUX port login authentication changes do not take effect until you exit the CLI and log in again.

## Configuring none authentication for AUX port login

Step	Command	Remarks
1. Enter system view	<b>system-view</b>	—
2. Enter one or more AUX user interface view	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
3. Specify the none authentication mode	<b>authentication-mode none</b>	Required.
4. Configure common settings for AUX login	—	Optional. See " <a href="#">Configuring common settings for AUX port login (optional).</a> "

After the configuration, next time you log in to the device through the AUX port, you are prompted to press enter. A prompt, such as <HP>, appears after you press **Enter**, as shown in [Figure 20](#).



Figure 20 Configuration page

```
*****
* 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.                 *
*****

User interface aux0 is available.

Please press ENTER.

<HP>
#Jan 1 00:03:34:696 2007 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console
%Jan 1 00:03:34:697 2007 HP SHELL/5/SHELL_LOGIN: Console logged in from aux0.
<HP>_
```

## Configuring password authentication for AUX port login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter one or more AUX user interface views.	<b>user-interface aux</b> <i>first-number [ last-number ]</i>	—
3. Specify the password authentication mode.	<b>authentication-mode</b> <b>password</b>	Required.
4. Set the local password.	<b>set authentication password</b> <b>{ cipher   simple } password</b>	Required. By default, no local password is set.
5. Configure common settings for AUX login.	—	Optional. See " <a href="#">Configuring common settings for AUX port login (optional)</a> ."

After the configuration, next time you log in to the device through the AUX port, 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 21](#).

Figure 21 Configuration page

```
*****
* 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.                 *
*****

User interface aux0 is available.

Please press ENTER.

Login authentication

Password:
<HP>
#Jan 1 00:07:32:966 2007 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console
%Jan 1 00:07:32:966 2007 HP SHELL/5/SHELL_LOGIN: Console logged in from aux0.
<HP>_
```

# Configuring AAA authentication for AUX port login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter one or more AUX user interface views.	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
3. Specify the AAA authentication mode.	<b>authentication-mode scheme</b>	Required.  Optional. <ul style="list-style-type: none"><li>• By default, command authorization is not enabled.</li><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 yes, the command can be executed.</li></ul>
4. Enable command authorization.	<b>command authorization</b>	

Step	Command	Remarks
5. Enable command accounting.	<b>command accounting</b>	Optional. <ul style="list-style-type: none"> <li>By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li> <li>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.</li> </ul>
6. Exit to system view.	<b>quit</b>	—
7. Configure authentication mode.	a. Enter default ISP domain view.	Optional. By default, the AAA scheme is <b>local</b> .
	b. Apply specified AAA scheme to domain.	If you specify the local AAA scheme, perform the configuration concerning local user as well. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well: <ul style="list-style-type: none"> <li>For RADIUS and HWTACACS configuration, see <i>Security Configuration Guide</i>.</li> <li>Configure the username and password on the AAA server. (For more information, see <i>Security Configuration Guide</i>.)</li> </ul>
	c. Exit to system view.	
8. Create local user and enter local user view.	<b>local-user</b> <i>user-name</i>	Required.
9. Set authentication password for local user.	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required.

Step	Command	Remarks
10. Specify command level of local user.	<b>authorization-attribute level</b> <i>level</i>	Optional. By default, the command level is 0.
11. Specify service type for local user.	<b>service-type terminal</b>	Required. By default, no service type is specified.
12. Configure common settings for AUX login.	—	Optional. See " <a href="#">Configuring common settings for AUX port login (optional)</a> ."

After enabling 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 **authorization-attribute level** *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*.

After the configuration, when you log in to the device through the AUX port, 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 22](#).

**Figure 22 Configuration page**

```

*****
* 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.                    *
*****

User interface aux0 is available.

Please press ENTER.

Login authentication

Username:abcd
Password:
<HP>
#Jan 1 00:08:25:152 2007 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:abcd login from Console
%Jan 1 00:08:25:152 2007 HP SHELL/5/SHELL_LOGIN: abcd logged in from aux0.
<HP>

```

## Configuring common settings for AUX port login (optional)

### ⚠ CAUTION:

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

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable display of copyright information.	<b>copyright-info enable</b>	Optional. Enabled by default.
3. Enter AUX interface view.	<b>interface aux 0</b>	—
4. Set the work mode to flow.	<b>async mode { flow   protocol }</b>	Optional. <b>flow</b> by default.
5. Enter the AUX user interface view.	<b>user-interface aux first-number [ last-number ]</b>	—
6. Configure AUX port properties.	a. Configure baud rate.	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.
	b. Configure parity check mode.	Optional. By default, the parity check mode of the AUX port is set to <b>none</b> , which means no check bit.
	c. Configure stop bits.	Optional. By default, the stop bits of the AUX 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.

Step	Command	Remarks
		Optional. By default, the data bits of the AUX port is 8. Data bits is the number of bits representing one character. The setting depends on the contexts to be transmitted. For example, you can set it to 7 if standard ASCII characters are to be sent, and set it to 8 if extended ASCII characters are to be sent.
d. Configure data bits.	<b>databits</b> { 5   6   7   8 }	
e. Define shortcut key for starting session.	<b>activation-key</b> <i>character</i>	Optional. By default, you can press <b>Enter</b> to start a session.
f. Define task termination shortcut key.	<b>escape-key</b> { <b>default</b>   <i>character</i> }	Optional. By default, you can press <b>Ctrl+C</b> to terminate a task.
g. Configure stop bits detection.	<b>stopbit-error</b> <b>intolerance</b>	Optional. By default, no stop bits are detected.
h. Configure flow control mode.	<b>flow-control</b> { <b>hardware</b>   <b>none</b>   <b>software</b> } <b>flow-control hardware</b> <i>flow-control-type1</i> [ <b>software</b> <i>flow-control-type2</i> ] <b>flow-control software</b> <i>flow-control-type1</i> [ <b>hardware</b> <i>flow-control-type2</i> ]	Optional. By default, an independent AUX port performs hardware flow control, and an AUX/console port does not perform any flow control.
i. Configure terminal display type.	<b>terminal type</b> { <b>ansi</b>   <b>vt100</b> }	Optional. By default, the terminal display type is ANSI. The device supports two types of terminal display: ANSI and VT100. HP recommends you to set 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.

Step		Command	Remarks
j.	Configure user privilege level for login users.	<b>user privilege level</b> <i>level</i>	Optional. By default, the default command level is 0 for the AUX user interface.
k.	Set maximum number of lines on next screen.	<b>screen-length</b> <i>screen-length</i>	Optional. By default, the next screen displays 24 lines at most. A value of 0 disables the function.
l.	Set history command buffer size.	<b>history-command max-size</b> <i>value</i>	Optional. By default, the buffer saves 10 history commands at most.
m.	Set idle-timeout timer.	<b>idle-timeout</b> <i>minutes</i> [ <i>seconds</i> ]	Optional. The default idle-timeout is 10 minutes. The system automatically terminates the user's connection if there is no information interaction between the device and the user in timeout time. Setting idle-timeout to 0 disables the timer.

## Configuration requirements

Object	Requirements
Device	Configure the authentication mode. For more information, see <a href="#">"Configuring none authentication for AUX port login,"</a> <a href="#">"Configuring password authentication for AUX port login,"</a> and <a href="#">"Configuring AAA authentication for AUX port login."</a>
Terminal	Run the hyper terminal program. Configure the hyper terminal attributes.

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

Setting	Default
Bits per second	9600 bps
Flow control	On for an independent AUX port, and off for the console and AUX port that share the same physical port
Parity	None
Stop bits	1
Data bits	8

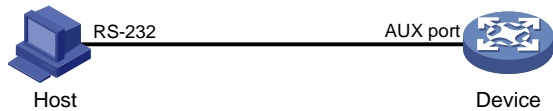
# Login procedure

## ⚠ CAUTION:

Identify the interface to avoid connection errors.

1. 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 AUX port of your device.

**Figure 23 Connect the device and PC**



The serial port of a PC does not support hot-swap, so do not plug or unplug the console cable to or from the PC when your device is powered on. 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 (see [Figure 24](#) through [Figure 26](#)):
  - **Bits per second—9600**
  - **Data bits—8**
  - **Parity—None**
  - **Stop bits—1**
  - **Flow control—None**

## 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 24 Connection description**

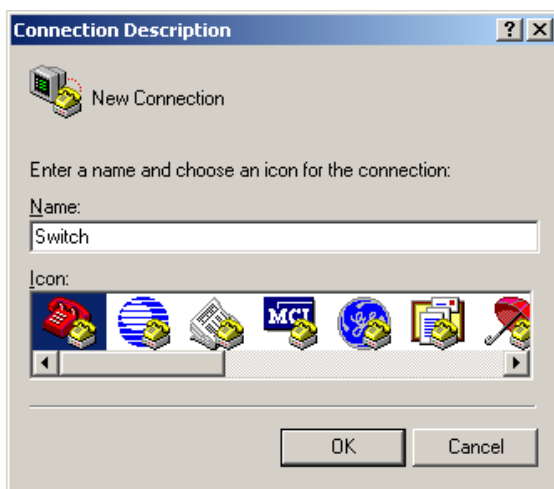
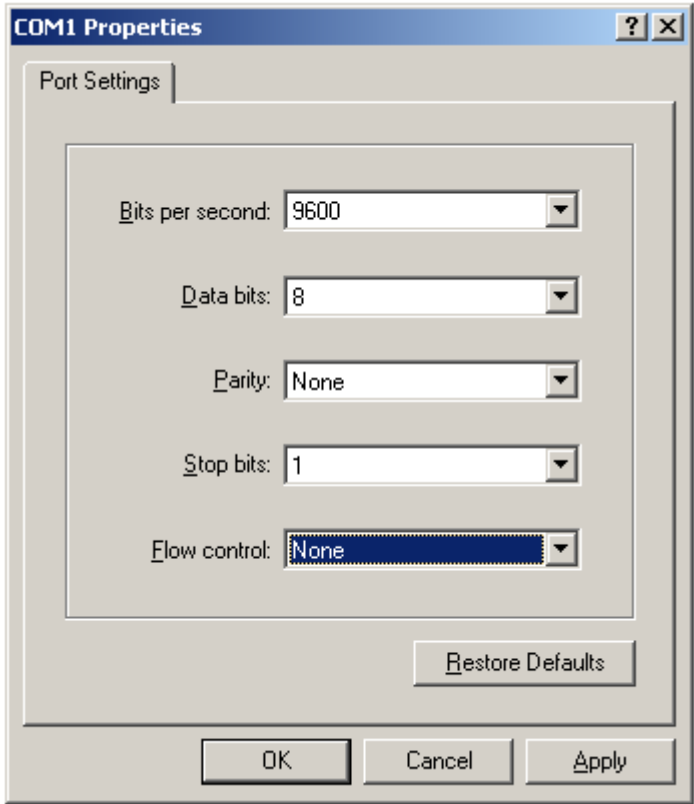




Figure 25 Specify the serial port used to establish the connection



Figure 26 Set the properties of the serial port



3. Turn on the device. You are prompted to enter the login password if the device successfully completes the POST. A prompt, such as <HP>, appears after you press **Enter**, as shown in [Figure 27](#).

**Figure 27 Configuration page**

```
id=0x19500fff,proc=0x508dc4
id=0x19510fff,proc=0x35b08c0
id=0x19518fff,proc=0x36f3348
id=0x19700100,proc=0x50c644
id=0x19700fff,proc=0xa8fd94
id=0x19703fff,proc=0xa8a9a4
id=0x1a000fff,proc=0x2225dc4
id=0x1cfff000,proc=0x21548dc
id=0x26000fff,proc=0x19cb7d0
id=0x27607100,proc=0x50a524

User interface aux0 is available.

Press ENTER to get started.
<HP>
#Jan 1 00:02:09:385 2007 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console
%Jan 1 00:02:09:386 2007 HP SHELL/5/SHELL_LOGIN: Console logged in from aux0.
<HP>_
```

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

## Logging in through modems

You can use two modems to remotely maintain a switch through its AUX port over the PSTN when the IP network connection is broken.

## Configuration requirements

For remote login through the AUX port using modems:

Object	Requirement
Administrator side	The PC is correctly connected to the modem.
	The modem is connected to a telephone cable that works properly.
	The telephone number of the remote modem connected to the AUX port of the remote switch is obtained.
Device side	The AUX port is correctly connected to the modem.
	Configurations have been configured on the modem.
	The modem is connected to a telephone cable that works properly.
	Authentication configuration has been completed on the remote switch.

## Login procedure

1. Set up a configuration environment as shown in [Figure 28](#):

### ⚠ CAUTION:

- The baud rate of the AUX port must be lower than the transmission rate of the modem. Otherwise, packets may be lost.
  - The parity check mode, stop bits, and data bits of the AUX port adopt the default settings.
- a. Connect the serial port of the PC and the AUX port of the device to a modem, respectively.
  - b. Connect the modems to a telephone cable, respectively.
  - c. Obtain the telephone number of the modem on the device side.

**Figure 28 Connect the PC to the device through modems**



2. Perform the following configurations on the modem 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&K0**—Disable local flow control
  - **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.

3. On the PC, launch a terminal emulation utility (such as HyperTerminal in Windows XP/Windows 2000) and create a connection by using the telephone number of the modem on the device side.

**Figure 29 Create a connection**



**Figure 30 Enter the phone number**



---

**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.

---

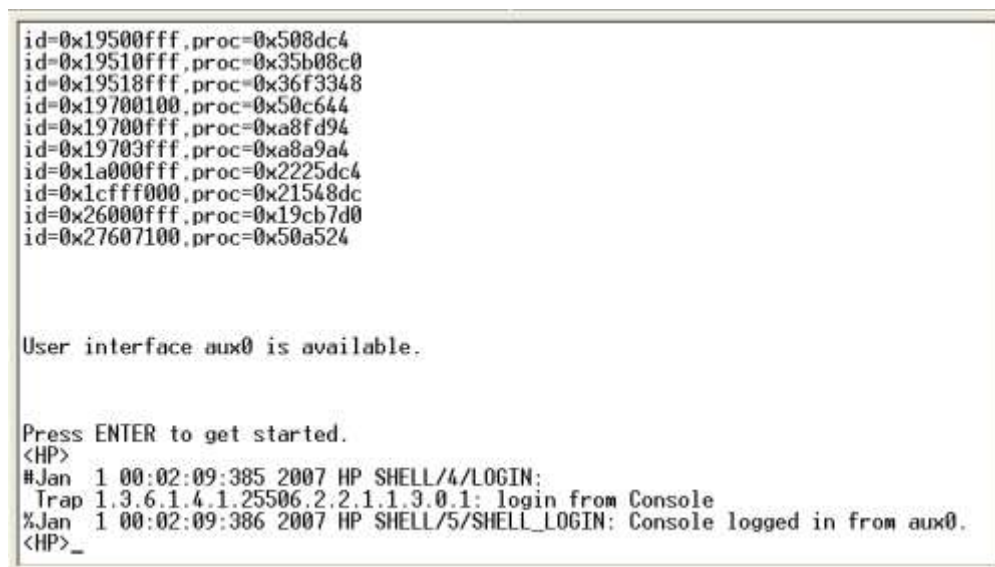
4. Dial the telephone number to establish a connection to the device.

### Figure 31 Dial the number




- When the character string `CONNECT9600` is displayed on the terminal, press **Enter** as prompted. A prompt, such as `<HP>`, appears.

### Figure 32 Configuration page



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

To terminate the connection between the PC and device, execute the **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**, execute the **ATH** command, and the connection is terminated if **OK** is displayed. You can also 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 may be always online, and you will fail to dial in next time.

## Modem login authentication modes

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

- **none**—Requires no username and password at login. This mode is insecure.
- **password**—Requires password authentication at login. Keep your password. If you lose your password, you cannot log in to the device through password authentication. You can log in to the device through the console port to view or modify the password.
- **scheme**—Uses AAA for user authentication, authorization, and accounting at login. AAA is a uniform framework for implementing network access management. This document describes only how to use AAA for local authentication and remote authentication. For more information about AAA configuration, see *Security Configuration Guide*. Keep your username and password. If you lose your local password, log in to the device through modems to view or modify the login password. If you lose your remote authentication password, contact the administrator.

**Table 15 Configuration required for different modem login authentication modes**

Authentication mode	Configuration	Remarks
None	Configure the device not to authenticate users.	See <a href="#">"Configuring none authentication for modem login."</a>
Password	Configure the device to authenticate users by using the local password.	See <a href="#">"Configuring password authentication for modem login."</a>
	Set the local password.	
AAA	Configure the device to use AAA for users.	See <a href="#">"Configuring AAA authentication for modem login."</a>
	Configure AAA on the device.	
	To configure local authentication:	
	1. Configure a local user and specify the password.	
	2. Configure the device to use local authentication.	
	To configure remote RADIUS or HWTACACS authentication:	
	1. Configure the RADIUS or HWTACACS scheme on the device.	
	2. Configure the username and password on the AAA server.	
	3. Configure the device to use the scheme for user authentication.	

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

## Configuring none authentication for modem login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter one or more AUX user interface views.	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
3. Specify the none authentication mode.	<b>authentication-mode none</b>	Required
4. Configure common settings for VTY user interfaces.	—	Optional See " <a href="#">Configuring common settings for VTY user interfaces (optional)</a> ."

After the configuration, when you log in to the device through modems, you are prompted to press **Enter**. A prompt, such as <HP>, appears after you press **Enter**, as shown in [Figure 33](#).

**Figure 33** Configuration page

```
*****
* 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. *
*****

User interface aux0 is available.

Please press ENTER.

<HP>
#Jan 1 00:06:13:765 2007 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console
#Jan 1 00:06:13:766 2007 HP SHELL/5/SHELL_LOGIN: Console logged in from aux0.
<HP>
```

## Configuring password authentication for modem login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter one or more AUX user interface views.	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
3. Specify the password authentication mode.	<b>authentication-mode password</b>	Required. By default, the modem login authentication mode of the device that has a separate AUX port is password, and that of the device with the console and AUX port sharing the same physical port is none.
4. Set the local password.	<b>set authentication password { cipher   simple } password</b>	Required. By default, no local password is set.
5. Configure common settings for VTY user interfaces.	—	Optional. For more information, see " <a href="#">Configuring common settings for VTY user interfaces (optional)</a> ".

After the configuration, when you log in to the device through modems, 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 34.

**Figure 34 Configuration page**

```

*****
* 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.                 *
*****

User interface aux0 is available.

Please press ENTER.

Login authentication

Password:
<HP>
#Jan 1 00:07:32:966 2007 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1: login from Console
%Jan 1 00:07:32:966 2007 HP SHELL/5/SHELL_LOGIN: Console logged in from aux0.
<HP>_

```



## Configuring AAA authentication for modem login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enter AUX user interface view.	<b>user-interface aux</b> <i>first-number</i> [ <i>last-number</i> ]	—
3. Specify the AAA authentication mode.	<b>authentication-mode scheme</b>	<p>Required.</p> <p>Whether local, RADIUS, or HWTACACS authentication is adopted depends on the configured AAA scheme.</p> <p>By default, the modem login authentication mode of the device that has a separate AUX port is password, and that of the device with the console and AUX port sharing the same physical port is none.</p>
4. Enable command authorization.	<b>command authorization</b>	<p>Optional.</p> <ul style="list-style-type: none"><li>• By default, command authorization is not enabled.</li><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 yes, the command can be executed.</li></ul>
5. Enable command accounting.	<b>command accounting</b>	<p>Optional</p> <ul style="list-style-type: none"><li>• By default, command accounting is disabled. The accounting server does not record the commands executed by users.</li><li>• 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.</li></ul>

Step	Command	Remarks
6. Exit to system view.	<b>quit</b>	—
7. Configure authentication mode.	a. Enter default ISP domain view. <b>domain</b> <i>domain- name</i>	Optional. By default, the AAA scheme is <b>local</b> .
	b. Apply specified AAA scheme to domain. <b>authentication default</b> { <b>hwtaacs- scheme</b> <i>hwtaacs- scheme-name</i> [ <b>local</b> ]   <b>local</b>   <b>none</b>   <b>radius- scheme</b> <i>radius- scheme-name</i> [ <b>local</b> ] }	If you specify the local AAA scheme, perform the configuration concerning local user as well. If you specify an existing scheme by providing the <i>radius-scheme-name</i> argument, perform the following configuration as well: <ul style="list-style-type: none"><li>For RADIUS and HWTACACS configuration, see <i>Security Configuration Guide</i>.</li><li>Configure the username and password on the AAA server. (For more information, see <i>Security Configuration Guide</i>.)</li></ul>
	c. Return to system view. <b>quit</b>	
8. Create local user and enter local user view.	<b>local-user</b> <i>user- name</i>	Required.
9. Set authentication password for local user.	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required.
10. Specify command level of local user.	<b>authorization-attribute level</b> <i>level</i>	Optional. By default, the command level is 0.
11. Specify service type for local user.	<b>service-type terminal</b>	Required. By default, no service type is specified.
12. Configure common settings for VTY user interfaces.	—	Optional. See " <a href="#">Configuring common settings for VTY user interfaces (optional)</a> ."

After enabling 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 **authorization-attribute level** *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*.

After the configuration, when you log in to the device through modems, 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 35.

**Figure 35 Configuration page**

```
*****
* 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.                 *
*****

User interface aux0 is available.

Please press ENTER.

Login authentication

Username:abcd
Password:
<HP>
#Jan 1 00:08:25:152 2007 HP SHELL/4/LOGIN:
Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:abcd login from Console
%Jan 1 00:08:25:152 2007 HP SHELL/5/SHELL_LOGIN: abcd logged in from aux0.
<HP>
```

## Configuring common settings for modem login (optional)

### ⚠ CAUTION:

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

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable display of copyright information.	<b>copyright-info enable</b>	Optional. Enabled by default.
3. Enter AUX interface view.	<b>interface aux 0</b>	—
4. Set the work mode to flow.	<b>async mode { flow   protocol }</b>	Optional. <b>flow</b> by default.
5. Enter one or more AUX user interface views.	<b>user-interface aux first-number [ last-number ]</b>	—

Step	Command	Remarks
6. Configure AUX port properties.	a. Configure baud rate. <b>speed</b> <i>speed-value</i>	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.
	b. Configure baud rate. <b>parity</b> { <b>even</b>   <b>mark</b>   <b>none</b>   <b>odd</b>   <b>space</b> }	Optional. By default, the parity check mode of the AUX port is set to <b>none</b> , which means no check bit.
	c. Configure baud rate. <b>stopbits</b> { <b>1</b>   <b>1.5</b>   <b>2</b> }	Optional. By default, the stop bits 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.
	d. Configure baud rate. <b>databits</b> { <b>5</b>   <b>6</b>   <b>7</b>   <b>8</b> }	Optional. By default, the data bits of the AUX port is 8. Data bits is the number of bits representing one character. The setting depends on the contexts to be transmitted. For example, you can set it to 7 if standard ASCII characters are to be sent, and set it to 8 if extended ASCII characters are to be sent.
	e. Configure baud rate. <b>activation-key</b> <i>character</i>	Optional. By default, you can press <b>Enter</b> to start a session.
	f. Configure baud rate. <b>escape-key</b> { <b>default</b>   <i>character</i> }	Optional. By default, you can press <b>Ctrl+C</b> to terminate a task.

