

HP 5920 & 5900 Switch Series

Fundamentals

Configuration Guide

Part number: 5998-2891

Software version: Release2207

Document version: 6W100-20121130



Legal and notice information

© Copyright 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

Using the CLI	1
CLI views	1
Entering system view from user view	2
Returning to the upper-level view from any view	2
Returning to user view	2
Accessing the CLI online help	2
Using the undo form of a command	3
Entering a command	3
Editing a command line	3
Entering a string or text type value for an argument	4
Abbreviating commands	4
Configuring and using command keyword aliases	4
Configuring and using command hotkeys	5
Enabling redisplaying entered-but-not-submitted commands	6
Understanding command-line error messages	6
Using the command history function	7
Controlling the CLI output	8
Pausing between screens of output	8
Numbering each output line from a display command	9
Filtering the output from a display command	9
Saving the output from a display command to a file	11
Viewing and managing the output from a display command effectively	13
Saving the running configuration	13
Login overview	14
Logging in through the console port for the first device access	15
Logging in to the CLI	18
CLI overview	18
CLI user interfaces	18
Login authentication modes	19
User roles	19
Logging in through the console port locally	19
Configuring none authentication for console login	20
Configuring password authentication for console login	20
Configuring scheme authentication for console login	21
Configuring common AUX user interface settings	21
Logging in through Telnet	22
Configuring Telnet login on the device	23
Using the device to log in to a Telnet server	27
Logging in through SSH	28
Configuring SSH login on the device	28
Using the device to log in to an SSH server	29
Displaying and maintaining CLI login	29
Accessing the device through SNMP	31
Configuring SNMPv3 access	31
Configuring SNMPv1 or SNMPv2c access	32

Controlling user access.....	33
Controlling Telnet/SSH logins.....	33
Configuration procedures.....	33
Configuration example.....	33
Controlling SNMP access.....	34
Configuration procedure.....	34
Configuration example.....	35
Configuring command authorization.....	36
Configuration procedure.....	36
Configuring command accounting.....	36
Configuration procedure.....	37
Configuring RBAC.....	38
Overview.....	38
Permission assignment.....	38
Assigning user roles.....	40
Configuration task list.....	40
Creating user roles.....	40
Configuring user role rules.....	41
Configuring feature groups.....	42
Changing resource access policies.....	42
Changing the interface policy of a user role.....	42
Changing the VLAN policy of a user role.....	43
Changing the VPN instance policy of a user role.....	43
Assigning user roles.....	43
Enabling the default user role function.....	44
Assigning user roles to remote AAA authentication users.....	44
Assigning user roles to local AAA authentication users.....	44
Assigning user roles to non-AAA authentication users on user interfaces.....	45
Configuring user role switching.....	45
Configuration guidelines.....	45
Configuring user role switching authentication.....	46
Switching the user role.....	46
Displaying RBAC settings.....	47
RBAC configuration example for local AAA authentication users.....	47
Network requirements.....	47
Configuration procedure.....	47
Verifying the configuration.....	48
RBAC configuration example for RADIUS authentication users.....	49
Network requirements.....	49
Configuration procedure.....	50
Verifying the configuration.....	51
RBAC configuration example for HWTACACS authentication users.....	52
Network requirements.....	52
Configuration procedure.....	52
Verifying the configuration.....	54
Troubleshooting RBAC.....	55
Local users have more access permissions than intended.....	55
Login attempts by RADIUS users always fail.....	56
Configuring FTP.....	57
Using the device as an FTP server.....	57
Configuring basic parameters.....	57
Configuring authentication and authorization.....	58
Manually releasing FTP connections.....	58