Step		Command	Remarks
g.	Configure stop bits detection.	<b>stopbit-error intolerance</b>	Optional. By default, no stop bits are detected.
h.	Configure flow control mode.	<b>flow-control { hardware   none   software }</b> <b>flow-control hardware</b> <i>flow-control-type1</i> [ <b>software</b> <i>flow-control-type2</i> ] <b>flow-control software</b> <i>flow-control-type1</i> [ <b>hardware</b> <i>flow-control-type2</i> ]	Optional. By default, an independent AUX port performs hardware flow control, and an AUX/console port does not perform any flow control.
i.	Configure terminal display type.	<b>terminal type { ansi   vt100 }</b>	Optional. By default, the terminal display type is ANSI. The device supports two types of terminal display: ANSI and VT100. HP recommends you to set 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.
j.	Configure user privilege level for login users.	<b>user privilege level</b> <i>level</i>	Optional. 3 by default.
k.	Set maximum number of lines on next screen.	<b>screen-length</b> <i>screen-length</i>	Optional. By default, the next screen displays 24 lines at most. A value of 0 disables the function.

Step	Command	Remarks
<b>l.</b> Set the history command buffer size.	<b>history-command max-size</b> <i>value</i>	Optional. By default, the buffer saves 10 history commands at most.
<b>m.</b> Set idle-timeout timer.	<b>idle-timeout</b> <i>minutes</i> [ <i>seconds</i> ]	Optional. The default idle-timeout is 10 minutes. The system automatically terminates the user's connection if there is no information interaction between the device and the user within the idle-timeout time. Setting idle-timeout to 0 disables the timer.
<b>n.</b> Set maximum interval allowed between off-hook and dialing.	<b>modem timer answer</b> <i>time</i>	Optional. By default, the interval is 60 seconds.
<b>o.</b> Configure modem to operate in auto-answer mode.	<b>modem auto-answer</b>	Optional By default, a modem operates in nonauto answer mode.
<b>p.</b> Enable modem call-in/call-out on user interface.	<b>modem</b> { <b>both</b>   <b>call-in</b>   <b>call-out</b> }	Optional. By default, both modem call-in and call-out are disabled.

## Displaying and maintaining CLI login

Task	Command	Remarks
Display information about the user interfaces that are being used.	<b>display users</b> [ [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.
Display information about all user interfaces that the device supports.	<b>display users all</b> [ [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.
Display user interface information.	<b>display user-interface</b> [ <i>num1</i>   { <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> } <i>num2</i> ] [ <b>summary</b> ] [ [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.
Display the configuration of the device when it serves as a Telnet client.	<b>display telnet client configuration</b> [ [ { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.

Task	Command	Remarks
Release a specified user interface.	<b>free user-interface</b> { <i>num1</i>   { <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> } <i>num2</i> }	<p>Available in user view.</p> <p>Multiple users can log in to the system to simultaneously configure the device. In some circumstances, when the administrator wants to make configurations without interruption from the users logged in through other user interfaces, the administrator can execute the command to release the connections established on the specified user interfaces.</p> <p>You cannot use this command to release the connection you are using.</p>
Lock the current user interface.	<b>lock</b>	<p>Available in user view.</p> <p>By default, the current user interface is not locked.</p>
Send messages to the specified user interfaces.	<b>send</b> { <b>all</b>   <i>num1</i>   { <b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b> } <i>num2</i> }	Available in user view.

# Web login

The device provides a built-in web server. It enables you to log in to the web interface of the device from a PC.

The device supports the following web login methods:

- **HTTP login**—the HTTP is used for transferring web page information across the Internet. It is an application-layer protocol in the TCP/IP protocol suite. The connection-oriented TCP is adopted at the transport layer. The device supports HTTP 1.0.
- **HTTPS login**—the HTTPS refers to the HTTP protocol that supports the SSL protocol. HTTPS uses SSL to encrypt the data exchanged between the HTTPS client and the server to ensure data security and integrity. You can define a certificate attribute-based access control policy to allow legal clients to access the device securely and prohibit illegal clients.

## Configuration requirements

Object	Requirements
Device	Configure the IP address of the device interface. Make sure the device and the PC can reach each other.
	By default, the IP address of the device is 192.168.1.1/24.
	<a href="#">Configuring HTTP login.</a> <a href="#">Configuring HTTPS login.</a> Required to use one approach.
PC	Install a web browser.
	Obtain the IP address of the device interface.

## Configuring HTTP login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable the HTTP service.	<b>ip http enable</b>	Required. Enabled by default.
3. Configure the HTTP service port number.	<b>ip http port</b> <i>port-number</i>	Optional. 80 by default. If you execute the command multiple times, the last one takes effect.



Step	Command	Remarks
4. Associate the HTTP service with an ACL.	<b>ip http acl</b> <i>acl-number</i>	Optional. By default, the HTTP service is not associated with any ACL. Associating the HTTP service with an ACL enables the device to allow only clients permitted by the ACL to access the device.
5. Create a local user and enter local user view.	<b>local-user</b> <i>user-name</i>	Required.
6. Configure a password for the local user.	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required. By default, no password is configured for the local user.
7. Specify the command level of the local user.	<b>authorization-attribute level</b> <i>level</i>	Required. No command level is configured for the local user.
8. Specify the Telnet service type for the local user.	<b>service-type web</b>	Required. By default, no service type is configured for the local user.
9. Exit to system view.	<b>quit</b>	—
10. Enter interface view.	<b>interface</b> <i>interface-type</i> { <i>interface-number</i>   <i>interface-number.subnumber</i> }	Required.
11. Assign an IP address and subnet mask to the device interface.	<b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> }	Required.

# Configuring HTTPS login

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Associate the HTTPS service with an SSL server policy.	<b>ip https ssl-server-policy</b> <i>policy-name</i>	<p>Required.</p> <p>By default, the HTTPS service is not associated with any SSL server policy.</p> <ul style="list-style-type: none"><li>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.</li><li>Any changes to the SSL server policy associated with the HTTP service that is enabled do not take effect.</li></ul>
3. Enable the HTTPS service.	<b>ip https enable</b>	<p>Required.</p> <p>Disabled by default.</p> <p>Enabling the HTTPS service triggers an SSL handshake negotiation process. During the process, if the local certificate of the device exists, the SSL negotiation succeeds, and the HTTPS service can be started properly. If no local certificate exists, a certificate application process is triggered by the SSL negotiation. Because the application process takes much time, the SSL negotiation often fails and the HTTPS service cannot be started normally. In that case, you must execute <b>ip https enable</b> multiple times to start the HTTPS service.</p>
4. Associate the HTTPS service with a certificate attribute-based access control policy.	<b>ip https certificate access-control-policy</b> <i>policy-name</i>	<p>Optional.</p> <p>By default, the HTTPS service is not associated with any certificate-based attribute access control policy.</p> <ul style="list-style-type: none"><li>Associating the HTTPS service with a certificate-based attribute access control policy enables the device to control the access rights of clients.</li><li>You must configure <b>client-verify enable</b> in the associated SSL server policy. If not, no clients can log in to the device.</li><li>The associated SSL server policy must contain at least one <b>permit</b> rule. Otherwise, no clients can log in to the device.</li><li>For more information about certificate attribute-based access control policies, see <i>Security Configuration Guide</i>.</li></ul>
5. Configure the port number of the HTTPS service.	<b>ip https port</b> <i>port-number</i>	<p>Optional.</p> <p>443 by default.</p>

Step	Command	Remarks
6. Associate the HTTPS service with an ACL.	<b>ip https acl</b> <i>acl-number</i>	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.
7. Create a local user and enter local user view.	<b>local-user</b> <i>user-name</i>	Required.
8. Configure a password for the local user.	<b>password</b> { <b>cipher</b>   <b>simple</b> } <i>password</i>	Required. By default, no password is configured for the local user.
9. Specify the command level of the local user.	<b>authorization-attribute level</b> <i>level</i>	Required. By default, no command level is configured for the local user.
10. Specify the Telnet service type for the local user.	<b>service-type telnet</b>	Required. By default, no service type is configured for the local user.
11. Exit to system view.	<b>quit</b>	—
12. Enter interface view.	<b>interface</b> <i>interface-type</i> { <i>interface-number</i>   <i>interface-number.subnumber</i> }	Required.
13. Assign an IP address and subnet mask to the device interface.	<b>ip address</b> <i>ip-address</i> { <i>mask</i>   <i>mask-length</i> }	Required.

## Displaying and maintaining web login

Task	Command	Remarks
Display information about web users.	<b>display web users</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.
Display HTTP state information.	<b>display ip http</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.
Display HTTPS state information.	<b>display ip https</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.

# Configuration examples

## HTTP login example

### Network requirements

As shown in [Figure 36](#), the PC is connected to the device over an IP network. The IP address of the Device is 192.168.0.22/24.

Use the PC to log in to the device through HTTP.

**Figure 36 Network diagram**



### Configuration procedure

#### 1. Configure the device

# Configure the IP address of the interface Ethernet 1/1 as 192.168.0.22 and the subnet mask as 255.255.255.0.

```
[Sysname] interface ethernet1/1
[Sysname-Ethernet1/1] ip address 192.168.0.22 255.255.255.0
[Sysname-Ethernet1/1] quit
```

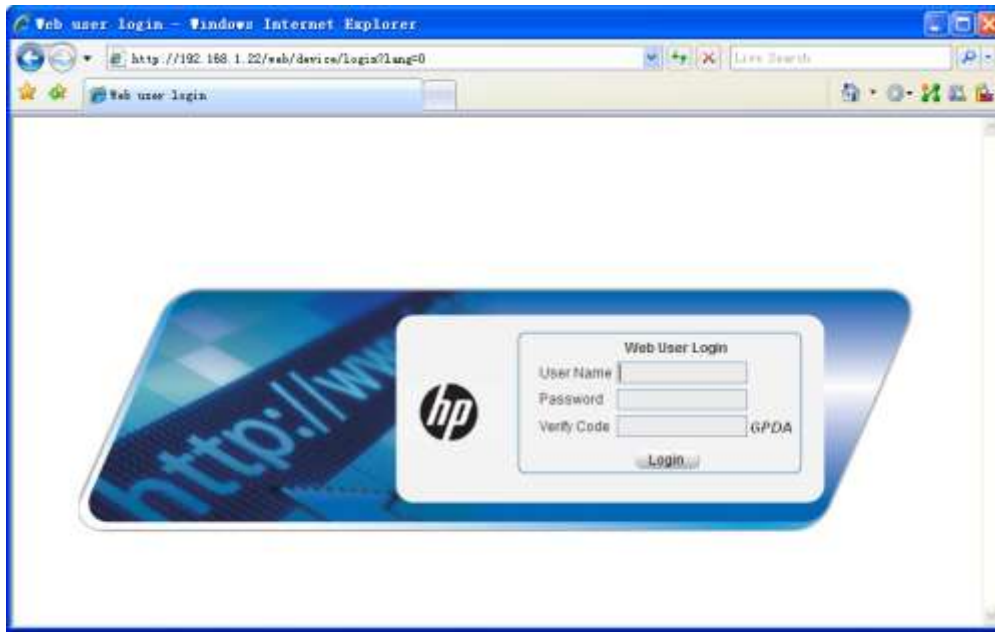
# Create a local user named **admin**, and set the password to **admin** for the user. Specify the Telnet service type for the local user, and set the command level to 3 for this user.

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

#### 2. Use the PC to log in to the device

# On the PC, run the web browser. Enter the IP address of the device in the address bar. The web login page appears.

Figure 37 Web login page



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

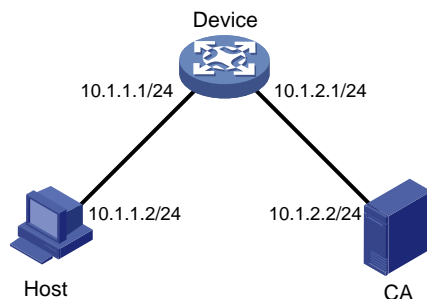
## HTTPS login example

### Network requirements

As shown in Figure 38, 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.
- Configure the host to act as the HTTPS client. Request a certificate for it.
- Install SCEP add-on on the CA and set the computer's name to **new-ca**. In this example, the CA runs Windows Server, and is used to issue certificates to the device and host.

Figure 38 Network diagram



### Configuration procedure

Before performing the following configuration, ensure the Device, Host, and CA can reach each other.

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

# NMS login

An 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. At present, the device supports multiple NMS programs, such as IMC.

Configuration requirements of NMS login:

Object	Requirements
Device	Configure the IP address of the device interface
	Make sure the device and the NMS can reach each other
	Configure SNMP settings
NMS	Configure the NMS. For more information, see the manual of your NMS

## Configuring NMS login

Connect the Ethernet port of the PC to an Ethernet port of the device, as shown in [Figure 39](#). Ensure the PC and device can reach each other.

**Figure 39 Network diagram for configuring NMS login**



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

To configure SNMPv1 and SNMPv2c settings:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable SNMP agent.	<b>snmp-agent</b>	Optional. Disabled by default. You can enable SNMP agent with this command or any command that begins with <b>snmp-agent</b> .
3. Create or update MIB view information.	<b>snmp-agent mib-view { excluded   included } view-name oid-tree [ mask mask-value ]</b>	Optional. By default, the MIB view name is ViewDefault and OID is 1.



Step		Command	Remarks
4. Configure SNMP NMS access right.	Directly	Configure SNMP community.  <b>snmp-agent community { read   write } community-name [ acl acl-number   mib-view view-name ]*</b>	Required. Use either approach.
	Indirectly	a. Configure SNMP group.  <b>snmp-agent group { v1   v2c } group-name [ read-view read-view [ write-view write-view [ notify-view notify-view ] [ acl acl-number ]</b>	The direction configuration approach is for SNMPv1 or SNMPv2c. The community name configured on the NMS should be consistent with the username configured on the agent. The indirect configuration approach is for SNMPv3.
		b. Add user to SNMP group.  <b>snmp-agent usm-user { v1   v2c } user-name group-name [ acl acl-number ]</b>	

To configure SNMPv3 settings:

Step...	Command...	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable SNMP agent.	<b>snmp-agent</b>	Optional. Disabled by default. You can enable SNMP agent by using any command that begins with <b>snmp-agent</b> (except for <b>snmp-agent calculate-password</b> ).
3. Configure an SNMP group and specify its access right.	<b>snmp-agent group v3 group-name [ authentication   privacy ] [ read-view read-view [ write-view write-view [ notify-view notify-view ] [ acl acl-number ]</b>	Required. By default, no SNMP group is configured.
4. Add a user to the SNMP group.	<b>snmp-agent usm-user v3 user-name group-name [ [ cipher ] authentication-mode { md5   sha } auth-password [ privacy-mode { 3des   aes128   des56 } priv-password ] [ acl acl-number ]</b>	Required. If the <b>cipher</b> keyword is specified, both <i>auth-password</i> and <i>priv-password</i> are cipher text passwords.

# NMS login example

In this example, IMC is used as the NMS for illustration.

## 1. Configure the device

# Assign 1.1.1.1/24 for the IP address of device. Make sure the device and the NMS can reach each other. (Details not shown)

# Enter system view.

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

# Enable the SNMP agent.

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

# Configure an SNMP group.

```
[Sysname] snmp-agent group v3 managev3group read-view test write-view test
```

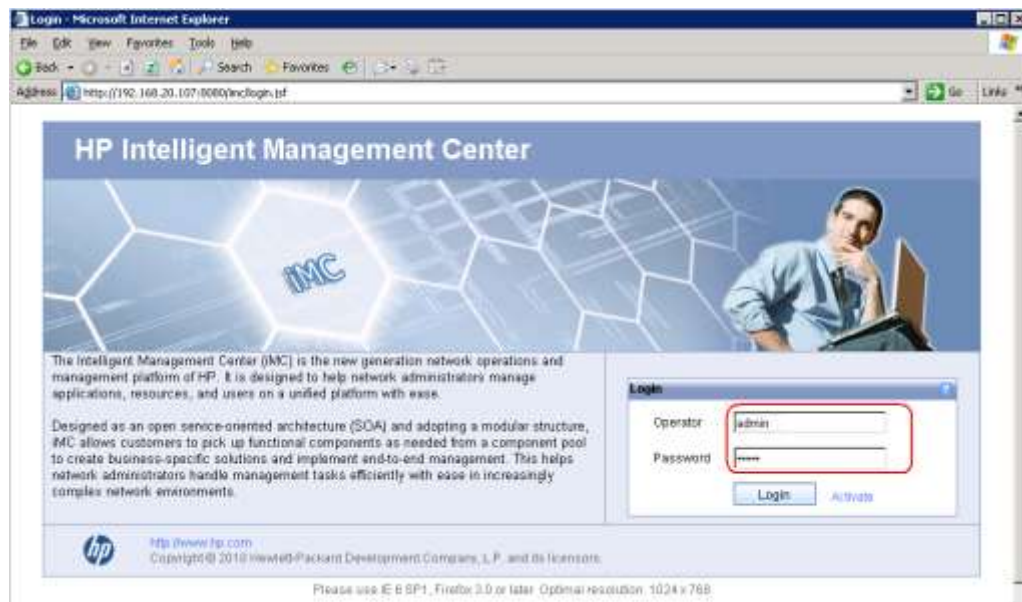
# Add a user to the SNMP group.

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

## 2. Configure the NMS

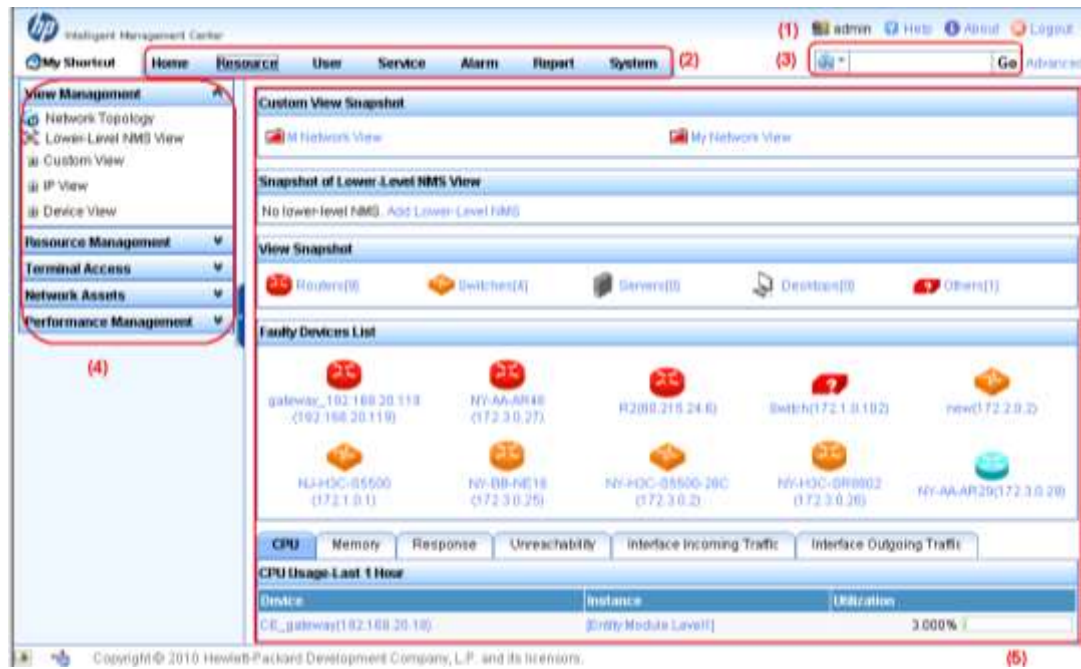
On the PC, start the browser. In the address bar, enter **http://192.168.4.112:8080/IMC**, where 192.168.4.112 is the IP address of the IMC.

Figure 40 IMC login page



Enter the username and password, and then click **Login**. The IMC homepage appears, as shown in Figure 41.

Figure 41 IMC homepage



Log in to the IMC and configure SNMP settings for the IMC to find the device. After the device is found, you can 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 help information.

# User login control

The device provides the following login control methods:

Login through	Login control methods	ACL used
Telnet	Configuring source IP-based login control over Telnet users	Basic ACL
	Configuring source and destination IP-based login control over Telnet users	Advanced ACL
	Configuring source MAC-based login control over Telnet users	Ethernet frame header ACL
NMS	Configuring source IP-based login control over NMS users	Basic ACL
Web	Configuring source IP-based login control over web users	Basic ACL

## Configuring login control over Telnet users

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

Basic ACLs match the source IP addresses of packets, so you can 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*.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Create a basic ACL and enter its view, or enter the view of an existing basic ACL.	<b>acl [ ipv6 ] number <i>acl-number</i></b> <b>[ name <i>name</i> ] [ match-order { config   auto } ]</b>	Required. By default, no basic ACL exists.
3. Configure rules for an IPv4 basic ACL.	<b>rule [ <i>rule-id</i> ] { deny   permit }</b> <b>[ counting   fragment   logging  </b> <b>source { <i>sour-addr</i> <i>sour-wildcard</i>  </b> <b>any }   time-range <i>time-range-</i></b> <b><i>name</i>   vpn-instance <i>vpn-instance-</i></b> <b><i>name</i> ] *</b>	Required in an IPv4 networking environment. By default, an IPv4 basic ACL does not contain any rule. The <b>logging</b> function is available only when the application module that uses the ACL supports the logging function.

Step	Command	Remarks
4. Configure rules for an IPv6 basic ACL.	<b>rule</b> [ <i>rule-id</i> ] { <b>deny</b>   <b>permit</b> } [ <b>counting</b>   <b>fragment</b>   <b>logging</b>   <b>source</b> { <i>ipv6-address prefix-length</i>   <i>ipv6-address/prefix-length</i>   <b>any</b> }   <b>time-range</b> <i>time-range-name</i>   <b>vpn-instance</b> <i>vpn-instance-name</i> ] *	Required in an IPv6 networking environment. By default, an IPv6 basic ACL does not contain any rule. The <b>logging</b> function is available only when the application module that uses the ACL supports the logging function.
5. Exit the basic ACL view.	<b>quit</b>	—
6. Enter user interface view.	<b>user-interface</b> [ <i>type</i> ] <i>first-number</i> [ <i>last-number</i> ]	—
7. Use the ACL to control user login by source IP address.	<b>acl</b> [ <b>ipv6</b> ] <i>acl-number</i> { <b>inbound</b>   <b>outbound</b> }	Required. <b>inbound</b> : Filters incoming Telnet packets. <b>outbound</b> : Filters outgoing Telnet packets.

## Configuring source and destination IP-based login control over Telnet users

Advanced ACLs can match both source and destination IP addresses of packets, so you can 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:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Create an advanced ACL and enter its view, or enter the view of an existing advanced ACL.	<b>acl</b> [ <b>ipv6</b> ] <b>number</b> <i>acl-number</i> [ <b>name</b> <i>name</i> ] [ <b>match-order</b> { <b>config</b>   <b>auto</b> } ]	Required. By default, no advanced ACL exists.
3. Configure rules for the ACL.	<b>rule</b> [ <i>rule-id</i> ] { <b>permit</b>   <b>deny</b> } <i>rule-string</i>	Required.
4. Exit advanced ACL view.	<b>quit</b>	—
5. Enter user interface.	<b>user-interface</b> [ <i>type</i> ] <i>first-number</i> [ <i>last-number</i> ]	—
6. Use the ACL to control user login by source and destination IP addresses.	<b>acl</b> [ <b>ipv6</b> ] <i>acl-number</i> { <b>inbound</b>   <b>outbound</b> }	Required. <ul style="list-style-type: none"> <li><b>inbound</b>—Filters incoming Telnet packets.</li> <li><b>outbound</b>—Filters outgoing Telnet packets.</li> </ul>

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

Ethernet frame header ACLs can match the source MAC addresses of packets, so you can 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*.

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

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Create an Ethernet frame header ACL and enter its view.	<b>acl number</b> <i>acl-number</i> [ <b>name</b> <i>name</i> ] [ <b>match-order</b> { <b>config</b>   <b>auto</b> } ]	Required. By default, no Ethernet frame header ACL exists.
3. Configure rules for the ACL.	<b>rule</b> [ <i>rule-id</i> ] { <b>permit</b>   <b>deny</b> } <i>rule-string</i>	Required.
4. Exit the advanced ACL view.	<b>quit</b>	—
5. Enter user interface view.	<b>user-interface</b> [ <i>type</i> ] <i>first-number</i> [ <i>last-number</i> ]	—
6. Use the ACL to control user login by source MAC address.	<b>acl</b> <i>acl-number</i> <b>inbound</b>	Required. <b>inbound</b> : Filters incoming Telnet packets.

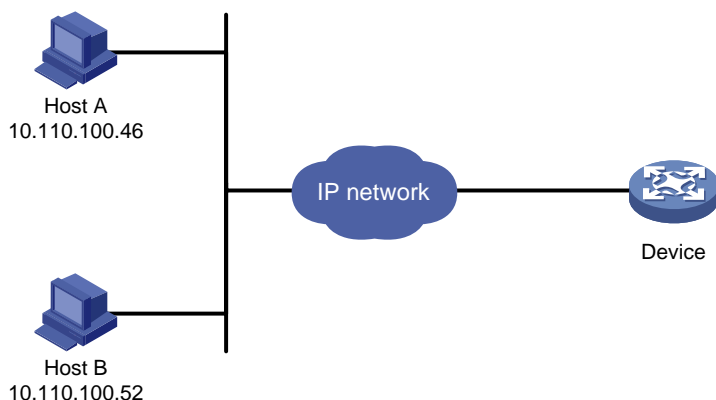
The configuration does not take effect if the Telnet client and server are not in the same subnet.

## Source MAC-based login control configuration example

### Network requirements

As shown in Figure 42, configure an ACL on the Device to permit only incoming Telnet packets sourced from Host A and Host B.

Figure 42 Network diagram



## Configuration procedure

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

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

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

```
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] acl 2000 inbound
```

# Configuring source IP-based login control over NMS users

You can 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, you can control SNMP user access to the device.

## Configuration preparation

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

## Configuration steps

Basic ACLs match the source IP addresses of packets, so you can 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*.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Create a basic ACL and enter its view, or enter the view of an existing basic ACL.	<b>acl</b> [ <b>ipv6</b> ] <b>number</b> <i>acl-number</i> [ <b>name</b> <i>name</i> ] [ <b>match-order</b> { <b>config</b>   <b>auto</b> } ]	Required. By default, no basic ACL exists.
3. Create rules for this ACL.	<b>rule</b> [ <i>rule-id</i> ] { <b>deny</b>   <b>permit</b> } [ <b>counting</b>   <b>fragment</b>   <b>logging</b>   <b>source</b> { <i>sour-addr</i> <i>sour-wildcard</i>   <b>any</b> }   <b>time-range</b> <i>time-range-name</i>   <b>vpn-instance</b> <i>vpn-instance-name</i> ] *	Required.
4. Exit the basic ACL view.	<b>quit</b>	—
5. Associate this SNMP community with the ACL.	<b>snmp-agent community</b> { <b>read</b>   <b>write</b> } <i>community-name</i> [ <b>acl</b> <i>acl-number</i>   <b>mib-view</b> <i>view-name</i> ] *	Required.

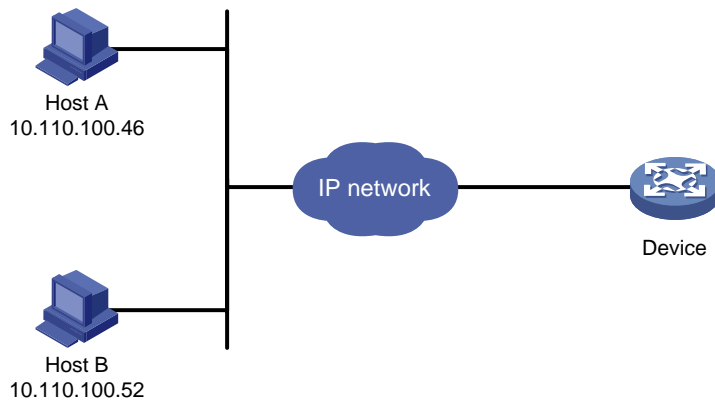
Step	Command	Remarks
6. Associate the SNMP group with the ACL.	<pre>snmp-agent group { v1   v2c } group-name [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl acl-number ]</pre> <pre>snmp-agent group v3 group-name [ authentication   privacy ] [ read-view read-view ] [ write-view write-view ] [ notify-view notify-view ] [ acl acl-number ]</pre>	<p>You can associate the ACL when creating the community, the SNMP group, and the user.</p> <p>For more information about SNMP, see <i>Network Management and Monitoring Configuration Guide</i>.</p>
7. Associate the user with the ACL.	<pre>snmp-agent usm-user { v1   v2c } user-name group-name [ acl acl-number ]</pre> <pre>snmp-agent usm-user v3 user-name group-name [ [ cipher ] authentication-mode { md5   sha } auth-password [ privacy-mode { 3des   aes128   des56 } priv-password ] [ acl acl-number ]</pre>	

## Configuration example

### Network requirements

As shown in [Figure 43](#), configure the device to allow only NMS users from Host A and Host B to access.

**Figure 43 Network diagram**



### Configuration procedure

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

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

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

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



# Configuring source IP-based login control over web users

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

## Configuration preparation

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

## Configuration steps

Basic ACLs match the source IP addresses of packets, so you can 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*.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Create a basic ACL and enter its view, or enter the view of an existing basic ACL.	<b>acl</b> [ <b>ipv6</b> ] <b>number</b> <i>acl-number</i> [ <b>name</b> <i>name</i> ] [ <b>match-order</b> { <b>config</b>   <b>auto</b> } ]	Required. By default, no basic ACL exists.
3. Create rules for this ACL.	<b>rule</b> [ <i>rule-id</i> ] { <b>deny</b>   <b>permit</b> } [ <b>counting</b>   <b>fragment</b>   <b>logging</b>   <b>source</b> { <i>sour-addr</i> <i>sour-wildcard</i>   <b>any</b> }   <b>time-range</b> <i>time-range-name</i>   <b>vpn-instance</b> <i>vpn-instance-name</i> ] *	Required.
4. Exit the basic ACL view.	<b>quit</b>	—
5. Associate the HTTP service with the ACL.	<b>ip http acl</b> <i>acl-number</i>	Required to use one command.
6. Associate the HTTPS service with the ACL.	<b>ip https acl</b> <i>acl-number</i>	

## Logging off online web users

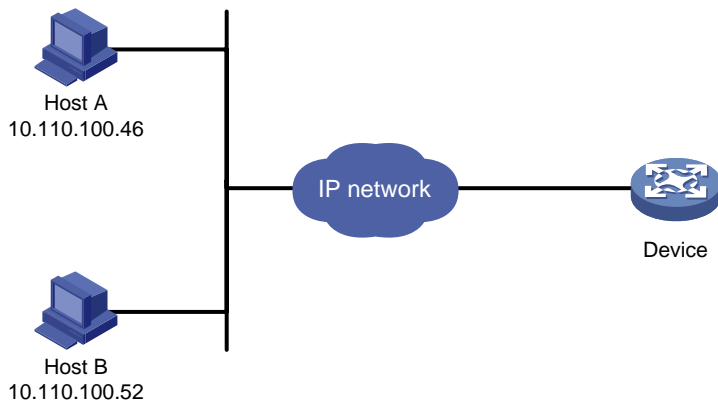
Task	Command	Remarks
Log off online web users.	<b>free web-users</b> { <b>all</b>   <b>user-id</b> <i>user-id</i>   <b>user-name</b> <i>user-name</i> }	Required. Execute the command in user interface view.

# Configuration example

## Network requirements

As shown in [Figure 44](#), configure the device to allow only web users from Host B to access.

**Figure 44 Network diagram**



## Configuration procedure

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

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

```
[Sysname] acl number 2030 match-order config
```

```
[Sysname-acl-basic-2030] rule 1 permit source 10.110.100.52 0
```

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

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

# Device management

## Overview

Device management includes monitoring the operating status of devices and configuring their running parameters.

Flash memory is exemplified in this document.

The configuration tasks in this document are order independent. You can perform these tasks in any order.

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Supported storage medium	Flash memory USB disk	Flash memory USB disk	CF card USB disk	Flash memory (supported by the MSR30-10, MSR30-11E, and MSR30-11F) CF card (supported by the MSR30-16, MSR30-20, MSR30-40, and MSR30-60) USB disk	Flash memory (not supported by the MPUF) CF card USB disk

## Configuring the device name

A device name identifies a router in a network and works as the user view prompt at the CLI. For example, if the device name is **Sysname**, the user view prompt is <Sysname>.

To configure the device name:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure the device name.	<b>sysname</b> <i>sysname</i>	Optional. The default device name is <b>HP</b> .

## Changing the system time

You must synchronize your device with a trusted time source by using NTP or changing the system time before you run it on the network. Network management depends on an accurate system time setting, because the timestamps of system messages and logs use the system time.

In a small-sized network, you can manually set the system time of each device.

## Configuration guidelines

You can change the system time by configuring the relative time, time zone, and daylight saving time. The configuration result depends on their configuration order (see [Table 16](#)). In the first column of this table, 1 represents the **clock datetime** command, 2 represents the **clock timezone** command, and 3 represents the **clock summer-time** command. To verify the system time setting, use the **display clock** command. This table assumes that the original system time is 2005/1/1 1:00:00.

**Table 16 System time configuration results**

Command	Effective system time	Configuration example	System time
1	<i>date-time</i>	clock datetime 1:00 2007/1/1	01:00:00 UTC Mon 01/01/2007
2	Original system time $\pm$ zone-offset	clock timezone zone-time add 1	02:00:00 zone-time Sat 01/01/2005
1, 2	<i>date-time</i> $\pm$ zone-offset	clock datetime 2:00 2007/2/2 clock timezone zone-time add 1	03:00:00 zone-time Fri 02/02/2007
2, 1	<i>date-time</i>	clock timezone zone-time add 1 clock datetime 3:00 2007/3/3	03:00:00 zone-time Sat 03/03/2007
3	Original system time outside daylight saving time range. System time does not change until it falls into daylight saving time range.	clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2	01:00:00 UTC Sat 01/01/2005
	Original system time in daylight saving time range: The system time increases by <i>summer-offset</i> .	clock summer-time ss one-off 00:30 2005/1/1 1:00 2005/8/8 2	03:00:00 ss Sat 01/01/2005 If original system time plus <i>summer-offset</i> is beyond daylight saving time range, original system time does not change. After disabling daylight saving setting, system time automatically decreases by <i>summer-offset</i> .
	<i>date-time</i> outside daylight saving time range: <i>date-time</i>	clock datetime 1:00 2007/1/1 clock summer-time ss one-off 1:00 2006/1/1 1:00 2006/8/8 2	01:00:00 UTC Mon 01/01/2007
1, 3	<i>date-time</i> in the daylight saving time range: <i>date-time</i> + <i>summer-offset</i>	clock datetime 8:00 2007/1/1 clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2	10:00:00 ss Mon 01/01/2007 If <i>date-time</i> plus <i>summer-offset</i> is outside daylight saving time range, system time equals <i>date-time</i> . After disabling daylight saving setting, system time automatically decreases by <i>summer-offset</i> .

Command	Effective system time	Configuration example	System time
3, 1 (date-time outside the daylight saving time range)	<i>date-time</i>	clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 clock datetime 1:00 2008/1/1	01:00:00 UTC Tue 01/01/2008
3, 1 (date-time in the daylight saving time range)	<i>date-time – summer-offset</i> outside daylight saving time range: <i>date-time – summer-offset</i>	clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 clock datetime 1:30 2007/1/1	23:30:00 UTC Sun 12/31/2006
	<i>date-time – summer-offset</i> in daylight saving time range: <i>date-time</i>	clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2 clock datetime 3:00 2007/1/1	03:00:00 ss Mon 01/01/2007
2, 3 or 3, 2	Original system clock $\pm$ zone-offset outside daylight saving time range: Original system clock $\pm$ zone-offset	clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2	02:00:00 zone-time Sat 01/01/2005
	Original system clock $\pm$ zone-offset outside daylight saving time range: Original system clock $\pm$ zone-offset + summer-offset	clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2005/1/1 1:00 2005/8/8 2	System clock configured: 04:00:00 ss Sat 01/01/2005
1, 2, 3 or 1, 3, 2	<i>date-time <math>\pm</math> zone-offset</i> outside daylight saving time range: <i>date-time <math>\pm</math> zone-offset</i>	clock datetime 1:00 2007/1/1 clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2	02:00:00 zone-time Mon 01/01/2007
	<i>date-time <math>\pm</math> zone-offset</i> outside daylight saving time range: <i>date-time <math>\pm</math> zone-offset + summer-offset</i>	clock datetime 1:00 2007/1/1 clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2007/1/1 1:00 2007/8/8 2	04:00:00 ss Mon 01/01/2007

Command	Effective system time	Configuration example	System time
2, 3, 1 or 3, 2, 1	<i>date-time</i> outside daylight saving time range: <i>date-time</i>	clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 clock datetime 1:00 2007/1/1	01:00:00 zone-time Mon 01/01/2007
	<i>date-time</i> in daylight saving time range, but <i>date-time</i> – <i>summer-offset</i> outside summer-time range: <i>date-time</i> – <i>summer-offset</i>	clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 clock datetime 1:30 2008/1/1	23:30:00 zone-time Mon 12/31/2007
	Both <i>date-time</i> and <i>date-time</i> – <i>summer-offset</i> in daylight saving time range: <i>date-time</i>	clock timezone zone-time add 1 clock summer-time ss one-off 1:00 2008/1/1 1:00 2008/8/8 2 clock datetime 3:00 2008/1/1	03:00:00 ss Tue 01/01/2008

## Configuration steps

Step	Command	Remarks
1. Set the system time and date.	<b>clock datetime</b> <i>time date</i>	Optional. Available in user view.
2. Enter system view.	<b>system-view</b>	—
3. Set the time zone.	<b>clock timezone</b> <i>zone-name</i> { <b>add</b>   <b>minus</b> } <i>zone-offset</i>	Optional. UTC time zone by default.
4. Set a daylight saving time scheme.	Set a nonrecurring scheme: <b>clock summer-time</b> <i>zone-name</i> <b>one-off</b> <i>start-time start-date end-time end-date add-time</i>	Optional. Use either command.
	Set a recurring scheme: <b>clock summer-time</b> <i>zone-name</i> <b>repeating</b> <i>start-time start-date end-time end-date add-time</i>	By default, daylight saving time is disabled, and the UTC time zone applies.

## Enabling displaying the copyright statement

The router by default displays the copyright statement when a Telnet or SSH user logs in, or when a console user quits user view. You can disable or enable the function as needed. The following is a sample copyright statement:

```
*****
```

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

Step...	Command...	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable displaying the copyright statement.	<b>copyright-info enable</b>	Optional. Enabled by default.

## Configuring banners

Banners are messages the system displays when a user connects to the router to perform login authentication, and start interactive configuration.

### Banner types

You can configure the following types of banners:

- **Legal banner**—Appears after the system displays the copyright or license statement for a user attempting to log in. To continue authentication or login, the user must enter **Y** or press **Enter**. To quit the process, the user must enter **N**. **Y** and **N** are case insensitive.
- **MOTD banner**—Displays the greeting message, and appears after the legal banner and before the login banner.
- **Login banner**—Appears only when password or scheme login authentication has been configured.
- **Incoming banner**—Appears for modem dial-in users and the shell banner appears for users that use any other access method to access the CLI.

### Message input modes

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

#### 1. Single-line input

In single-line input mode, all banner information is input in the same line. The start and end characters of the input text must be the same and are not part of the banner information. The input text, together with the command keywords, cannot exceed 510 characters. In this mode, do not press **Enter** after typing the banner information. For example, to configure a banner like "Have a nice day." use the following command:

```
<System> system-view
[System] header shell %Have a nice day.%
```

#### 2. Multiple-line input

In multiple-line input mode, you can press **Enter** to separate the banner information in multiple lines. In this case, up to 2000 characters can be typed.

Multi-line input can be performed with the following methods:

- **Method 1**—Press the **Enter** key directly after the command keywords, type the banner information, and end with the % character. The % character is not part of the banner information. For example, to configure a banner like "Have a nice day. Please input the Password!", use the following commands:

```
<System> system-view
[System] header shell
Please input banner content, and quit with the character '%'.--System prompt
```

Have a nice day.  
Please input the Password!%

- **Method II**—Type a character after the command keywords at the first line, and then press **Enter**. Type the banner information, and end with the character you typed at the first line. The start character and the end character are not part of the banner information. For example, to configure a banner like "Have a nice day. Please input the Password!", use the following commands:

```
<System> system-view
[System] header shell A
Please input banner content, and quit with the character 'A'.--System prompt
Have a nice day.
Please input the Password!A
```

- **Method III**—Type multiple characters after the command keywords at the first line (with the first and last characters being different), and then press **Enter**. Type the rest banner information, and end with the first character you typed at the first line. The first input character at the first line and the end character are not part of the banner information. For example, to configure a banner like "Have a nice day. Please input the Password!", use the following commands:

```
<System> system-view
[System] header shell AHave a nice day.
Please input banner content, and quit with the character 'A'.--System prompt
Please input the Password!A
```

## Configuration steps

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure the incoming banner.	<b>header incoming</b> <i>text</i>	Optional
3. Configure the login banner.	<b>header login</b> <i>text</i>	Optional
4. Configure the legal banner.	<b>header legal</b> <i>text</i>	Optional
5. Configure the shell banner.	<b>header shell</b> <i>text</i>	Optional
6. Configure the MOTD banner.	<b>header motd</b> <i>text</i>	Optional

## Configuring the maximum number of concurrent users

When multiple users configure a setting in system view, only the last configuration applies. When the maximum number of concurrent users is reached, other users cannot enter system view.

To configure the maximum number of users that can enter the system view simultaneously:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure the maximum number of concurrent users.	<b>configure-user count</b> <i>number</i>	Optional. By default, up to two users are allowed to perform operations in system view at the same time.



# Configuring the exception handling method

You can configure the router to handle system exceptions by one of the following methods:

- **reboot**—The router automatically reboots to recover from the error condition.
- **maintain**—The router stays in the error condition so you can collect complete data, including error messages, for diagnosis. In this approach, you must manually reboot the router.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure the exception handling method.	<b>system-failure { maintain   reboot }</b>	Optional. By default, the system reboots when an exception occurs.

## Rebooting the router

### CAUTION:

- A reboot can interrupt network services.
- To avoid data loss, use **save** to save the current configuration before a reboot.
- Use **display startup** and **display boot-loader** to check that you have correctly set the startup configuration file and the main system software image file. If the main system software image file has been corrupted or does not exist, the router cannot reboot. You must respecify a main system software image file, or power off the router and then power it on so the system can reboot with the backup system software image file.

You can reboot the router in one of the following ways to recover from an error condition:

- Reboot the router immediately at the CLI.
- At the CLI, schedule a reboot to occur at a specific time and date or after a delay.
- Power off and then power on the router. This method might cause data loss and hardware damage, and is the least preferred method.

Reboot at the CLI enables easy remote device maintenance.

## Rebooting the router immediately at the CLI

Task	Command	Remarks
Reboot a subcard or the router immediately	<b>reboot [ slot slot-number ]</b>	Required

## Scheduling a device reboot

The system displays the alert "REBOOT IN ONE MINUTE" one minute before the reboot.

For data security, if you are performing file operations at the reboot time, the system does not reboot. Perform one of the following commands in user view to schedule a device reboot:

Task	Command	Remarks
Schedule a reboot to occur at a specific time and date.	<b>schedule reboot at</b> <i>hh:mm [ date ]</i>	Required.
Schedule a reboot to occur after a delay.	<b>schedule reboot delay</b> { <i>hh:mm   mm</i> }	Use either command. The scheduled reboot function is disabled by default.

## Scheduling jobs

You can schedule a job to automatically run a command or a set of commands without administrative interference. The commands in a job are polled every minute. When the scheduled time for a command is reached, the job automatically executes the command. If a confirmation is required while the command is running, the system automatically enters **Y**. If characters are required, the system automatically enters a default character string, or enter an empty character string when there is no default character string.