Displaying and maintaining the FTP server	58
FTP server configuration example	59
Using the device as an FTP client	60
Establishing an FTP connection	60
Managing directories on the FTP server	61
Working with files on the FTP server	61
Switching to another user account	63
Maintaining and troubleshooting the FTP connection	63
Terminating the FTP connection	63
Displaying command help information	63
Displaying and maintaining FTP client	64
FTP client configuration example	64
Configuring TFTP	66
Configuring the device as an IPv4 TFTP client	66
Configuring the device as an IPv6 TFTP client	66
Managing the file system	68
File name formats	68
Managing files	69
Displaying file information	69
Displaying the contents of a text file	69
Renaming a file	69
Copying a file	69
Moving a file	70
Compressing/decompressing a file	70
Deleting/restoring a file	70
Deleting files from the recycle bin	70
Managing directories	71
Displaying the current working directory	71
Changing the current working directory	71
Creating a directory	71
Removing a directory	71
Managing storage media	72
Repairing a storage medium	72
Formatting a storage medium	72
Setting the operation mode for files and folders	72
Managing configuration files	73
Overview	73
Configuration types	73
Next-startup configuration file redundancy	73
Configuration file formats	74
Startup configuration file selection	74
Configuration file content organization and format	74
Enabling configuration encryption	75
Saving the running configuration	75
Configuring configuration rollback	76
Configuration task list	76
Configuring configuration archive parameters	76
Enabling automatic configuration archiving	77
Manually archiving the running configuration	78
Performing a configuration rollback	78
Specifying a next-startup configuration file	79
Backing up the main next-startup configuration file to a TFTP server	79
Restoring the main next-startup configuration file from a TFTP server	80

Deleting a next-startup configuration file	80
Displaying and maintaining configuration files	81
Upgrading software	82
Overview	82
Software types	82
Software file naming conventions	82
Comware image redundancy and loading procedure	82
System startup process	83
Upgrade methods	84
Non-ISSU upgrade procedure summary	85
Preparing for the upgrade	85
Preloading the Boot ROM image to Boot ROM	85
Specifying the startup image file and completing the upgrade	86
Displaying and maintaining software image settings	88
Non-ISSU software upgrade example	88
Network requirements	88
Configuration procedure	88
ISSU overview	90
ISSU methods	90
ISSU methods for a compatible version	90
ISSU method for an incompatible version	91
ISSU command series	91
ISSU prerequisites	92
ISSU restrictions and guidelines	92
Performing an ISSU by using issu series commands	94
Performing an ISSU for a multi-member IRF fabric	94
Performing an ISSU for a single-member IRF fabric	95
Displaying and maintaining ISSU	97
Performing an ISSU by using install series commands	98
Obtaining the software images issued in an IPE file	98
Installing or upgrading software images	98
Uninstalling patch images	99
Rolling back the software configuration	99
Aborting a software activate/deactivate operation	100
Verifying the software change confirmation status and software image integrity and consistency	100
Removing inactive software images	100
Displaying and maintaining ISSU	101
Managing the device	102
Configuring the device name	102
Setting the system time	102
Enabling displaying the copyright statement	103
Configuring banners	103
Banner types	103
Banner input modes	103
Configuration procedure	104
Setting the operating mode	105
Rebooting the device	105
Configuration guidelines	105
Rebooting devices immediately at the CLI	106
Scheduling a device reboot	106
Scheduling a task	106
Configuration guidelines	106

Configuration procedure	106
Schedule configuration example	108
Configuring the preferred airflow direction	111
Setting the port status detection timer	112
Setting memory usage thresholds	112
Configuring the temperature alarm thresholds	114
Disabling all USB interfaces	115
Verifying and diagnosing transceiver modules	115
Verifying transceiver modules	115
Diagnosing transceiver modules	116
Displaying and maintaining device management configuration	116
Using the emergency shell	118
Managing the file system	118
Obtaining a system image from an FTP/TFTP server	119
Configuring the management Ethernet interface	119
Checking the connectivity to a server	120
Accessing the server	120
Loading the system image	121
Rebooting the device	121
Displaying device information in emergency shell mode	121
Emergency shell usage example	122
Network requirements	122
Usage procedure	122
Automatic configuration	125
Understanding automatic configuration	125
Overall automatic configuration process	125
Automatic-configuration parameter acquisition process	127
Configuration file acquisition process	128
Deploying and configuring servers for automatic configuration	129
DHCP server configuration guidelines	130
TFTP server configuration guidelines	130
Configuring Tcl	131
Restrictions and benefits	131
Entering Tcl configuration view from user view	131
Returning from Tcl configuration view to user view	131
Support and other resources	132
Contacting HP	132
Subscription service	132
Related information	132
Documents	132
Websites	132
Conventions	133
Index	135