You can configure jobs in a nonmodular or modular approach. Use the nonmodular approach for a one-time command execution and use the modular approach for complex maintenance work.

**Table 17 A comparison of nonmodular and modular approaches**

Comparison item	Scheduling a job in the nonmodular approach	Scheduling a job in the modular approach
Configuration method	Configure all elements in one command.	Separate job, view, and time settings.
Can multiple jobs be configured	No.	Yes.
Can a job have multiple commands	No. If you use <b>schedule job</b> repeatedly, only the last configuration takes effect.	Yes. You can use <b>time</b> in job view to configure commands to be executed at different time points.
Supported views	User view and system view. In <b>schedule job</b> , <i>shell</i> represents user view, and <i>system</i> represents system view.	All views. In <b>time</b> , <i>monitor</i> represents user view.
Supported commands	Commands in user view and system view.	Commands in all views.
Can a job be repeatedly executed	No.	Yes.
Can a job be saved	No.	Yes.

## Configuration guidelines

- To have a job successfully run a command, ensure the specified view and command are valid. The system does not verify their validity.
- The configuration interface, view, and user status that you have before job execution restores even if the job has run a command that changes the user interface (for example, **telnet**, **ftp**, and **ssh2**), the view (for example, **system-view** and **quit**), or the user status (for example, **super**).

- The jobs run in the background without displaying any messages except log, trap and debugging messages.
- In the modular approach:
  - Every job can have only one view and up to 10 commands. If you specify multiple views, the one specified last takes effect.
  - Enter a view name in its complete form. Most commonly used view names include **monitor** for user view, **system** for system view, **Ethernetx/x** for Ethernet interface view, and **Vlan-interfacex** for VLAN interface view.
  - The time ID (*time-id*) must be unique in a job. If two times and command bindings have the same time ID, the one configured last takes effect.

## Scheduling a job in the nonmodular approach

Task	Command	Remarks
Schedule a job to run a command at a specific time.	<b>schedule job at</b> <i>time</i> [ <i>date</i> ] <b>view</b> <i>view command</i>	Required. Use either command.
Schedule a job to run a command after a delay.	<b>schedule job delay</b> <i>time</i> <b>view</b> <i>view command</i>	Changing the system time can affect the execution time of the job set by <b>schedule job at</b> but not <b>schedule job delay</b> .

## Scheduling a job in the modular approach

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Create a job and enter job view.	<b>job</b> <i>job-name</i>	Required.
3. Specify the view in which the commands in the job run.	<b>view</b> <i>view-name</i>	Required. You can specify only one view for a job. The job executes all commands in the specified view.
4. Add commands to the job.	a. Configure a command to run at a specific time and date: <b>time</b> <i>time-id</i> <b>at</b> <i>time date</i> <b>command</b> <i>command</i>	Required. Use any of the commands.
	b. Configure a command to run at a specific time: <b>time</b> <i>time-id</i> { <b>one-off</b>   <b>repeating</b> } <b>at</b> <i>time</i> [ <b>month-date</b> <i>month-day</i>   <b>week-day</b> <i>week-daylist</i> ] <b>command</b> <i>command</i>	Changing the system time can affect the execution time of the job set by <b>time at</b> but not <b>time delay</b> .

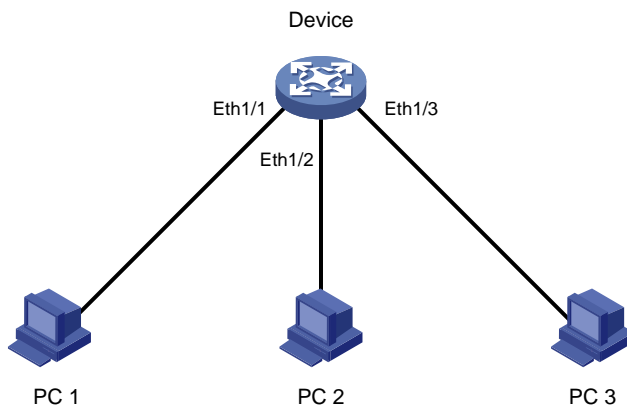
Step	Command	Remarks
c.	Configure a command to run after a delay:	<code>time time-id { one-off   repeating } delay time command command</code>

## Scheduled job configuration example

### Network requirements

Configure scheduled tasks on the router to enable interfaces Ethernet 1/1, Ethernet 1/2, and Ethernet 1/3 at 8:00 and disabled them at 18:00 on working days every week, to control the access of the PCs connected to these interfaces.

Figure 45 Network diagram



### Configuration procedure

# Enter system view.

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

# Create a job **pc1**, and enter its view.

```
[Sysname] job pc1
```

# Configure the job to be executed in the view of Ethernet 1/1.

```
[Sysname-job-pc1] view ethernet 1/1
```

# Configure the router to start Ethernet 1/1 at 8:00 on working days every week.

```
[Sysname-job-pc1] time 1 repeating at 8:00 week-day mon tue wed thu fri command undo shutdown
```

# Configure the router to shut down Ethernet 1/1 at 18:00 on working days every week.

```
[Sysname-job-pc1] time 2 repeating at 18:00 week-day mon tue wed thu fri command shutdown
```

```
[Sysname-job-pc1] quit
```

# Create a job **pc2**, and enter its view.

```
[Sysname] job pc2
```

# Configure the job to be executed in the view of Ethernet 1/2.

```
[Sysname-job-pc2] view ethernet 1/2
```

# Configure the router to start Ethernet 1/2 at 8:00 on working days every week.

```

[Sysname-job-pc2] time 1 repeating at 8:00 week-day mon tue wed thu fri command undo shutdown
# Configure the router to shut down Ethernet 1/2 at 18:00 on working days every week.
[Sysname-job-pc2] time 2 repeating at 18:00 week-day mon tue wed thu fri command shutdown
[Sysname-job-pc2] quit

# Create a job pc3, and enter its view.
[Sysname] job pc3

# Configure the job to be executed in the view of Ethernet 1/3.
[Sysname-job-pc3] view ethernet 1/3

# Configure the router to start Ethernet 1/3 at 8:00 on working days every week.
[Sysname-job-pc3] time 1 repeating at 8:00 week-day mon tue wed thu fri command undo shutdown

# Configure the router to shut down Ethernet 1/3 at 18:00 on working days every week.
[Sysname-job-pc3] time 2 repeating at 18:00 week-day mon tue wed thu fri command shutdown
[Sysname-job-pc3] quit

# Display information about scheduled jobs.
[Sysname] display job
Job name: pc1
    Specified view: Ethernet1/1
    Time 1: Execute command undo shutdown at 08:00 Mondays Tuesdays Wednesdays Thursdays Fridays
    Time 2: Execute command shutdown at 18:00 Mondays Tuesdays Wednesdays Thursdays Fridays
Job name: pc2
    Specified view: Ethernet1/2
    Time 1: Execute command undo shutdown at 08:00 Mondays Tuesdays Wednesdays Thursdays Fridays
    Time 2: Execute command shutdown at 18:00 Mondays Tuesdays Wednesdays Thursdays Fridays
Job name: pc3
    Specified view: Ethernet1/3
    Time 1: Execute command undo shutdown at 08:00 Mondays Tuesdays Wednesdays Thursdays Fridays
    Time 2: Execute command shutdown at 18:00 Mondays Tuesdays Wednesdays Thursdays Fridays

```

## Configuring a detection interval

Some protocol modules might shut down ports under specific circumstances. For example, an MSTP module will automatically shut down a port receiving configuration messages after the BPDU guard function is enabled on the port. Then, the router enables a detection timer and detects the status of the port. If the port is still down when the detection timer expires, the router automatically brings up the port.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure a detection interval.	<b>shutdown-interval</b> <i>time</i>	Optional. The detection interval is 30 seconds by default.

# Configuring card temperature thresholds

You can set the temperature alarm thresholds to monitor the temperature of a card. When the temperature of a card reaches the threshold, the router generates alarms.

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Configure temperature thresholds for a card	No	No	Yes	Yes	Yes

To configure a card temperature threshold:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure temperature thresholds for a card.	<b>temperature-limit</b> <i>slot-number</i> <i>lower-value upper-value</i>	Optional

# Configuring NMS monitored interfaces

Typically, when managing a device using an NMS, you must configure an IP address on the NMS for the managed device, and the NMS uses this address to monitor and manage the device. If the IP address of the interface connecting the device and the NMS changes or the interface fails (interface status becomes down), the NMS cannot use the previously configured IP address to establish a connection with the managed device.

If you configure a monitored interface for the NMS, the managed device monitors the IP address of the interface in real time. When the interface gets or changes its IP address, the device sends traps to the NMS to inform it of the new IP address, and thus the NMS can keep managing the device by using the new IP address.

In your networking, you can connect two interfaces on the device to the NMS to realize link backup and increase reliability. You can configure the device to monitor the two interfaces: one as the primary monitored interface and the other as the secondary monitored interface. However, the device can monitor the IP address of only one interface at one time.

- If you configure only the primary interface or the secondary interface, the device monitors the IP address of the configured interface. If the interface gets or changes its IP address when the interface status is up, the device sends traps to the NMS to inform it of the available IP address.
- If you configure both the primary and secondary interfaces, the device monitors the primary interface first. When the primary interface gets an IP address, the device sends traps to the NMS to inform it of the available IP address. When the primary interface is up and has a valid IP address, the device does not care about the IP address changes of the secondary interface. If the configuration of the primary interface is removed, the interface is down, or its IP address is deleted or modified, the device begins to monitor the secondary interface, and when the secondary interface gets an IP address, the device sends traps to the NMS to inform it of the available IP address. After that, during the time the secondary interface is up and has a valid IP address, the device does not care about the IP address changes of the primary interface, until the secondary interface is down or its IP address is deleted or modified.

You can define the role of the monitored interface (primary or secondary), and HP recommends specifying the interface with a better route to the NMS or stable link state as the primary.

To ensure the router can send the traps to the NMS, you must configure the NMS as the trap destination host on the router. For more information, see *Network Management and Monitoring Configuration Guide*.

The previously mentioned IP address change of an interface indicates that the interface gets a new IP address after its original IP address is deleted.

The execution of **shutdown** and **undo shutdown**, as well as plugging in and plugging out network cables result in the status change (from up to down, or the opposite) of an interface.

Configuring the IP address manually or allocating IP address dynamically by using DHCP in interface view triggers the sending of traps from the router to the NMS.

The router monitors only the change of an IPv4 address, not the change of an IPv6 address.

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Configure the monitored interfaces for the NMS.	Yes	Yes	No	No	No

To configure the monitored interface for the NMS:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure the primary monitored interface for the NMS.	<b>nms primary monitor-interface</b> <i>interface-type interface-number</i>	Required. Use either command.
3. Configure the secondary monitored interface for the NMS.	<b>nms secondary monitor-interface</b> <i>interface-type interface-number</i>	By default, the NMS does not monitor any interface on the router.

## Configuring an interface card working mode

The router supports multiple interface card types. Some cards have only one function, for example, SIC-1FEA (1-port 10/100 Mbps Ethernet interface card, mainly used to implement communication between a router and a LAN); some interface cards have multifunctional modules, for example, FIC-2E1 (2-port channelized E1/PRI interface card, the specified interfaces on which can be configured to implement E1, CE1, or ISDN PRI access); some cards can be configured with different working modes. At present, the router supports the following switching modes:

- **CPOS 155 Mbps (E1/T1)**—Supports switching between E1 and T1 of the entire interface card. When the interface card works in E1 mode, all the interfaces on the interface card can receive, send and process E1 data flows, and provide CE1 access. When the interface card works in T1 mode, all the interfaces on the interface card can receive, send, and process T1 data flows, and provide CT1 access.
- **ESM (IPsec/SSL)**—Supports switching between IPsec and SSL encryption modes of the ESM interface card. When the ESM interface card works in IPsec mode, it supports the IPsec protocol. When the ESM interface card works in SSL mode, it supports the SSL protocol.
- **G.SHDSL.BIS (atm/auto/efm)**—Supports switching between ATM and EFM of the entire interface card. When the interface card works in ATM mode, all its interfaces receive and transmit only ATM packets. When the interface card works in EFM mode, all its interfaces receive and transmit only Layer 3 Ethernet packets. When the interface card works in auto mode, all its interfaces operate in the auto-negotiation mode. As a result, you can use the ATM network for Ethernet packet transmission by

switching the interface card to operate in EFM mode, thus protecting user investment and improving packet transmission speed by avoiding ATM devices from converting packets between Ethernet packets and ATM cells.

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Set the working mode of an interface card.	No	No	Yes	Yes	Yes

To configure the working mode of an interface card:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Set the working mode of an interface card.	<b>card-mode slot slot-number mode-name</b>	Optional. The <i>mode-name</i> argument might take the value of <b>e1</b> or <b>t1</b> for CPOS interface cards, <b>ipsec</b> or <b>ssl</b> for ESM interface cards, and <b>atm</b> , <b>auto</b> , or <b>efm</b> for G.SHDSL.BIS interface cards.

To make the configured working mode take effect, restart the router or hot swap the interface card (if the interface card supports hot swapping) after you change the working mode.

## Clearing unused 16-bit interface indexes

The router must maintain persistent 16-bit interface indexes and keep one interface index match one interface name for network management. After deleting a logical interface, the router retains its 16-bit interface index so the same index can be assigned to the interface at interface recreation.

To avoid index depletion causing interface creation failures, you can clear all 16-bit indexes that have been assigned but not in use. The operation does not affect the interface indexes of the interfaces that have been created, but the indexes assigned to re-created interfaces might change.

### CAUTION:

A confirmation is required when you execute this command. The command will not run if you fail to make a confirmation within 30 seconds or enter **N** to cancel the operation.

Task	Command	Remarks
Clear the 16-bit interface indexes saved but not used in the current system.	<b>reset unused porttag</b>	Required. Available in user view.

## Verifying and diagnosing transceiver modules

The commonly used transceiver modules are SFP transceivers.



**Table 18 Commonly used transceiver modules**

Transceiver type	Application environment	Whether can be an optical transceiver	Whether can be an electrical transceiver
SFP	Generally used for 100M/1000M Ethernet interfaces or POS 155M/622M/2.5G interfaces	Yes	Yes

## Verifying transceiver modules

You can verify the genuineness of a transceiver module in the following ways:

- Display the key parameters of a transceiver module, including its transceiver type, connector type, central wavelength of the transmit laser, transfer distance, and vendor name.
- Display its electronic label. The electronic label is a profile of the transceiver module and contains the permanent configuration, including the card name, serial number, and vendor name.

To identify an antispoofing transceiver module customized by HP, use the **Vendor Name** field in the prompt information of **display transceiver**. If the field is **HP**, it is considered an HP-customized transceiver module.

Step	Command	Remarks
1. Display key parameters of transceiver modules.	<b>display transceiver</b> { <b>controller</b> [ <i>controller-type controller-number</i> ]   <b>interface</b> [ <i>interface-type interface-number</i> ] } [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available for all transceiver modules
2. Display transceiver modules' electronic label information.	<b>display transceiver manuinfo</b> { <b>controller</b> [ <i>controller-type controller-number</i> ]   <b>interface</b> [ <i>interface-type interface-number</i> ] } [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available for antispoofing transceiver modules customized by HP only

## Diagnosing transceiver modules

The device provides the alarm function and digital diagnosis function for transceiver modules. When a transceiver module fails or works inappropriately, you can check for alarms present on the transceiver module to identify the fault source or examine the key parameters monitored by the digital diagnosis function, including the temperature, voltage, laser bias current, TX power, and RX power.

Perform the following commands in any view to diagnose transceiver modules:

Task	Command	Remarks
Display alarms present on transceiver modules.	<b>display transceiver alarm</b> { <b>controller</b> [ <i>controller-type controller-number</i> ]   <b>interface</b> [ <i>interface-type interface-number</i> ] } [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available for all transceiver modules.
Display the present measured values of the digital diagnosis parameters for pluggable transceivers.	<b>display transceiver diagnosis</b> { <b>controller</b> [ <i>controller-type controller-number</i> ]   <b>interface</b> [ <i>interface-type interface-number</i> ] } [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available for anti-spoofing pluggable optical transceivers customized by HP only.

## Displaying and maintaining device management

For diagnosis or troubleshooting, you can use separate **display** commands to collect running status data module by module, or use **display diagnostic-information** to bulk collect running data for multiple modules. The **display diagnostic-information** command equals: **display clock**, **display version**, **display device**, and **display current-configuration**.

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Display the temperature information of the router.	No	No	Yes	Yes	Yes
Display the operating state of fans.	No	No	Yes	Yes	Yes
Display state of the RPS.	No	No	No	Yes (except the MSR30-1X routers)	Yes

To display device management:

Task	Command	Remarks
Display system version information.	<b>display version</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the system time and date.	<b>display clock</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the terminal user information.	<b>display users</b> [ <b>all</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display information about the users logged in to the device but are not under user view.	<b>display configure-user</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display or save operating statistics for multiple feature modules.	<b>display diagnostic-information</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display CPU usage statistics.	<b>display cpu-usage</b> [ <i>entry-number</i> [ <i>offset</i> ] [ <b>verbose</b> ] [ <b>from-device</b> ] ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	

Task	Command	Remarks
Display historical CPU usage statistics in a chart.	<b>display cpu-usage history</b> [ task <i>task-id</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display hardware information.	<b>display device</b> [ <i>cf-card</i>   <i>usb</i> ] [ slot <i>slot-number</i>   <b>verbose</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the electrical label data for the device.	<b>display device manuinfo</b> [ slot <i>slot-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display device temperature statistics.	<b>display environment</b> [ <i>cpu</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the operating state of fans.	<b>display fan</b> [ <i>fan-id</i>   <b>verbose</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display memory usage statistics.	<b>display memory</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the power state.	<b>display power</b> [ <i>power-id</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display RPS state information.	<b>display rps</b> [ <i>rps-id</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the mode of the last reboot.	<b>display reboot-type</b> [ slot <i>slot-number</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the configuration of the job configured by using <b>schedule job</b> .	<b>display schedule job</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the device reboot setting.	<b>display schedule reboot</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the configuration of jobs configured by using <b>job</b> .	<b>display job</b> [ <i>job-name</i> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	
Display the exception handling method.	<b>display system-failure</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	

For more information about the **display users** command, see *Fundamentals Command Reference*.

---

# Configuration file management

The device provides the configuration file management function. You can manage configuration files on the user-friendly CLI.

## Overview

A configuration file contains a set of commands. You can save the current configuration to a configuration file so that the configuration can take effect after a device reboot. In addition, you can view the configuration information, or upload or download the configuration file to or from another device.

## Types of configuration

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

### Factory defaults

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

Factory defaults may differ from the default settings of commands and vary with device models.

### Startup configuration

Use startup configuration for initialization when the device boots. If this file does not exist, the system boots using the factory defaults.

You can view the startup configuration in either of the following ways:

- Use **display startup** to view the current 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 current 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 the system operation. The running configuration is stored in a temporary storage medium. You must save a setting you have made so it can survive a reboot.

Use **display current-configuration** to view the current configuration.

## Configuration file format and content

A configuration file is saved as a text file, following these rules:

- A configuration file contains commands, and only nondefault 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 medium. You can 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 the network rapidly, saving the configuration workload.

A device starts up using only one configuration file. However, you can specify two startup configuration files: one main startup configuration file and one 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, there are at most one main startup configuration file and one backup startup configuration file. You can specify neither of the two files (displayed as NULL).

You can specify main and backup startup configuration files to be used at the next startup of the device by two 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 for the next 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 factory defaults.

## Saving the running configuration

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

Complete these tasks to save the current configuration:

Task	Remarks
Encrypting a configuration file	Optional
Configuration save modes	Required

## Encrypting a configuration file

Configuration file encryption enables you to encrypt a configuration file before saving it by using **save**. To read the encrypted configuration file, you must decrypt it with a legal key, thus protecting the configuration file. Two kinds of keys are supported to encrypt a configuration file. You can select either of them according to your application environment:

- **Private key**—A configuration file encrypted with this kind of key can be decrypted and recognized only by the local device.
- **Public key**—A configuration file encrypted with this kind of key can be decrypted and recognized by all devices supporting this feature.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable configuration file encryption.	<b>configuration encrypt</b> { <b>private-key</b>   <b>public-key</b> }	Optional.  Disabled by default, that is, the current valid configurations are directly saved to the configuration file.  Use <b>display saved-configuration</b> to view the encrypted configuration file.  The <b>more</b> command cannot decrypt the file. If you use <b>more</b> , an error message or garbled characters are displayed.

## Configuration save modes

- **Fast saving mode**—Using **save** without the **safely** keyword. This mode saves the file more quickly, but is likely to lose the existing configuration file 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.
- **Safe mode**—Using **save** with the **safely** keyword. This mode saves the file more slowly, but can retain the configuration file in the device even if the device reboots or the power fails during the process. The safe mode is preferred in environments where a stable power supply is unavailable or remote maintenance is involved.

Task	Command	Remarks
Save the current configuration to the specified file, but the configuration file will not be set as the file for the next startup.	<b>save file-url</b>	Required.
Save the current configuration to the root directory of the storage medium and specify the file as the startup configuration file that is used at the next system startup.	<b>save [ safely ] [ backup   main ] [ force ]</b>	Use either command. Available in any view.

The configuration file must have the extension **.cfg**.

The **save [ safely ]** and **save [ safely ] main** commands have 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 factory defaults, and after the device reboots, you will need to respecify a startup configuration file for the next system startup (see "[Specifying a startup configuration file for the next 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**, or, 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. It is a good practice to use the configuration file that is generated by using the backup function (manually or automatically). Configuration rollback can be applied in these 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:

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 command:

- 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 with different configurations in the running configuration.

## Configuration task list

Task	Remarks
Configuring parameters for saving the current running configuration	Required
Enabling running configuration automatic sav	Required
Manually saving the running configuration	Use either approach
Setting a configuration rollback	Required

## Configuring parameters for saving the current 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.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Configure the path and filename prefix for saving configuration files.	<b>archive configuration</b> <b>location</b> <i>directory</i> <b>filename-prefix</b> <i>filename-prefix</i>	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.
3. Set the maximum number of configuration files that can be saved.	<b>archive configuration</b> <b>max</b> <i>file-number</i>	Optional. The default number is 5. If <b>undo archive configuration location</b> is executed, the running configuration cannot be saved either manually or automatically. The configuration is restored to the default by executing <b>archive configuration interval</b> and <b>archive configuration max</b> , meanwhile, the saved configuration files are cleared. The value of the <i>file-number</i> argument is determined by memory space. HP recommends setting a comparatively small value for the <i>file-number</i> argument if the available memory space is small.



## Enabling running configuration automatic save

You can 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:

- If the configuration of the device does not change frequently, manually save the running configuration as needed.
- If a low-speed storage medium (such as a flash) is used, save the running configuration manually, or configure automatic saving with an interval longer than 1,440 minutes (24 hours).
- If a high-speed storage medium (such as a CF card) is used and the configuration of the device changes frequently, set a shorter saving interval.

To enable automatic saving of the running configuration:

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

## Manually saving the running configuration

Automatic saving of the running configuration occupies system resources, and frequent saving can greatly affect system performance. If the system configuration does not change frequently, it is a good practice to 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, you can manually save the running configuration so the device can revert to the previous state if and when the configuration fails.

Task	Command	Remarks
Manually save the running configuration.	<b>archive configuration</b>	Required. Available in user view. Specify the path and filename prefix for saving configuration files before you manually save the running configuration; otherwise, the operation fails.

## Setting configuration rollback

### ⚠ CAUTION:

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, namely, you cannot get the actual undo form of the command by 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 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.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Roll back the configuration.	<b>configuration replace file filename</b>	Required.

## Specifying a startup configuration file for the next startup

### ⚠ CAUTION:

A configuration file must use **.cfg** as its extension name. The startup configuration file must be saved in the storage media's root directory.

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

- Use **save**. If you save the running configuration to the specified configuration file in the interactive mode, the system 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:

Task	Command	Remarks
Specify a startup configuration file for the next startup.	<b>startup saved-configuration</b> <i>cfgfile</i> [ <b>backup</b>   <b>main</b> ]	Required. Available in user view.

## 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 a TFTP server. The backup operation backs up the main startup configuration file to the TFTP server.

## Backup prerequisites

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

## Backup procedure

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

Task	Command	Remarks
Back up the startup configuration file to be used at the next startup to a TFTP server.	<b>backup startup-configuration to</b> <i>dest-addr [dest- filename ]</i>	Required. Available in user view.

# Deleting a startup configuration file for the next startup

You can delete a startup configuration file to be used at the next startup. You can choose to delete either 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 upgrading 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 use factory defaults at the next startup.

To delete 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 the device. Use it with caution.

Task	Command	Remarks
Delete a startup configuration file to be used at the next startup from the storage medium.	<b>reset saved-configuration</b> [ <b>backup</b>   <b>main</b> ]	Required. Available in user view.

# Restoring a startup configuration file

The restore function allows you to copy a configuration file from a TFTP server to the device and specify the file as the startup configuration file to be used at the next startup. The restore operation restores the main startup configuration file.

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

Task	Command	Remarks
Restore a startup configuration file to be used at the next startup.	<b>restore startup-configuration from</b> <i>src-addr src-filename</i>	Required. Available in user view. After executing the command, use <b>display startup</b> (in user view) to verify that the filename of the configuration file to be used at the next system startup is the same as that specified by the <i>filename</i> argument.

## Displaying and maintaining a configuration file

Task	Command	Remarks
Display the information about configuration rollback.	<b>display archive configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the current configuration of the device.	<b>display current-configuration</b> [ [ <b>configuration</b> [ <i>configuration</i> ]   <b>controller</b>   <b>interface</b> [ <i>interface-type</i> ] [ <i>interface-number</i> ]   <b>exclude modules</b> ] [ <b>by-linenum</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ] ]	Available in any view
Display the running configuration file saved on the storage medium of the device.	<b>display saved-configuration</b> [ <b>by-linenum</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the configuration files used at this and the next system startup.	<b>display startup</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display the valid configuration under the current view.	<b>display this</b> [ <b>by-linenum</b> ] [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view

# Managing files

## Overview

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 saved on your device and organize them under different directories for easy management.

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Storage media	Flash	Flash	CF card	Flash (supported on MSR30-10, MSR30-11E, and MSR30-11F)	Flash (not supported on MPUF)
	USB disk	USB disk	USB disk	CF card (supported on MSR30-16, MSR30-20, MSR30-40, and MSR30-60) USB disk	CF card USB disk

## Storage media naming rules

The names of storage media are the names of the storage media type, for example, flash or cfa0.

## Filename formats

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

Format	Description	Length	Example
<i>file-name</i>	Specifies a file in the current working directory.	1 to 91 characters	a.cfg indicates a file named <b>a.cfg</b> in the current working directory
<i>path/ file-name</i>	Specifies a file in the specified folder in the current working directory. <i>path</i> indicates the name of the folder. You can specify multiple folders, indicating a file under a multi-level folder.	1 to 135 characters	test/a.cfg indicates a file named <b>a.cfg</b> in the <b>test</b> folder in the current working directory
<i>drive:/ [path]/ file-name</i>	Specifies a file in the specified storage medium on the device. <i>drive</i> represents the storage medium name, which is usually <b>flash</b> or <b>cf</b> . If there is only one storage medium on the device, you do not need to provide information about the storage medium. If multiple storage media exist on the device, you must provide the related information to identify the storage medium.	1 to 135 characters	flash:/test/a.cfg indicates a file named <b>a.cfg</b> in the <b>test</b> folder in the root directory of Flash

# Managing directories

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

## Displaying directory information

Task	Command	Remarks
Display directory or file information.	<b>dir</b> [ /all ] [ <i>file-url</i>   /all-file systems ]	Required. Available in user view.

## Displaying the current working directory

Task	Command	Remarks
Display the current working directory.	<b>pwd</b>	Required. Available in user view.

## Changing the current working directory

Task	Command	Remarks
Change the current working directory.	<b>cd</b> { <i>directory</i>   ..   / }	Required. Available in user view.

## Creating a directory

Task	Command	Remarks
Create a directory.	<b>mkdir</b> <i>directory</i>	Required. Available in user view.

## Removing a directory

Task	Command	Remarks
Remove a directory.	<b>rmdir</b> <i>directory</i>	Required. Available in user view. The directory to be removed must be empty, so before you remove a directory, you must delete all the files and the subdirectory in this directory. For file deletion, see <b>delete</b> . For subdirectory deletion, see <b>rmdir</b> . Executing <b>rmdir</b> automatically deletes the files in the recycle bin in the current directory.

# Managing files

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

You can create a file by copying, downloading or using **save**.

## Displaying file information

Task	Command	Remarks
Display file or directory information.	<b>dir</b> [ /all ] [ <i>file-url</i>   /all-file systems ]	Required. Available in user view.

## Displaying file contents

Task	Command	Remarks
Display the contents of a file.	<b>more</b> <i>file-url</i>	Required. Only a .txt file can be displayed. Available in user view.

## Renaming a file

Task	Command	Remarks
Rename a file.	<b>rename</b> <i>fileurl-source fileurl-dest</i>	Required. Available in user view.

## Copying a file

Task	Command	Remarks
Copy a file.	<b>copy</b> <i>fileurl-source fileurl-dest</i>	Required. Available in user view.

## Moving a file

Task	Command	Remarks
Move a file.	<b>move</b> <i>fileurl-source fileurl-dest</i>	Required. Available in user view.

## Deleting a file

The files in the recycle bin still occupy storage space.

- To delete a file in the recycle bin, execute **reset recycle-bin** in the directory where the file originally belongs.
- To save storage space, empty the recycle bin periodically with **reset recycle-bin**.



### CAUTION:

The **delete /unreserved file-url** command deletes a file permanently and the action cannot be undone. Executing this command equals executing **delete file-url** and then **reset recycle-bin** in the same directory.

Task	Command	Remarks
Move a file to the recycle bin or delete it permanently.	<b>delete</b> [ <b>/unreserved</b> ] <i>file-url</i>	Required. Available in user view.

## Restoring a file from the recycle bin

Task	Command	Remarks
Restore a file from the recycle bin.	<b>undelete</b> <i>file-url</i>	Required. Available in user view.

## Emptying the recycle bin

Step	Command	Remarks
1. Enter the original working directory of the file to be deleted.	<b>cd</b> { <i>directory</i>   <b>..</b>   <b>/</b> }	Optional. If the original directory of the file to be deleted is not the current working directory, this command is required. Available in user view.
2. Delete the file in the current directory and in the recycle bin.	<b>reset recycle-bin</b> [ <b>/force</b> ]	Required. Available in user view.

## Performing batch operations

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 it to the device. If the suffix of the file is not **.bat**, use **rename** to change the suffix to **.bat**.

Executing a batch file does not guarantee successful execution of every command in the batch file. If a command has error settings or the conditions for executing the command are not satisfied, this command fails to be executed, and the system skips the command to the next one.



Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Execute a batch file.	<b>execute</b> <i>filename</i>	Required.

## Performing storage media operations

Efficient file management is facilitated by the operations that can be performed on the storage media.

### Managing storage media space

When the space of a storage medium becomes inaccessible due to abnormal operations, you can use **fixdisk** to restore the space of the storage medium. Executing **format** formats the storage medium, and all the data on the storage medium is deleted.

#### CAUTION:

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

Step	Command	Remarks
1. Restore storage media space.	<b>fixdisk</b> <i>device</i>	Optional. Available in user view.
2. Format storage media.	<b>format</b> <i>device</i> [ <b>FAT16</b>   <b>FAT32</b> ]	Optional. <b>FAT16</b> and <b>FAT32</b> are not applicable to a flash card. Available in user view.

### Mounting/unmounting storage media

For a hot swappable storage medium (excluding flash), such as a CF card, use **mount** and **umount** to mount or unmount it.

- By default, a storage medium is automatically mounted when connected to the device. However, when a storage medium is connected to a lower version system, the system cannot recognize the storage medium. To perform read and write operations to the storage medium, you must mount it.
- An unmounted device is in disconnected state, and can be removed safely. If you unplug a storage medium without unmounting it, files on the storage medium or even the storage medium itself may be damaged.
- An unmounted storage medium can be used only when it is mounted again.

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Mount/unmount a storage medium.	Yes	Yes	Yes	Yes	Yes



#### CAUTION:

- When mounting or unmounting a storage medium, or performing file operations on it, do not unplug or switchover the storage medium or the card where the storage medium resides. The file system could be damaged.
- Before removing a mounted storage medium from the system, unmount it to avoid damaging the storage medium.

To mount or unmount a storage medium:

Step	Command	Remarks
Mount a storage medium.	<b>mount</b> <i>device</i>	Optional. By default, a storage medium is automatically mounted and in mounted state when connected to the system.
Unmount a storage medium.	<b>umount</b> <i>device</i>	Optional. By default, a storage medium is automatically mounted and in mounted state when connected to the system.

## Displaying and maintaining the NAND flash memory

The physical space of the NAND flash memory is divided into multiple blocks, each 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. Bad blocks cannot be used to store data, and the system must skip the bad blocks when it allocates storage spaces to files. You can get the locations of bad blocks and repair them at the CLI.

Step	Command	Remarks
1. Display the number and location of bad blocks in the NAND flash memory.	<b>display nandflash badblock-location</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Required. Available in any view.
2. Repair bad blocks.	<b>fixdisk</b> <i>device</i>	Required. Available in user view.

### Checking files

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
NAND flash	No	No	No	Yes Only supported on MSR30-10, MSR30-11E, and MSR30-11F	No

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

Step	Command	Remarks
1. Display the space distribution of the specified file in the NAND flash memory.	<b>display nandflash file-location</b> <i>filename</i> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.
2. Display data on the specified physical page.	<b>display nandflash page-data</b> <i>page-value</i> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	

## Setting prompt modes

The system provides the following prompt modes:

- **alert**—The system warns you 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 prevent system problems.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Set the operation prompt mode of the file system.	<b>file prompt { alert   quiet }</b>	Optional. The default is <b>alert</b> .

## File management examples

# 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
```

```
19540 KB total (2521 KB free)
```

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

```
<Sysname> cd test
```

```
<Sysname> mkdir mytest
```

```
%Created dir flash:/test/mytest.
```

# Display the current working directory.

```
<Sysname> pwd
```

```
flash:/test
```

# Display the files and the subdirectories in the test directory.

```
<Sysname> dir
```

```
Directory of flash:/test/
```

0 drw- - Feb 16 2006 15:28:14 mytest

2540 KB total (2519 KB free)

**# Return to the upper directory.**

<Sysname> cd ..

**# Display the current working directory.**

<Sysname> pwd

flash:

# Configuring FTP

The FTP is an application layer protocol used to share files between server and client over a TCP/IP network.

FTP uses TCP ports 20 and 21. Port 20 is used to transmit data, and port 21 is used to transmit control commands. For more information about FTP basic operations, see RFC 959.

FTP transfers files in the following modes:

- **Binary mode**—Transfers files as raw data, such as **.bin** and **.btm** files.
- **ASCII mode**—Transfers files as text, such as **.txt**, **.bat**, and **.cfg** files.

## Operation

FTP adopts the client/server model. Your device can function either as the client or the server, as shown in Figure 46.

- When the device serves as the FTP client, a user can telnet to it from a PC, and execute **ftp** to establish a connection to the remote FTP server on the PC to upload/download files to/from the PC.
- When the device serves as the FTP server, a user can FTP to the device from a PC that runs the FTP client and upload/download files to/from the device.

**Figure 46 Network diagram for FTP**



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

**Table 19 Configuration when the device serves as the FTP client**

Device	Configuration	Remarks
Device (FTP client)	Use <b>ftp</b> to establish the connection to the remote FTP server	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.
PC (FTP server)	Enable FTP server on the PC, and configure the username, password, user privilege level, and so on.	—

When the device serves as the FTP server, perform the following configuration:

**Table 20 Configuration when the device serves as the FTP server**

Device	Configuration	Remarks
Device (FTP server)	Enable the FTP server function.	Disabled by default. You can use <b>display ftp-server</b> to view the FTP server configuration on the device.
	Configure authentication and authorization.	Configure the username, password, and authorized directory for an FTP user. 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.
	Configure the FTP server operating parameters.	Parameters such as the FTP connection timeout time.
PC (FTP client)	Use the FTP client program to log in to the FTP server.	You can log in to the FTP server only after entering the correct FTP username and password.

Ensure 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.

## 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 you can access the FTP server, you must establish a connection from the FTP client to the FTP server. Use either **ftp** to establish the connection directly or use **open** in FTP client view to establish the connection.

When using **ftp** or **ftp client source**, specify the source interface (such as a loopback or dialer interface) 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 FTP client follows these rules to select the source IP address of packets sent to the FTP server:

- If no source IP address is specified, the IP address of the output interface of the route to the server is used as the source IP address.
- The source IP address specified with **ftp client source** or **ftp** is used.
- If you first use **ftp client source** to specify a source IP address and then use **ftp** to specify another source IP address, the latter is used.
- The source IP address specified with **ftp client source** applies to all FTP connections while the one specified with **ftp** applies to the current FTP connection only.

## Establishing an IPv4 FTP connection

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Specify the source IP address of sent FTP packets.	<b>ftp client source { interface interface-type interface-number   ip source-ip-address }</b>	Optional. By default, the source IP address is determined by the route from the FTP client to the FTP server. If no primary IP address is configured on the specified source interface, you cannot establish an FTP connection. If you use <b>ftp client source</b> 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.
3. Return to user view.	<b>quit</b>	—
4. Log in to the remote FTP server directly in user view.	<b>ftp [ server-address [ service-port ] [ vpn-instance vpn-instance-name ] [ source { interface interface-type interface-number   ip source-ip-address } ] ]</b>	Use either approach. <ul style="list-style-type: none"> <li>In user view: <b>ftp</b> is available.</li> <li>In FTP client view: <b>open</b> is available.</li> </ul>
5. Log in to the remote FTP server indirectly in FTP client view.	<b>ftp</b>  <b>open server-address [ service-port ]</b>	

## Establishing an IPv6 FTP connection

Task	Command	Remarks
Log in to the remote FTP server directly in user view	<b>ftp ipv6 [ server-address [ service-port ] [ vpn-instance vpn-instance-name ] [ source ipv6 source-ipv6-address ] [ -i interface-type interface-number ] ]</b>	Use either approach. <ul style="list-style-type: none"> <li>In user view: <b>ftp ipv6</b> is available.</li> <li>In FTP client view: <b>open ipv6</b> command is available.</li> </ul>
Log in to the remote FTP server indirectly in FTP client view	<b>ftp ipv6</b>  <b>open ipv6 server-address [ service-port ] [ -i interface-type interface-number ]</b>	

## Managing directories on the FTP server

After the device serving as the FTP client established a connection with an FTP server, you can 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](#)."

Step	Command	Remarks
1. Display detailed information about a directory or file on the remote FTP server.	<b>dir</b> [ <i>remotefile</i> [ <i>localfile</i> ] ]	Optional
2. Query a directory or file on the remote FTP server.	<b>ls</b> [ <i>remotefile</i> [ <i>localfile</i> ] ]	Optional
3. Change the working directory of the remote FTP server.	<b>cd</b> { <i>directory</i>   <i>..</i>   <i>/</i> }	Optional
4. Return to the upper level directory of the remote FTP server.	<b>cdup</b>	Optional
5. Display the working directory that is being accessed.	<b>pwd</b>	Optional
6. Create a directory on the remote FTP server.	<b>mkdir</b> <i>directory</i>	Optional
7. Remove the specified working directory on the remote FTP server.	<b>rmdir</b> <i>directory</i>	Optional

## Operating the files on the FTP server

After the device serving as the FTP client has established a connection with an FTP server, you can 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 more information about establishing an FTP connection, see "[Establishing an FTP connection](#)."

1. Use **dir** or **ls** to display the directory and the location of the file on the FTP server.
2. Delete useless files for effective use of the storage space.
3. Set the file transfer mode. FTP transmits files in two modes: ASCII and binary. ASCII mode transfers files as text. Binary mode transfers files as raw data.
4. Use **lcd** to display the local working directory of the FTP client. You can upload the file under this directory, or save the downloaded file under this directory.
5. Upload or download the file.



To operate the files on an FTP server:

Step	Command	Remarks
1. Display detailed information about a directory or file on the remote FTP server.	<b>dir</b> [ <i>remotefile</i> [ <i>localfile</i> ] ]	Optional. The <b>ls</b> command only displays the name of a directory or file. The <b>dir</b> command displays detailed information such as the file size and creation time.
2. Query a directory or file on the remote FTP server.	<b>ls</b> [ <i>remotefile</i> [ <i>localfile</i> ] ]	Optional. The <b>ls</b> command only displays the name of a directory or file. The <b>dir</b> command displays detailed information such as the file size and creation time.
3. Delete the specified file on the remote FTP server permanently.	<b>delete</b> <i>remotefile</i>	Optional.
4. Set the file transfer mode to ASCII.	<b>ascii</b>	Optional. ASCII by default.
5. Set the file transfer mode to binary.	<b>binary</b>	Optional. ASCII by default.
6. Set the data transmission mode to passive.	<b>passive</b>	Optional. Passive by default.
7. Display the local working directory of the FTP client.	<b>lcd</b>	Optional.
8. Upload a file to the FTP server.	<b>put</b> <i>localfile</i> [ <i>remotefile</i> ]	Optional.
9. Download a file from the FTP server.	<b>get</b> <i>remotefile</i> [ <i>localfile</i> ]	Optional.

## Using another username to log in to the FTP server

After the device serving as the FTP client has established a connection with the FTP server, you can 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.

Task	Command	Remarks
Use another username to relog in after successfully logging in to the FTP server.	<b>user</b> <i>username</i> [ <i>password</i> ]	Optional

## Maintaining and debugging the FTP connection

After a device serving as the FTP client has established a connection with the FTP server, you can perform the following operations to locate and diagnose FTP connection problems. For more information about establishing an FTP connection, see "[Establishing an FTP connection](#)."

Step	Command	Remarks
1. Display the help information of FTP-related commands supported by the remote FTP server.	<b>remotehelp</b> [ <i>protocol-command</i> ]	Optional.
2. Enable information display in a detailed manner.	<b>verbose</b>	Optional. Enabled by default.
3. Enable FTP related debugging when the device acts as the FTP client.	<b>debugging</b>	Optional. Disabled by default.

## Terminating an FTP connection

After the device serving as the FTP client has established a connection with the FTP server, you can use any of the following commands to terminate the FTP connection. For more information about establishing an FTP connection, see "[Establishing an FTP connection](#)."

Task	Command	Remarks
Terminate the connection to the FTP server without exiting FTP client view.	<b>disconnect</b>	Optional. Equal to <b>close</b> .
Terminate the connection to the FTP server without exiting FTP client view.	<b>close</b>	Optional. Equal to <b>disconnect</b> .
Terminate the connection to the FTP server and return to user view.	<b>bye</b>	Optional. Equal to <b>quit</b> in FTP client view.
Terminate the connection to the FTP server and return to user view.	<b>quit</b>	Optional. Available in FTP client view, equal to <b>bye</b> .

## FTP client configuration example

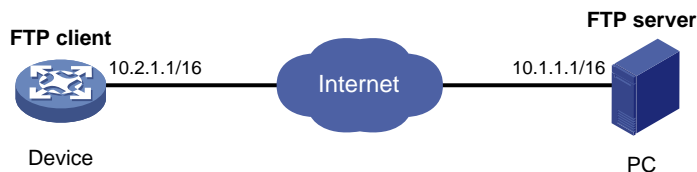
### Network requirements

As shown in [Figure 47](#), the device and PC are reachable to each other.

The device downloads a boot file from the PC for device upgrade, and uploads the configuration file to the PC for backup.

On the PC, the FTP client has an FTP user account, with the username **abc** and the password **abc**, to log in to the FTP server.

**Figure 47 Network diagram**



## Configuration procedure

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
Press CTRL+K to abort
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 Device.

```
[ftp] get newest.bin
227 Entering Passive Mode (10,1,1,1,10,68).
125 BINARY mode data connection already open, transfer starting for /newest.bin.
226 Transfer complete.
FTP: 23951480 byte(s) received in 95.399 second(s), 251.00K byte(s)/sec.
```

# Upload the configuration file **config.cfg** of 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
221 Server closing
```

# Specify **newest.bin** as the main boot file for next startup.

```
<Sysname> boot-loader file newest.bin main
```

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

```
<Sysname> reboot
```

The boot file used at the next startup must be saved under the root directory of the storage medium. You can copy or move a file to the root directory of the storage medium. For more information about **boot-loader**, see *Fundamentals Command Reference*.

## Configuring the FTP server

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

- In 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 if any anomaly, power failure for example, occurs during a file transfer.
- In 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.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Enable the FTP server.	<b>ftp server enable</b>	Required. Disabled by default.
3. Use an ACL to control FTP clients' access to the device.	<b>ftp server acl</b> <i>acl-number</i>	Optional. By default, no ACL is used to control FTP clients' access to the device.
4. Configure the idle-timeout timer.	<b>ftp timeout</b> <i>minutes</i>	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.
5. Set the file update mode for the FTP server.	<b>ftp update { fast   normal }</b>	Optional. Normal update is used by default.
6. Quit to user view.	<b>quit</b>	—
7. Manually release the FTP connection established with the specified username.	<b>free ftp user</b> <i>username</i>	Optional. Available in user view.

## 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, authorize the user to access the directories and configure a password for the user.

Make the following configuration perform authentication and authorization on a local FTP user. To authenticate remote FTP users, you must configure AAA. For detailed configuration about AAA, see *Security Command Reference*.

In local authentication, the device checks the input username and password against those configured on the device. In remote authentication, the device sends the input username and password to the remote authentication server for authentication.

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

When the device serves as the FTP server, to perform the write operations (upload, create, and delete for example) on the device's file system, the FTP login users must be level 3 users; to perform other operations, for example, read operation, users of any level from 0 to 3 are allowed.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Create a local user and enter its view.	<b>local-user</b> <i>user-name</i>	Required. No local user exists by default, and the system does not support FTP anonymous user access.
3. Assign a password to the user.	<b>password</b> { <b>simple</b>   <b>cipher</b> } <i>password</i>	Required.
4. Assign the FTP service to the user.	<b>service-type</b> <b>ftp</b>	Required. By default, the system does not support anonymous FTP access, and does not assign any service. If the FTP service is assigned, the root directory of the device is used by default.
5. Configure user properties.	<b>authorization-attribute</b> { <b>acl</b> <i>acl-number</i>   <b>callback-number</b> <i>callback-number</i>   <b>idle-cut</b> <i>minute</i>   <b>level</b> <i>level</i>   <b>user-profile</b> <i>profile-name</i>   <b>vlan</b> <i>vlan-id</i>   <b>work-directory</b> <i>directory-name</i> } *	Optional. By default, the FTP/SFTP users can access the root directory of the device, and the user level is 0. You can change the default configuration by using this command.

## FTP server configuration example

### Network requirements

As shown in Figure 48, the device and PC are reachable to each other.

The PC keeps the newest boot file of the device. Use FTP to upgrade the device and back up the configuration file.

Set the username to **abc** and the password to **abc** for the FTP client to log in to the FTP server.

**Figure 48 Network diagram**



## Configuration procedure

### 1. Configure the device (FTP server)

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

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

# 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
```

2540 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)): abc
331 Password required for abc.
Password:
230 User logged in.
```

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

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

```
# Upload the configuration file newest.bin to the device.
ftp> put newest.bin
200 Port command okay.
150 Opening ASCII mode data connection for /newest.bin.
226 Transfer complete.
ftp> bye
221 Server closing.

c:\>
```

---

**NOTE:**

- You can 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 (For a device that has been partitioned, the configuration file must be saved on the first partition.).
  - After transferring the Boot ROM program through FTP, you must execute **bootrom update** to upgrade the Boot ROM.
- 

### 3. Upgrade the device

# Specify **newest.bin** as the main boot file for next startup.

```
<Sysname> boot-loader file newest.bin main
```

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

```
<Sysname> reboot
```

The boot file used at the next startup must be saved under the root directory of the storage medium. You can copy or move a file to the root directory of the storage medium. For more information about **boot-loader**, see *Fundamentals Command Reference*.

## Displaying and maintaining FTP

Task	Command	Remarks
Display the source IP address configuration of the FTP client.	<b>display ftp client configuration</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.
Display the configuration of the FTP server.	<b>display ftp-server</b>	Available in any view.
Display detailed information about logged-in FTP users.	<b>display ftp-user</b>	Available in any view.

# Configuring TFTP

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 operations, 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 two modes:

- **Binary mode**—Transfers files as raw data, such as **.bin** and **.btm** files.
- **ASCII mode**—Transfers files as text, such as **.txt**, **.bat**, and **.cfg** files.

## Operation

Only the TFTP client service is available with your device.

**Figure 49 Network diagram**



Before using TFTP, the administrator must configure IP addresses for the TFTP client and server, and ensure 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 21 Configuration when the device serves as the TFTP client**

Device	Configuration	Remarks
Device (TFTP client)	<ul style="list-style-type: none"><li>• Configure the IP address and routing function, and ensure the route between the device and the TFTP server is available.</li><li>• Use <b>tftp</b> to establish a connection to the remote TFTP server to upload/download files to/from the TFTP server.</li></ul>	—
PC (TFTP server)	Enable TFTP server on the PC, and configure the TFTP working directory.	—

## Configuring the TFTP client

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



- **Normal download**—The device writes the obtained file to the storage medium directly. If you download a remote file using a filename *destination-filename* that exists in the target directory, the device deletes the original file and saves the new one. If file download fails because of network disconnection or other reasons, the original 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 target directory, the original file is not overwritten. If file download fails because of 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 nonexistent in the target directory.

When using **tftp client source** or **tftp**, specify the source interface (such as a loopback or dialer interface) 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 TFTP packets.

The TFTP client follows these rules to select the source IP address of packets sent to the TFTP server:

- If no source IP address is specified, the IP address of the output interface of the route to the server is used as the source IP address.
- The source IP address specified with **tftp client source** or **tftp** is used.
- If you first use **tftp client source** to specify a source IP address and then use **tftp** to specify another source IP address, the latter is used.
- The source IP address specified with the **tftp client source** command applies to all TFTP connections while the one specified with the **tftp** command applies to the current TFTP connection only.

To configure the TFTP client:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Use an ACL to control the device's access to TFTP servers.	<b>tftp-server [ ipv6 ] acl</b> <i>acl-number</i>	Optional. By default, no ACL is used to control the device's access to TFTP servers.
3. Specify the source IP address of sent TFTP packets.	<b>tftp client source { interface</b> <i>interface-type interface-number</i>   <b>ip</b> <i>source-ip-address</i> }	Optional. By default, the source IP address is determined by the route from the TFTP client to the TFTP server.  If no primary IP address is configured on the source interface, no TFTP connection can be established.  If you use <b>tftp client source</b> 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.
4. Return to user view.	<b>quit</b>	—

Step	Command	Remarks
5. Download or upload a file in an IPv4 network.	<b>tftp</b> server-address { <b>get</b>   <b>put</b>   <b>sget</b> } source-filename [ destination-filename ] [ <b>vpn-instance</b> vpn-instance-name ] [ <b>source</b> { <b>interface</b> interface-type interface-number   <b>ip</b> source-ip-address } ]	Optional. Available in user view.
6. Download or upload a file in an IPv6 network.	<b>tftp ipv6</b> tftp-ipv6- server [ -i interface-type interface-number ] { <b>get</b>   <b>put</b> } source-filename [ destination-filename ] [ <b>vpn-instance</b> vpn-instance-name ]	Optional. Available in user view.

## Displaying and maintaining the TFTP client

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

## TFTP client configuration example

### Network requirements

As shown in Figure 50, the device and PC are reachable to each other.

The device downloads a boot file from the PC for upgrading and uploads a configuration file **config.cfg** to the PC for backup.

Figure 50 Smooth upgrading using the TFTP client function



### Configuration procedure

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). (Details not shown)
  - On the PC, enable the TFTP server
  - Configure a TFTP working directory
2. Configure Device (TFTP client)

# Download application file **newest.bin** from the 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 for next startup.

```
<Sysname> boot-loader file newest.bin main
```

# Reboot the device and the software is upgraded.

```
<Sysname> reboot
```

The boot file used for the next startup must be saved under the root directory of the storage medium. You can copy or move a file to the root directory of the storage medium. For more information about **boot-loader**, see *Fundamentals Command Reference*.

# License management

## Registering the software

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Registering the software	No	No	No	No	Yes. Supported only by MPU-G2.

The system software comes with a trial period. You must register the software within its trial period. If you do not register the software before the trial period expires, the software automatically restarts every 30 minutes.

To avoid continual system restarting because of trial period expiration, purchase a license for the software and register the software before the trial period expires. You can view the registration information by using **display license**.

Task	Command	Remarks
Register the system software.	<b>license register</b> <i>serial-number</i>	Required. Available in user view.

## Displaying and maintaining licenses

The following matrix shows the feature and router compatibility:

Feature	MSR900	MSR20-1X	MSR20	MSR30	MSR50
Displaying and maintaining licenses	No	No	No	No	Supported only by MPU-G2.

To display system software registration:

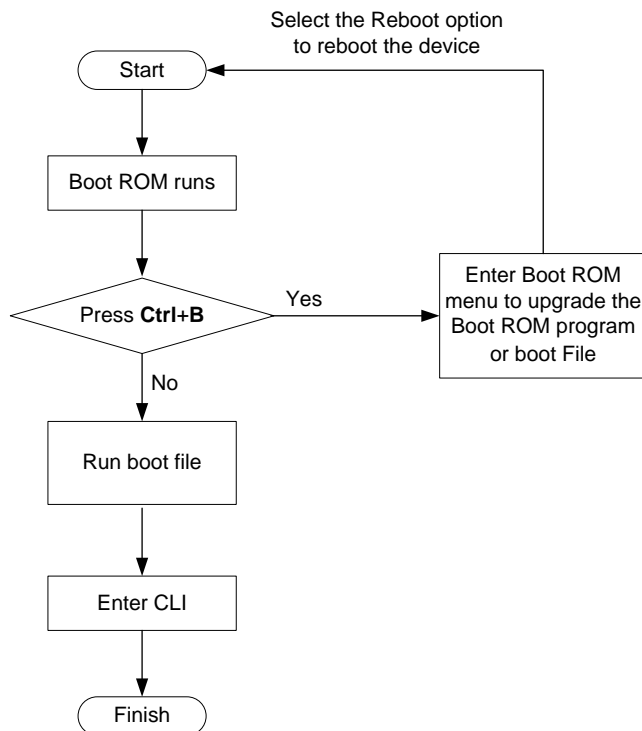
Task	Command	Remarks
Display the system software registration information.	<b>display license</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view.

# Configuring software upgrade

## Overview

Router software comprises the Boot ROM program and the system boot file. After being powered on, the router runs the Boot ROM program, initializes the hardware, and displays the hardware information. Then the router 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 router. [Figure 51](#) illustrates their relationship.

**Figure 51 Relationship between the Boot ROM program and the system boot file**



## 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 the upgrading through command lines. For instructions about how to upgrade them through the Boot ROM menu, see the installation menu of your router.

The upgrading at the CLI falls into the following categories:

Upgrade method	Upgrade object	Description
Software upgrade through a system reboot	Boot ROM program and system boot file	You must reboot the whole system to upgrade the software of a device. This causes running service interruption during the upgrade process, and is not recommended.
Software upgrade by installing hotfixes	System boot file	Hotfix is a fast, cost-effective method to repair software defects of a router. Compared with software version upgrade, hotfix can upgrade the software without interrupting the running services of the router. In other words, it can repair the software defects of the current version without rebooting the router.

## Software upgrade through a system reboot

### Upgrading the Boot ROM program through a system reboot

#### ⚠ CAUTION:

You must save the Boot ROM file in the root directory of the router. You can copy or move a file to change the path of it to the root directory.

1. Copy the Boot ROM program to the root directory of the router's storage media by using FTP or TFTP.
2. Specify the Boot ROM program to be used at the next boot at the CLI.
3. Reboot the router to make the specified Boot ROM program take effect.

Task	Command	Remarks
Read, restore, back up, or upgrade the Boot ROM program on routers or subcards.	<b>bootrom { backup   read   restore   update file file-url } [ slot slot-number -list ] [ all   part ]</b>	Required. All contents of the Boot ROM file are operated if the <b>all</b> and <b>part</b> keywords are not specified. Available in user view.

### 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. You can copy or move a file to change the path of it to the root directory.

1. Save the boot file to the root directory of the router's storage media by using FTP, TFTP, or other approaches.
2. Specify the boot file to be used at the next boot of the router at the CLI.
3. Reboot the router to make the boot file take effect.

To specify a boot file to be used at the next boot:

Task	Command	Remarks
Specify a boot file to be used at the next boot.	<b>boot-loader file</b> <i>file-url</i> { <b>main</b>   <b>backup</b> }	Required. Available in user view.

## Software upgrade by installing hotfixes

Hotfix is a fast, cost-effective method to repair software defects of a router. Compared with software upgrade, hotfix can upgrade the software without interrupting running services or rebooting the router.

### Basic concepts

#### Patch and patch file

A patch, also called patch unit, is a package to fix software defects. Generally, patches are released as patch files. A patch file may contain one or more patches for different defects. After being 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.

#### Incremental patch

An incremental patch means that the patch is dependent on the previous patch units. For example, if a patch file has three patch units, patch 3 can be running only after patch 1 and 2 take effect. You cannot run patch 3 separately.

The released patches are all incremental patches.

#### Common patch and temporary patch

- Common patches are those formally released through the version release flow.
- Temporary patches are those not formally released through the version release flow, but temporarily provided to solve the emergent problems.

The common patches always include the functions of the previous temporary patches to replace them. The patch type affects the patch loading process only; the system deletes all the temporary patches before it loads the common patch.

#### Patch package

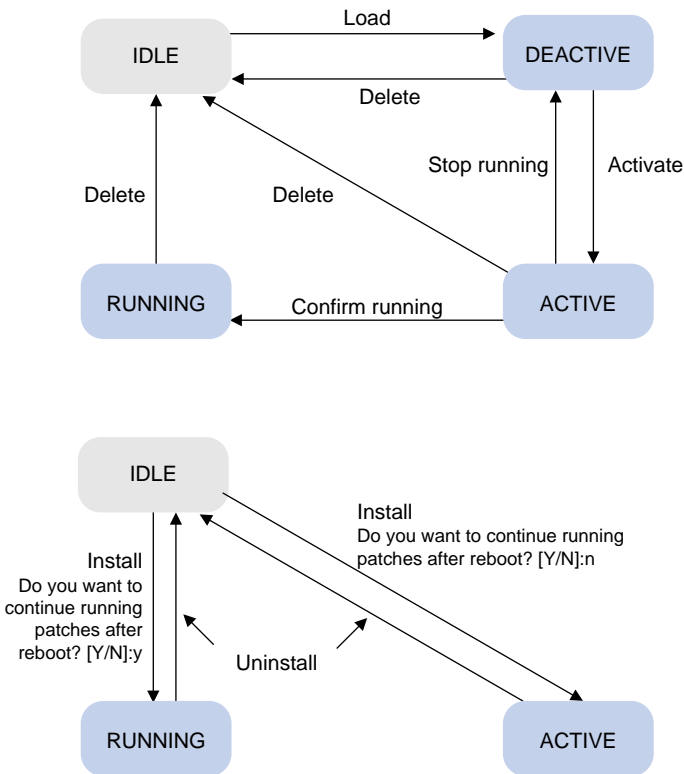
A patch package contains patches of the same version but for various types of cards. When executing a patch package, the system automatically finds out the proper patch for each card, and loads them to the cards, simplifying patch operation and patch version management.

### 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 52](#). 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 deactivate**,

**patch delete**, **patch install**, and **undo patch install**. For example, if you execute **patch active** for the patches in the DEACTIVE state, the patches turn to the ACTIVE state.

Figure 52 Relationship between patch state changes and command actions

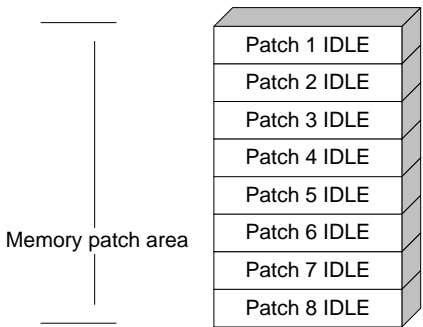


Information about patch states is saved in file **patchstate** on the flash. HP recommends you not operate this file.

**IDLE state**

Patches in the IDLE state are not loaded. You cannot install or run the patches, as shown in Figure 53 (suppose the memory patch area can load up to eight patches).

Figure 53 Patches are not loaded to the memory patch area



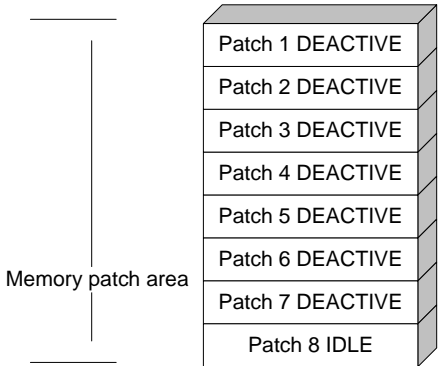
Currently, the memory patch area supports up to 200 patches.



### DEACTIVE state

Patches in the DEACTIVE state have been loaded to the memory patch area but have not yet run in the system. Suppose there are seven patches in the patch file to be loaded. 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 54](#).

**Figure 54** A patch file is loaded to the memory patch area

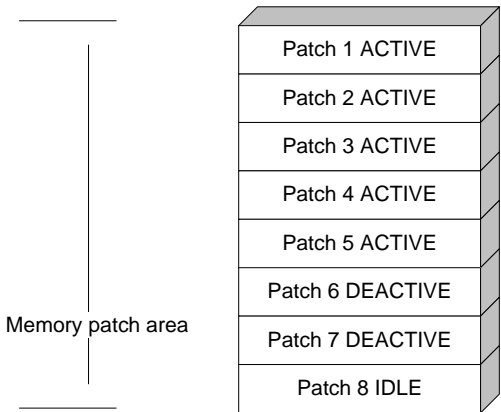


### ACTIVE state

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 54](#), 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 55](#).

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

**Figure 55** Patches are activated

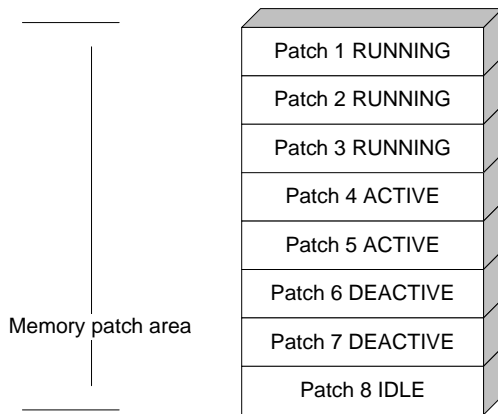


### RUNNING state

After you confirm the running of the ACTIVE patches, the state of the patches become RUNNING and are in the RUNNING state after system reboot. For the five patches in [Figure 55](#), 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 56](#).

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

Figure 56 Patches are running



## Configuration task list

Task		Remarks
Install patches	One-step patch installation	Use either approach.
	Step-by-step patch installation	The step-by-step patch installation allows you to control the patch status.
Step-by-step patch uninstallation		Optional.

## Configuration prerequisites

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

- 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 predefined and support for the PATCH-FLAG depends on router model or card type. 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 media (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.

The default name of a patch file is patchmain.bin.

## One-step patch installation

To install patches in one step, execute **patch install** with specifying either the directory where the patch file locates or the filename of the patch package.

After executing the command, the system displays the message "Do you want to continue running patches after reboot? [Y/N]:".

- Entering **y** or **Y**: All the 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** or **N**: All the 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.

To install a patch package, save the patch package file to the storage media of the AMB. The SMB and all interface cards will load the patch file from the AMB.

To install the patches in one step:

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Install the patches in one step.	<b>patch install</b> { <i>patch-location</i>   <b>file</b> <i>patch-package</i> }	Required.

The patch matches the card type and software version.

If you install a patch file by specifying the directory where the patch file locates, **patch install** changes the patch file location specified with **patch location** to the directory specified by the *patch-location* argument of **patch install**.

If you install a patch file by specifying the filename of the patch package, **patch install** will not change the patch file location specified with **patch location**.

To uninstall all patches in one operation, use **undo patch install**, which is the same as performing [Step-by-step patch uninstallation](#).

## Step-by-step patch installation

Step-by-step patch installation enables you to control the patch status during the patch installation process.

### Installation task list

Task	Remarks
<a href="#">Configuring the patch file location</a>	Optional. To install a patch package, skip this step.
<a href="#">Loading a patch file</a>	Required.
<a href="#">Activating patches</a>	Required.
<a href="#">Confirming running patches</a>	Optional.

### Configuring the patch file location

If you save the patch files to another storage media except the Flash on the router, you must specify the directory where the patch files are located with the *patch-location* argument. Then the system loads the appropriate patch files from the specified directory. If the router has only one storage media, you do not need to execute this command.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—

Step	Command	Remarks
2. Configure the patch file location.	<b>patch location</b> <i>patch-location</i>	Optional. <b>flash:</b> by default.

If you install a patch file by specifying the directory where the patch file locates, after **patch install** is executed, the system automatically changes patch file location specified with **patch location** to the directory specified by the *patch-location* argument of **patch install**. For example, if you execute **patch location** xxx and then **patch install** yyy, the patch file location automatically changes from xxx to yyy.

## Loading a patch file

Loading the right patch files is the basis of other hotfixing operations.

- If you install a patch from a patch file, the system loads a patch file from the Flash by default. If the system cannot find the patch file on the Flash, it tries to load the patch file from the CF card.
- If you install a patch from a patch package, the system finds the correct patch file in the patch package file and loads the patch file.



### CAUTION:

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

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Load the patch file from the storage media (such as the Flash or the CF card) to the memory patch area.	<b>patch load</b> [ <b>file</b> <i>patch-package</i> ]	Required.

## Activating patches

After activating a patch, the patch takes effect and is in the test-run stage. After the router is reset or rebooted, the patch becomes invalid.

If you find that an ACTIVE patch is a problem, reboot the router to deactivate the patch, to avoid a series of running faults resulting from patch error.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Activate patches.	<b>patch active</b> [ <i>patch-number</i> ]	Required.

## Confirming running patches

After you confirm the running of a patch, the patch state becomes RUNNING, and the patch is in the normal running stage. After the router is reset or rebooted, the patch is still valid.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Confirm the running of patches.	<b>patch run</b> [ <i>patch-number</i> ]	Required. This operation is applicable to patches in the ACTIVE state only.

# Step-by-step patch uninstallation

## Uninstallation task list

Task	Remarks
<a href="#">Stopping running patches</a>	Required
<a href="#">Deleting patches</a>	Required

## Stopping running patches

When you stop running a patch, the patch state becomes DEACTIVE, and the system returns to the way it ran before the patch was installed.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Stop running patches.	<b>patch deactivate</b> [ <i>patch-number</i> ]	Required.

## Deleting patches

Deleting patches only removes the patches from the memory patch area, and does not delete them from the storage media. The patches turn to IDLE state after this operation. After a patch is deleted, the system returns to the way it ran before the patch was installed.

Step	Command	Remarks
1. Enter system view.	<b>system-view</b>	—
2. Delete the specified patches from the memory patch area.	<b>patch delete</b> [ <i>patch-number</i> ]	Required.

# Displaying and maintaining software upgrade

Task	Command	Remarks
Display information about the boot file.	<b>display boot-loader</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	Available in any view
Display information about the patch package.	<b>display patch</b>	
Display the patch information.	<b>display patch information</b> [   { <b>begin</b>   <b>exclude</b>   <b>include</b> } <i>regular-expression</i> ]	

# Configuration examples

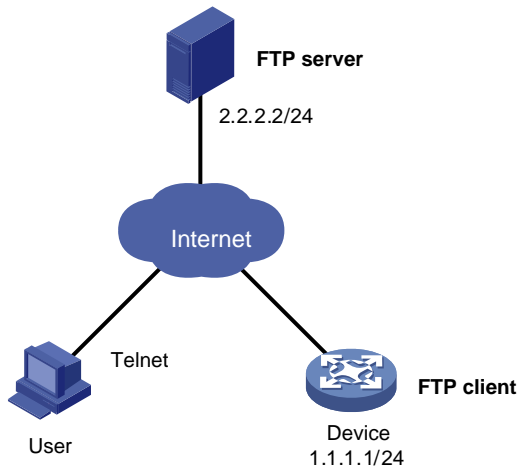
## Network requirement

As shown in [Figure 57](#), the current software version is **soft-version1** for the device. Upgrade the software version of the device to **soft-version2** and configuration file to **new-config** at a time when few services are processed (for example, at 3 am) through remote operations.

The latest application **soft-version2.bin** and the latest configuration file **new-config.cfg** are both saved in the **aaa** directory of the FTP server.

The device and FTP server can reach each other. A user can log in to the device via Telnet, and the user and device can reach each other.

**Figure 57 Network diagram**



## Configuration procedure

1. Configure the FTP server (Configurations may vary with different types of servers)
  - Set the access parameters for the FTP client (including enabling the FTP server function, setting the FTP username to **aaa** and password to **hello**, and setting the user to have access to the **flash:/aaa** directory).

```
<FTP-Server> system-view
[FTP-Server] ftp server enable
[FTP-Server] local-user aaa
[FTP-Server-luser-aaa] password cipher hello
[FTP-Server-luser-aaa] service-type ftp
[FTP-Server-luser-aaa] authorization-attribute work-directory flash:/aaa
```

- Use text editor on the FTP server to edit batch file **auto-update.txt**. The following is the content of the batch file:

```
return
startup saved-configuration new-config.cfg
boot-loader file soft-version2.bin main
reboot
```

2. Configure the device

# Log in to the FTP server (The prompt may vary with servers.)

```
<Device> ftp 2.2.2.2
Trying 2.2.2.2 ...
Press CTRL+K to abort
Connected to 2.2.2.2.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(2.2.2.2:(none)):aaa
331 Give me your password, please
Password:
230 Logged in successfully
[ftp]
```

# Download file **auto-update.txt** on the FTP server.

```
[ftp] ascii
[ftp] get auto-update.txt
```

# Download file **new-config.cfg** on the FTP server.

```
[ftp]get new-config.cfg
```

# Download file **soft-version2.bin** on the FTP server.

```
[ftp] binary
```

```
[ftp] get soft-version2.bin
```

```
[ftp] bye
```

```
<Device>
```

# Change the extension of file **auto-update.txt** to **.bat**.

```
<Device> rename auto-update.txt auto-update.bat
```

To ensure correctness of the file, use the **more** command to view the content of the file.

# Execute the scheduled automatic execution function to enable the device to be automatically upgraded at 3 am.

```
<Device> system-view
```

```
[Device] job autoupdate
```

```
[Device-job-autoupdate] view system-view
```

```
[Device-job-autoupdate] time 1 one-off at 03:00 command execute auto-update.bat
```

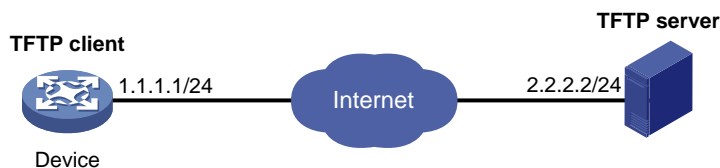
To check if the upgrade is successful after the device reboots, use **display version**.

## Hotfix configuration example

### Network requirements

- As shown in [Figure 58](#), the software running on the device is of some problem, and thus hotfixing is needed.
- The patch file **patch\_xxx.bin** is saved on the TFTP server.
- The IP address of the device is 1.1.1.1/24, and IP address of TFTP Server is 2.2.2.2/24. The device and TFTP server can reach each other.

**Figure 58 Network diagram of hotfix configuration**



### Configuration procedure

1. Configure TFTP Server. The configuration varies depending on server type. (Details not shown)
  - Enable the TFTP server function.
  - Save the patch file **patch\_xxx.bin** to the directory of the TFTP server.
2. Configure the device



#### CAUTION:

Ensure the free Flash space of the device is big enough to store the patch file.

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

# Load the patch file patch_xxx.bin from the TFTP server to the root directory of the device storage media.
<Device> tftp 2.2.2.2 get patch_xxx.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.
```



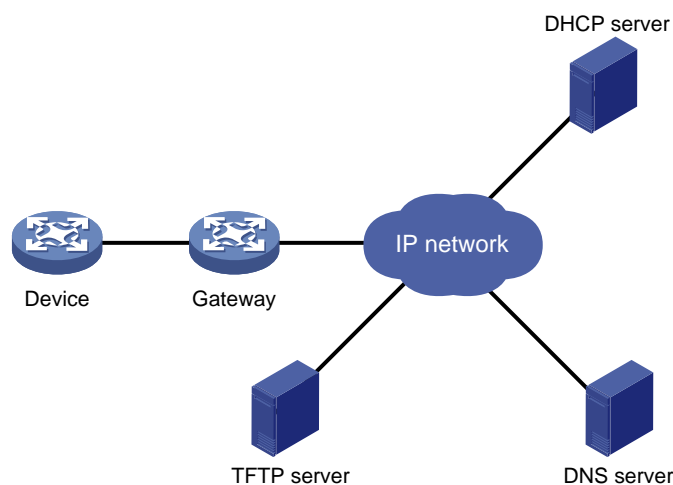
# Automatic configuration

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

Figure 59 Network diagram for automatic configuration



As shown in Figure 59, 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. The device gets the files needed from the TFTP server, such as the host name file that saves mappings between host IP addresses and host names, and the configuration file.
- **DNS server**—Resolves between IP addresses and host names. In some cases, the device resolves its IP address to the corresponding host name through the DNS server, and then uses the host name to request the configuration file with the same name (**hostname.cfg**) from the TFTP server. If the device gets the domain name of the TFTP server from the DHCP response, the device can also resolve the domain name of the TFTP server to the IP address of the TFTP server through the DNS server.

If the DHCP server, TFTP server, DNS server, and the device are not in the same network segment, you must configure the DHCP relay agent on the gateway, and configure routing protocols to enable each server and the device to reach one another.

## How automatic configuration works

Automatic configuration works in the following manner:

1. During startup, the device sets the first up interface (if up Layer 2 Ethernet interfaces exist, 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.
2. After getting related parameters, the device sends a TFTP request to obtain the configuration file from the specified TFTP server and executes the configuration file. If the client cannot get such parameters, it uses factory default configuration.

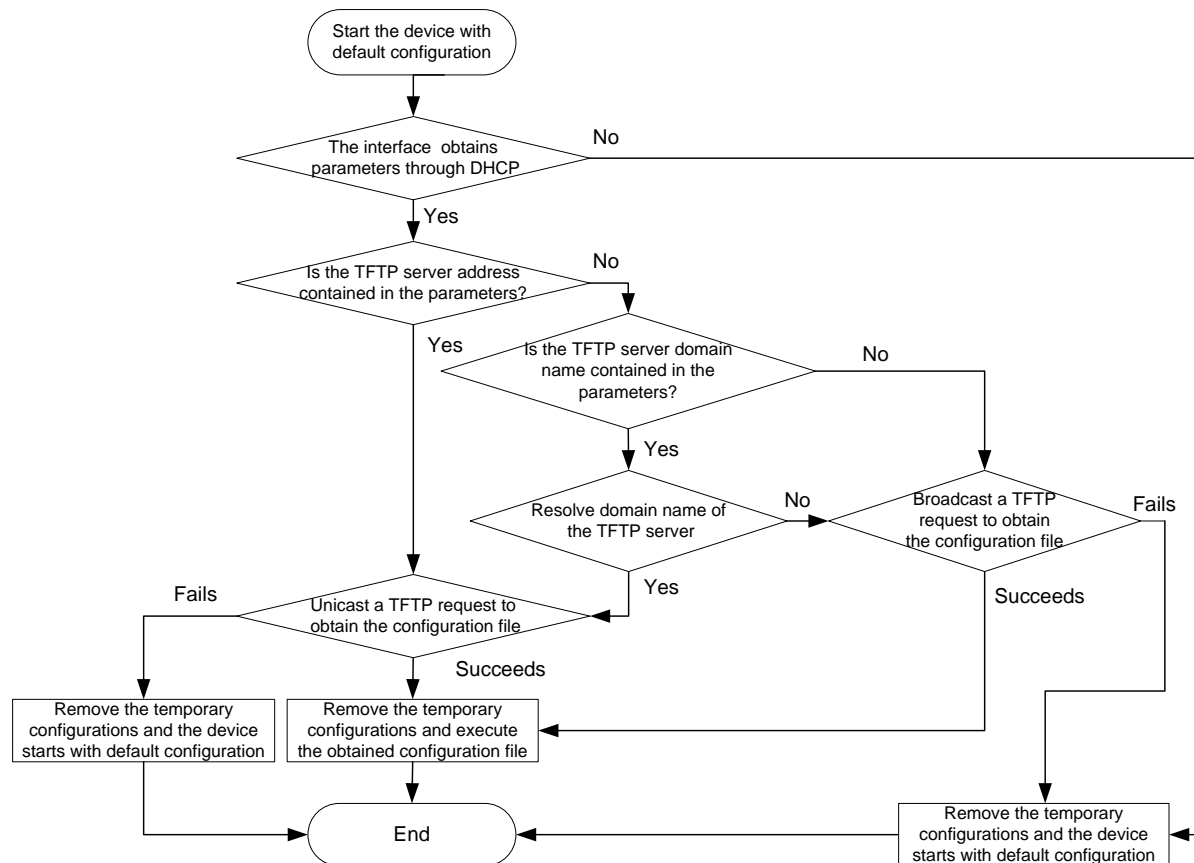
To implement automatic configuration, you must configure the DHCP server, DNS server, and TFTP server, but you do not need to perform any configuration on the device performing automatic configuration. The configuration of these servers varies with device models and is omitted.

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

## Work flow

Figure 60 shows the work flow of automatic configuration.

**Figure 60 Work flow of automatic configuration**



# Using DHCP to obtain an IP address and other configuration information

## Address acquisition process

As mentioned above, a device sets the first up interface as the DHCP client during startup. The DHCP client broadcasts a DHCP request, where the Option 55 field specifies the information that the client wants to obtain from the DHCP server such as the configuration file name, domain name, and IP address of the TFTP server, and DNS server IP address.

After receiving the DHCP response from the DHCP server, the device obtains the IP address and resolves the following fields in the DHCP response:

- **Option 67 or the file field**—Obtains the configuration file name. The device resolves Option 67 first. If Option 67 contains the configuration file name, the device does not resolve the file field. If not, the device resolves the file field.
- **Option 66**—Obtains the TFTP server domain name
- **Option 150**—Obtains the TFTP server IP address
- **Option 6**—Obtains the DNS server IP address

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

The temporary configuration contains two parts: the configuration made on the interface through which automatic configuration is performed, and **ip host** in the host name file (For more information, see *Layer 3—IP Services Command Reference*). The temporary configuration is removed by executing the corresponding **undo** commands.

For more information about DHCP, see *Layer 3—IP Services Configuration Guide*.

## DHCP server address pool selection principles

The DHCP server selects IP addresses and other network configuration parameters from an address pool for clients. DHCP supports the following types of address pools:

- **Dynamic address pool**—A dynamic address pool contains a range of IP addresses and other parameters that the DHCP server dynamically assigns to clients.
- **Static address pool**—A static address pool contains the binding of an IP address and a MAC address (or a client ID). The DHCP server assigns the IP address of the binding and specific configuration parameters to a requesting client whose MAC address or ID is contained in the binding. In this way, the client can get a fixed IP address.

Select address pools by using one of the following methods:

- If devices use the same configuration file, you can configure a dynamic address pool on the DHCP server to assign IP addresses and the same configuration parameters (for example, configuration file name) to the devices. In this case, the configuration file can only contain common configurations of the devices, and the specific configurations of each device need to be performed in other ways. For example, the configuration file can enable Telnet and create a local user on devices so the administrator can telnet to each device to perform specific configurations (for example, configure the IP address of each interface).
- If devices use different configuration files, you must configure static address pools to ensure 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 corresponding client IDs. To obtain a device's client ID, use **display dhcp server ip-in-use** to display address binding information on the DHCP server after the device obtains its IP address through DHCP.

## Obtaining the configuration file from the TFTP server

### File types

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, which is named **network.cfg**. The host name file stores mappings between IP addresses and host names.

For example, the host name file can include the following:



#### 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.

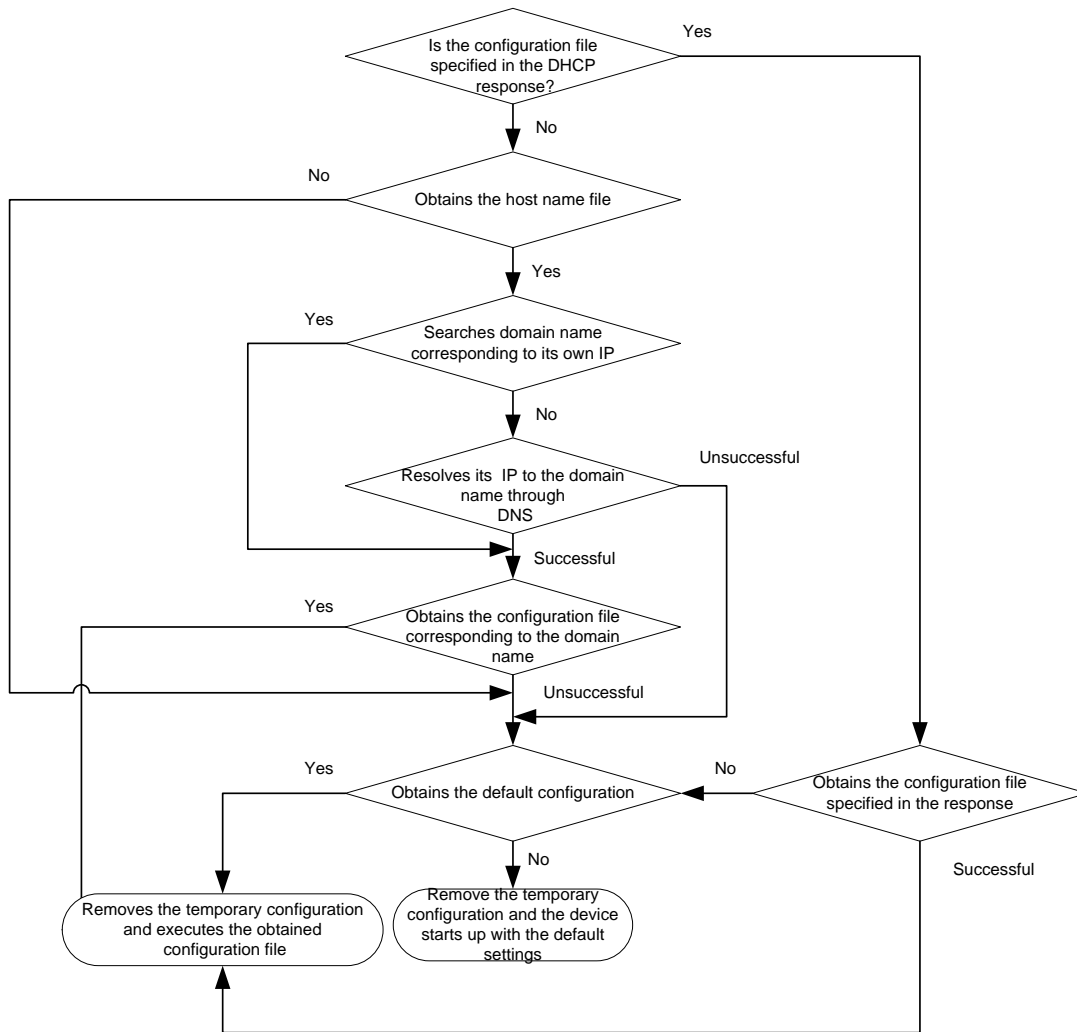
---

```
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 61 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 not, the device tries to get its host name from the host name file obtained from the TFTP server. If it fails, the device resolves its IP address to the host name through DNS server. Once the device gets its host name, it requests the configuration file with the same name from the TFTP server.
- If all the above operations fail, the device requests the default configuration file from the TFTP server.

## TFTP request sending mode

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

- If a legitimate TFTP server IP address is contained in the DHCP response, the device unicasts a TFTP request to the TFTP server.
- If not, the device resolves the TFTP server domain name contained in the DHCP response to the corresponding IP address through the DNS server. If successful, the device unicasts a TFTP request to the TFTP server; if not, the device broadcasts a TFTP request.

- If the IP address and the domain name of the TFTP server are not contained in the DHCP response or they are illegitimate, the device broadcasts a TFTP request.

After broadcasting a TFTP request, the device selects the TFTP server that responds first to obtain the configuration file. If the requested configuration file does not exist on the TFTP server, the request operation fails, and the device removes the temporary configuration and starts up with 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, so 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 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>
- HP Education <http://www.hp.com/learn>

# Conventions

This section describes the conventions used in this documentation set.





## Command conventions

Convention	Description
<b>Boldface</b>	<b>Bold</b> text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	<i>Italic</i> text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x   y   ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[ x   y   ... ]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x   y   ... } *	Asterisk-marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[ x   y   ... ] *	Asterisk-marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

## GUI conventions

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




## Symbols

Convention	Description
 <b>WARNING</b>	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 <b>CAUTION</b>	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.
 <b>IMPORTANT</b>	An alert that calls attention to essential information.
<b>NOTE</b>	An alert that contains additional or supplementary information.
 <b>TIP</b>	An alert that provides helpful information.

## Network topology icons

	Represents a generic network device, such as a router, switch, or firewall.
---	---



	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.

### Port numbering in examples

The port numbers in this document are for illustration only and might be unavailable on your device.

---

# Index

- 16-bit interface index, 105
- AAA authentication, 13, 14
- absolute numbering, 23
- accessing history commands, 8
- ACL
  - configuring source IP-based web login control, 91
- ACL (web login control), 90
- activating patches, 149
- ACTIVE patch state, 146
- address
  - DHCP acquisition process, 156
  - DHCP server pool selection principles, 156
- aliases (configuring), 6
- authentication
  - AUX port login modes, 48
  - configuring AUX port login AAA authentication, 51
  - configuring AUX port login none authentication, 49
  - configuring AUX port login password authentication, 50
  - configuring console login none authentication, 28
  - configuring console login password authentication, 29
  - configuring console login scheme authentication, 30
  - configuring FTP server, 133
  - configuring modem login AAA authentication, 66
  - configuring modem login none authentication, 64
  - configuring modem login password authentication, 65
  - configuring Telnet login none authentication, 37
  - configuring Telnet login password authentication, 38
  - configuring Telnet login scheme authentication, 39
  - console login modes, 27
  - modem login modes, 63
  - setting mode for user privilege level switch, 16
  - Telnet login modes, 36
- authorization (FTP server), 133
- automatic configuration, 154
  - executing configuration file, 159
  - file types, 157
  - how it works, 154
  - obtaining file from TFTP server, 157
  - obtaining IP address with DHCP, 156
  - obtaining the configuration file, 158
  - TFTP request sending mode, 158
- automatic save (running configuration), 114
- AUX port
  - configuring login AAA authentication, 51
  - configuring login none authentication, 49
  - configuring login optional common settings, 54
  - configuring login password authentication, 50
  - login, 48
  - login authentication modes, 48
- backing up (startup configuration file), 115
- banner
  - configuration, 96
  - message input mode, 96
  - types, 96
- batch operations, 121
- buffer (history buffer size), 9
- card
  - configuring interface card working mode, 104
  - temperature threshold, 103
- changing current working directory, 119
- checking
  - command line errors, 8

- NAND memory files, 123
- clearing unused interface indexes, 105
- CLI
  - checking syntax errors, 8
  - configuration, 1
  - display options, 9
  - displaying, 20
  - displaying login, 71
  - entering, 1
  - incomplete keywords, 5
  - login, 24
  - maintaining login, 71
  - overview, 1
  - using online help, 4
  - views, 2
- client
  - configuring device login as Telnet client, 44
  - configuring FTP client, 127
  - configuring TFTP, 137, 139
  - FTP configuration, 131
- command
  - accessing history commands, 8
  - configuring aliases, 6
  - configuring hotkeys, 6
  - configuring user level, 12
  - conventions used, 1
  - editing command lines, 5
  - entering, 5
  - filtering output information, 10
  - modifying level, 19
  - redisplaying unsubmitted commands, 7
  - undo form, 2
  - using history, 8
- common patch (hotfix), 144
- common settings
  - configuring AUX port login options, 54
  - configuring modem login options, 68
  - console options, 33
  - Telnet login (VTY user interfaces), 42
- configuration file
  - automatic device configuration, 154
  - backing up startup configuration file, 115
  - coexistence of multiples, 110
  - configuring parameters (saving current running configuration), 113
  - content, 110
  - deleting startup configuration file, 116
  - displaying, 117
  - enabling running configuration automatic save, 114
  - encrypting, 111
  - executing, 159
  - factory default configuration, 109
  - format, 110
  - management, 109
  - obtaining (automatic configuration), 158
  - restoring startup configuration file, 116
  - running configuration, 109
  - running configuration manual save, 114
  - saving running configuration, 110
  - setting configuration rollback, 115
  - setting rollback, 112
  - specifying startup configuration file, 115
  - startup, 110
  - startup configuration, 109
- configuring
  - AUX port login, 48
  - AUX port login AAA authentication, 51
  - AUX port login none authentication, 49
  - AUX port login optional common settings, 54
  - AUX port login password authentication, 50
  - banner, 96
  - card temperature thresholds, 103

- changing system time, 92
- CLI, 1
- CLI hotkeys, 6
- command aliases, 6
- configuration file management, 109
- console login none authentication, 28
- console login optional common settings, 33
- console login password authentication, 29
- console login scheme authentication, 30
- console port login, 24
- detection interval, 102
- device login as Telnet client, 44
- device name, 92
- exception handling, 98
- FTP, 126
- FTP client, 127, 131
- FTP server, 133, 134
- FTP server authentication, 133
- FTP server authorization, 133
- hotfix software upgrade, 152
- HTTP login, 73, 77
- HTTPS login, 75, 78
- interface card working mode, 104
- job scheduling, 99, 101
- max number concurrent users, 97
- modem login, 59
- modem login AAA authentication, 66
- modem login none authentication, 64
- modem login optional common settings, 68
- modem login password authentication, 65
- NMS login, 81
- NMS monitored interfaces, 103
- patch file location, 148
- saving current configuration, 19
- software upgrade, 142, 150
- source and destination IP-based Telnet user login control, 86
- source IP-based NMS user login control, 88, 89
- source IP-based Telnet user login control, 85
- source IP-based web user login control, 90, 91
- source MAC-based Telnet user login control, 87
- SSH client, 47
- SSH login, 44
- SSH server, 45
- Telnet login, 36
- Telnet login none authentication, 37
- Telnet login optional common settings (VTY user interfaces), 42
- Telnet login password authentication, 38
- Telnet login scheme authentication, 39
- Telnet user login control, 85
- TFTP, 137
- TFTP client, 137, 139
- user command levels, 12
- user login control, 85
- user privilege level, 13
- user privilege level under a user interface, 14, 15
- user privilege level using AAA authentication, 13, 14
- user privilege levels, 12
- confirming running patches, 149
- connecting
  - debugging FTP connection, 130
  - establishing FTP connection, 127
  - maintaining FTP connection, 130
  - terminating FTP connection, 131
- console
  - configuring login none authentication, 28
  - configuring login optional common settings, 33
  - configuring login password authentication, 29
  - configuring login scheme authentication, 30
  - logging in through console port, 24

- login authentication modes, 27
- contacting HP, 160
- content (configuration file), 110
- controlling CLI display, 9
- copying file, 120
- copyright display, 95
- creating directory, 119
- current working directory
  - changing, 119
  - displaying, 119
- DEACTIVE patch state, 146
- debugging FTP connection, 130
- deleting
  - file, 121
  - patches, 150
  - startup configuration file, 116
- device
  - automatic configuration, 154
  - changing system time, 92
  - clearing unused interface, 105
  - CLI configuration, 1
  - configuring banner, 96
  - configuring card temperature threshold, 103
  - configuring detection interval, 102
  - configuring exception handling, 98
  - configuring interface card working mode, 104
  - configuring login as Telnet client, 44
  - configuring max number concurrent users, 97
  - configuring name, 92
  - configuring NMS monitored interfaces, 103
  - diagnosing transceiver modules, 106
  - displaying management, 107
  - enabling copyright display, 95
  - management, 92
  - rebooting router, 98
  - rebooting router at the CLI, 98
  - scheduling job, 99, 101
  - scheduling reboot, 98
  - verifying transceiver modules, 106
- DHCP
  - address acquisition process, 156
  - automatic device configuration, 154
  - obtaining configuration information, 156
  - obtaining IP address, 156
  - server address pool selection principles, 156
- diagnosing transceiver modules, 106
- directory
  - changing current working directory, 119
  - creating, 119
  - displaying current working directory, 119
  - displaying information, 119
  - FTP server, 129
  - management, 119
  - removing, 119
- disabling multi-screen display, 10
- displaying
  - bad NAND memory blocks, 123
  - CLI login, 71
  - CLI options, 9
  - configuration file, 117
  - copyright, 95
  - current working directory, 119
  - device management, 107
  - directory information, 119
  - disabling multi-screen display, 10
  - file contents, 120
  - file information, 120
  - filtering output information, 10
  - FTP, 136
  - licenses, 141
  - multiscreen (CLI), 9
  - NAND flash memory, 123

- software upgrade, 150
- TFTP client, 139
- web login, 76
- displaying CLI, 20
- DNS (automatic device configuration), 154
- documentation
  - conventions used, 161
  - website, 160
- editing command lines, 5
- emptying recycle bin, 121
- enabling
  - copyright display, 95
  - running configuration automatic save, 114
- encrypting configuration file, 111
- entering
  - commands, 5
  - system view, 3
- errors (CLI), 8
- establishing
  - FTP connection, 127
  - IPv4 FTP connection, 128
  - IPv6 FTP connection, 128
- exception handling configuration, 98
- executing configuration file, 159
- exiting current view, 3
- factory default configuration, 109
- file
  - activating patches, 149
  - ACTIVE patch state, 146
  - backing up startup configuration file, 115
  - checking NAND memory files, 123
  - configuration file content, 110
  - configuration file format, 110
  - configuration file management, 109
  - configuring the patch file location, 148
  - confirming running patches, 149
  - copying, 120
  - DEACTIVE patch state, 146
  - deleting, 121
  - deleting patches, 150
  - deleting startup configuration file, 116
  - displaying contents, 120
  - displaying information, 120
  - emptying recycle bin, 121
  - enabling running configuration automatic save, 114
  - executing configuration file, 159
  - IDLE patch state, 145
  - loading patch file, 149
  - management, 118, 120
  - moving, 120
  - name format, 118
  - one-step patch installation, 147
  - operating FTP server files, 129
  - patch file, 144
  - patch package file, 144
  - patch status, 144
  - performing batch operations, 121
  - renaming, 120
  - restoring from recycle bin, 121
  - restoring startup configuration file, 116
  - running configuration manual save, 114
  - RUNNING patch state, 146
  - setting configuration rollback, 115
  - specifying startup configuration file, 115
  - step-by-step patch installation, 148
  - step-by-step patch uninstallation, 150
  - stopping running patches, 150
  - types (automatic configuration), 157
- file transfer protocol. *See* FTP
- filtering output information, 10
- format
  - configuration file, 110

- filename, 118
- FTP
  - client configuration, 131
  - configuration, 126
  - configuring client, 127
  - configuring server, 133
  - configuring server authentication, 133
  - configuring server authorization, 133
  - debugging connection, 130
  - displaying, 136
  - establishing connection, 127
  - establishing IPv4 connection, 128
  - establishing IPv6 connection, 128
  - maintaining connection, 130
  - managing server directories, 129
  - operating server files, 129
  - server configuration, 134
  - terminating connection, 131
  - TFTP. *See* TFTP
  - using another username for server login, 130
- history
  - accessing history commands, 8
  - setting history buffer size, 9
  - using command history, 8
- hotfix
  - ACTIVE patch state, 146
  - basic concepts, 144
  - common patch, 144
  - DEACTIVE patch state, 146
  - IDLE patch state, 145
  - incremental patch, 144
  - patch file, 144
  - patch package file, 144
  - patch status, 144
  - RUNNING patch state, 146
  - temporary patch, 144
  - upgrading software, 144
- hotkey configuration, 6
- HP
  - customer support and resources, 160
  - displaying licenses, 141
  - document conventions, 161
  - documents and manuals, 160
  - icons used, 161
  - license management, 141
  - maintaining licenses, 141
  - registering device software, 141
  - subscription service, 160
  - support contact information, 160
  - symbols used, 161
  - websites, 160
- HTTP login, 73, 77
- HTTPS login, 75, 78
- icons, 161
- IDLE patch state, 145
- incremental patch (hotfix), 144
- installing
  - patch (one-step installation), 147
  - patch (step-by-step installation), 148
  - software upgrade by hotfix installation, 144
  - uninstalling patch (step-by-step), 150
- interface
  - absolute numbering, 23
  - clearing, 105
  - configuring user privilege level under a user interface, 14, 15
  - numbering user interfaces, 23
  - relative numbering, 23
  - user interface overview, 22
- IP
  - configuring source and destination IP-based Telnet login control, 86

- configuring source IP-based Telnet login control, 85
- DHCP address acquisition process, 156
- establishing IPv6 FTP connection, 128
- establishing IPv4 FTP connection, 128
- obtaining address with DHCP, 156
- job
  - modular scheduling, 100
  - non-modular scheduling, 100
  - scheduling, 99, 101
- keyword
  - configuring keyword alias, 6
  - incomplete, 5
- license management, 141
- loading patch file, 149
- logging in
  - AUX port, 48
  - AUX port login authentication modes, 48
  - CLI login, 24
  - configuring HTTP login, 73, 77
  - configuring HTTPS login, 75, 78
  - configuring NMS login, 81
  - console login authentication modes, 27
  - console port, 24
  - methods, 21
  - modem, 59
  - modem login authentication modes, 63
  - NMS login, 81
  - SSH, 44
  - SSH client configuration, 47
  - SSH server configuration, 45
  - Telnet, 36
  - Telnet authentication modes, 36
  - user login control, 85
  - web login, 73
- logging off online web users, 90
- login method, 21

- MAC
  - configuring source IP-based NMS login control, 88, 89
  - configuring source MAC-based Telnet login control, 87
- maintaining
  - CLI login, 71
  - FTP connection, 130
  - licenses, 141
  - NAND flash memory, 123
- managing
  - configuring file, 109
  - directories, 119
  - files, 118, 120
  - FTP server directories, 129
  - storage media space, 122
- manuals, 160
- message (banner), 96
- method (software upgrade), 142
- mode
  - AUX port login authentication, 48
  - banner message input, 96
  - configuring interface card working mode, 104
  - console login authentication, 27
  - FTP configuration, 126
  - modem login authentication, 63
  - setting authentication mode for user privilege level switch, 16
  - setting prompt modes, 124
  - Telnet authentication, 36
  - TFTP request sending, 158
- modem
  - configuring login AAA authentication, 66
  - configuring login none authentication, 64
  - configuring login optional common settings, 68
  - configuring login password authentication, 65
  - login, 59



- login authentication modes, 63
- modifying command level, 19
- modular job scheduling, 100
- monitored interfaces (NMS), 103
- mounting storage media, 122
- moving file, 120
- multi-screen display, 9, 10
- naming storage media, 118
- NAND flash memory, 123
- network management
  - automatic device configuration, 154
  - CLI configuration, 1
  - device management, 92
  - FTP configuration, 126
  - hotfix software upgrade configuration, 152
  - license management, 141
  - software upgrade configuration, 142, 150
  - TFTP configuration, 137
- NMS
  - configuring login, 81
  - configuring monitored interfaces, 103
  - configuring source IP-based user login control, 88, 89
  - login, 81
- non-modular job scheduling, 100
- numbering
  - absolute numbering, 23
  - relative numbering, 23
  - user interfaces, 23
- obtaining
  - configuration file (automatic configuration, 158
  - configuration file from TFTP server, 157
- online help, 4
- operating
  - FTP server files, 129
- optional common settings
  - configuring AUX port login, 54
  - configuring modem login, 68
  - console, 33
  - Telnet login (VTY user interfaces), 42
- output (filtering information), 10
- package (patch), 144
- parameter (saving current running configuration), 113
- password
  - configuring console login password authentication, 29
  - configuring modem login password authentication, 65
  - configuring Telnet login password authentication, 38
- patch
  - activating patches, 149
  - ACTIVE state, 146
  - common, 144
  - configuring file location, 148
  - confirming running patches, 149
  - DEACTIVE state, 146
  - defined, 144
  - deleting patches, 150
  - file, 144
  - IDLE state, 145
  - incremental, 144
  - loading patch file, 149
  - one-step installation, 147
  - package file, 144
  - RUNNING state, 146
  - status, 144
  - step-by-step installation, 148
  - step-by-step uninstallation, 150
  - stopping running patches, 150
  - temporary, 144
- performing
  - batch operations, 121

- storage media operations, 122
- port
  - AUX port login authentication, 48
  - configuring AUX port login, 48
  - logging in through console port, 24
- privilege
  - configuring user level, 12, 13
  - modifying command level, 19
  - setting authentication mode for user level switch), 16
  - switching user level, 16, 18
- procedure
  - accessing history commands, 8
  - activating patches, 149
  - AUX port login, 57
  - backing up startup configuration file, 115
  - changing current working directory, 119
  - changing system time, 92
  - checking NAND memory files, 123
  - clearing unused interface indexes, 105
  - configuring AUX port login, 48
  - configuring AUX port login AAA authentication, 51
  - configuring AUX port login none authentication, 49
  - configuring AUX port login optional common settings, 54
  - configuring AUX port login password authentication, 50
  - configuring banner, 96
  - configuring card temperature threshold, 103
  - configuring CLI hotkeys, 6
  - configuring command aliases, 6
  - configuring console login none authentication, 28
  - configuring console login optional common settings, 33
  - configuring console login password authentication, 29
  - configuring console login scheme authentication, 30
  - configuring detection interval, 102
  - configuring device login as Telnet client, 44
  - configuring device name, 92
  - configuring exception handling, 98
  - configuring FTP, 126
  - configuring FTP client, 127, 131
  - configuring FTP server, 133, 134
  - configuring FTP server authentication, 133
  - configuring FTP server authorization, 133
  - configuring hotfix software upgrade, 152
  - configuring HTTP login, 73, 77
  - configuring HTTPS login, 75, 78
  - configuring interface card working mode, 104
  - configuring max number concurrent users, 97
  - configuring modem login, 59
  - configuring modem login AAA authentication, 66
  - configuring modem login none authentication, 64
  - configuring modem login optional common settings, 68
  - configuring modem login password authentication, 65
  - configuring NMS login, 81
  - configuring NMS monitored interfaces, 103
  - configuring parameters (saving current running configuration), 113
  - configuring patch file location, 148
  - configuring source and destination IP-based Telnet user login control, 86
  - configuring source IP-based NMS user login control, 88, 89
  - configuring source IP-based Telnet user login control, 85
  - configuring source IP-based web user login control, 90, 91
  - configuring source MAC-based Telnet user login control, 87
  - configuring SSH client, 47
  - configuring SSH login, 44
  - configuring SSH server, 45

- configuring Telnet login, 36
- configuring Telnet login none authentication, 37
- configuring Telnet login optional common settings (VTY user interfaces), 42
- configuring Telnet login password authentication, 38
- configuring Telnet login scheme authentication, 39
- configuring Telnet user login control, 85
- configuring TFTP client, 137, 139
- configuring user command levels, 12
- configuring user privilege level, 13
- configuring user privilege level under a user interface, 14, 15
- configuring user privilege level using AAA authentication, 13, 14
- configuring user privilege levels, 12
- confirming running patches, 149
- copying file, 120
- creating directory, 119
- debugging FTP connection, 130
- deleting file, 121
- deleting patches, 150
- deleting startup configuration file, 116
- diagnosing transceiver modules, 106
- disabling multi-screen display, 10
- displaying bad NAND memory blocks, 123
- displaying CLI, 20
- displaying CLI login, 71
- displaying configuration file, 117
- displaying current working directory, 119
- displaying device management, 107
- displaying directory information, 119
- displaying file contents, 120
- displaying file information, 120
- displaying FTP, 136
- displaying licenses, 141
- displaying software upgrade, 150
- displaying TFTP client, 139
- displaying the NAND flash memory, 123
- displaying web login, 76
- editing command lines, 5
- emptying recycle bin, 121
- enabling copyright display, 95
- enabling running configuration automatic save, 114
- encrypting configuration file, 111
- entering commands, 5
- establishing FTP connection, 127
- establishing IPv4 FTP connection, 128
- establishing IPv6FTP connection, 128
- installing patch (one-step), 147
- installing patch (step-by-step), 148
- job scheduling, 99, 101
- loading patch file, 149
- logging in through console port, 24
- logging off online web users, 90
- maintaining CLI login, 71
- maintaining FTP connection, 130
- maintaining licenses, 141
- maintaining the NAND flash memory, 123
- managing directories, 119
- managing files, 118, 120
- managing FTP server directories, 129
- managing storage media space, 122
- manually saving the running configuration, 114
- modem login, 60
- modifying command level, 19
- mounting storage media, 122
- moving file, 120
- operating FTP server files, 129
- performing batch operations, 121
- performing storage media operations, 122
- rebooting router, 98
- rebooting router at the CLI, 98
- redisplaying unsubmitted commands, 7

- removing directory, 119
- renaming file, 120
- repairing bad NAND memory blocks, 123
- restoring file from recycle bin, 121
- restoring startup configuration file, 116
- saving running configuration, 110
- scheduling device reboot, 98
- scheduling modular job, 100
- scheduling non-modular job, 100
- setting authentication mode (user privilege level switch), 16
- setting configuration rollback, 112, 115
- setting history buffer size, 9
- setting prompt modes, 124
- specifying startup configuration file, 115
- stopping running patches, 150
- switching user privilege level, 16, 18
- terminating FTP connection, 131
- uninstalling patch (step-by-step), 150
- unmounting storage media, 122
- upgrading boot file through system reboot, 143
- upgrading BootWare through system reboot, 143
- upgrading software through system reboot, 143
- upgrading software upgrade by installing hotfixes, 144
- using another username for FTP server login, 130
- verifying transceiver modules, 106

prompt modes, 124

rebooting

- boot file upgrade through system reboot, 143
- BootWare upgrade through system reboot, 143
- router, 98
- router at the CLI, 98
- scheduling, 98
- software upgrade through system reboot, 143

recycle bin

- emptying, 121
- restoring file, 121

redisplaying unsubmitted commands, 7

relative numbering, 23

removing directory, 119

renaming file, 120

repairing bad NAND memory blocks, 123

request sending mode (TFTP), 158

restoring

- file from recycle bin, 121
- startup configuration file, 116

returning to user view, 4

rollback

- setting configuration, 115
- setting configuration rollback, 112

router

- rebooting, 98
- rebooting at the CLI, 98
- scheduling reboot, 98

rule (storage media naming), 118

running configuration, 109

RUNNING patch state, 146

saving

- configuring parameters (current running configuration), 113
- current configuration, 19
- running configuration, 110
- running configuration manual save, 114

scheduling

- device reboot, 98
- job, 99, 101
- modular job, 100
- non-modular job, 100

scheme

- configuring console login scheme authentication, 30
- configuring modem login AAA authentication, 66

- configuring Telnet login password authentication, 39
- security (encrypting configuration file), 111
- server
  - configuring authentication (FTP), 133
  - configuring authorization (FTP), 133
  - configuring FTP server, 133
  - configuring SSH client, 47
  - configuring SSH server, 45
  - DHCP address pool selection principles, 156
  - FTP configuration, 134
  - managing FTP directories, 129
  - obtaining configuration file from TFTP server, 157
  - operating FTP files, 129
  - using another username for FTP login, 130
- setting
  - authentication mode (user privilege level switch), 16
  - configuration rollback, 112, 115
  - history buffer size, 9
  - prompt modes, 124
- software exception handling, 98
- software upgrade
  - boot file upgrade through system reboot, 143
  - BootWare upgrade through system reboot, 143
  - configuration, 142, 150
  - displaying, 150
  - hotfix configuration, 152
  - hotfix installation, 144
  - methods, 142
  - system reboot, 143
- specifying startup configuration file, 115
- SSH
  - configuring client, 47
  - configuring server, 45
  - logging in, 44
- startup
  - configuration, 109

- configuration file, 110, 115
- deleting startup configuration file, 116
- restoring startup configuration file, 116
- status
  - ACTIVE patch state, 146
  - DEACTIVE patch state, 146
  - IDLE patch state, 145
  - patch, 144
  - RUNNING patch state, 146
- stopping running patches, 150
- storage media
  - managing space, 122
  - mounting, 122
  - naming rules, 118
  - performing operations, 122
  - unmounting, 122
- subscription service, 160
- support and other resources, 160
- switching user privilege level, 16, 18
- symbols, 161
- system administration
  - changing system time, 92
  - configuring banner, 96
  - configuring device name, 92
  - device management, 92
  - enabling copyright display, 95
- Telnet
  - configuring device login as Telnet client, 44
  - configuring login none authentication, 37
  - configuring login password authentication, 38
  - configuring login scheme authentication, 39
  - configuring optional common settings (VTY user interfaces), 42
  - configuring source and destination IP-based user login control, 86
  - configuring source IP-based user login control, 85

- configuring source MAC-based user login control, 87
- configuring user login control, 85
- logging in, 36
- login authentication modes, 36
- temperature threshold, 103
- temporary patch (hotfix), 144
- terminating FTP connection, 131
- TFTP
  - automatic device configuration, 154
  - configuration, 137
  - configuring client, 137, 139
  - displaying client, 139
  - obtaining configuration file from server, 157
  - request sending mode, 158
- time
  - changing system time, 92
  - configuring detection interval, 102
- transceiver
  - diagnosing modules, 106
  - verifying modules, 106
- trivial file transfer protocol. *See* TFTP
- type
  - automatic configuration files, 157
  - banner, 96
  - device configuration, 109
  - factory default configuration, 109
  - running configuration, 109
  - startup configuration, 109
- UDP (TFTP configuration), 137
- undo command form, 2
- uninstalling patch (step-by-step), 150
- unmounting storage media, 122
- upgrading
  - boot file upgrade through system reboot, 143
  - BootWare upgrade through system reboot, 143
  - software, 142, 150
  - software upgrade by installing hotfixes, 144
  - software upgrade methods, 142
  - software upgrade through system reboot, 143
- user
  - configuring command levels, 12
  - configuring max number concurrent users, 97
  - configuring privilege level, 13
  - configuring privilege level under a user interface, 14, 15
  - configuring privilege level using AAA authentication, 13, 14
  - configuring privilege levels, 12
  - configuring source and destination IP-based Telnet login control, 86
  - configuring source IP-based NMS login control, 88, 89
  - configuring source IP-based Telnet login control, 85
  - configuring source IP-based web login control, 90, 91
  - configuring source MAC-based Telnet login control, 87
  - configuring Telnet login control, 85
  - interface overview, 22
  - logging off online web users, 90
  - login control, 85
  - numbering user interfaces, 23
  - setting authentication mode for privilege level switch), 16
  - switching privilege level, 16, 18
- using
  - command history, 8
  - DHCP to obtain an IP address, 156
  - DHCP to obtain configuration information, 156
  - FTP server login with different username, 130
  - online help, 4
- verifying transceiver modules, 106
- VTY user interface (Telnet login), 42

web

configuring HTTP login, 73, 77

configuring HTTPS login, 75, 78

configuring source IP-based user login control, 90,  
91

displaying web login, 76

logging off online users, 90

login, 73

websites, 160