Using the CLI

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

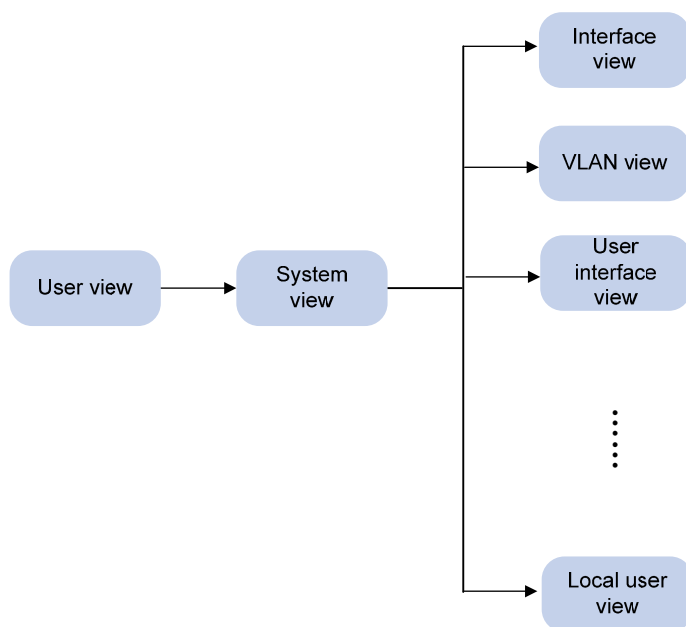
You can log in to the CLI in a variety of ways. For example, you can log in through the console port, or by using Telnet or SSH. For more information about login methods, see "Login overview."

CLI views

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

CLI views are hierarchically organized, as shown in Figure 1. Each view has a unique prompt, from which you can identify where you are and what you can do. For example, the prompt `[Sysname-vlan100]` shows that you are in VLAN 100 view and can configure attributes for that VLAN.

Figure 1 CLI views



You are placed in user view immediately after you are logged in to the CLI. The user view prompt is `<Device-name>`, where *Device-name* indicates the device name, defaults to **Sysname**, and can be changed by using the **sysname** command. In user view, you can perform basic operations including display, debug, file management, FTP, Telnet, clock setting, and reboot.

From user view, you can enter system view to configure global settings (such as the daylight saving time, banners, and hotkeys) and some functions. The system view prompt is `[Device-name]`.

From system view, you can enter different function views. For example, you can enter interface view to configure interface parameters, enter VLAN view to add ports to the specific VLAN, enter user interface view to configure login user attributes, or create a local user and enter local user view to configure attributes for the local user. A function view might have child views. For example, in BGP view, there are IPv4 unicast instance view and BGP-VPN IPv4 unicast instance view.

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

Entering system view from user view

Task	Command
Enter system view.	system-view

Returning to the upper-level view from any view

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

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

Returning to user view

You can return directly to user view from any other view by using the **return** command or pressing **Ctrl+Z**, instead of using the **quit** command multiple times.

To return directly to user view from any other view:

Task	Command
Return directly to user view.	return

Accessing the CLI online help

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

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

- Enter a question mark at a view prompt to display the first keyword of every command available in the view. For example:

```
<Sysname> ?
```

```
User view commands:
```

```
archive          Archive configuration
backup           Backup the startup configuration file to a TFTP server
boot-loader     Set boot loader
```

```
...
```

- Enter a space and a question mark after a command keyword to display all available, subsequent keywords and arguments.
 - If the question mark is in the place of a keyword, the CLI displays all possible keywords, each with a brief description. For example:

```
<Sysname> terminal ?
```

```
logging  Display logs on the current terminal
monitor  Enable to display logs on the current terminal
```

- If the question mark is in the place of an argument, the CLI displays the description of the argument. For example:

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

<1-4094> is the value range for the argument. **<cr>** indicates that the command is complete and you can press **Enter** to execute the command.

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

```
<Sysname> f?
  fixdisk
  format
  free
  ftp
<Sysname> display ftp?
  ftp
  ftp-server
  ftp-user
```

Using the undo form of a command

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

Entering a command

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

Editing a command line

To edit a command line, use the keys listed in [Table 1](#) or the hotkeys listed in [Table 2](#). When you are finished, you can press **Enter** to execute the command.

Table 1 Command line editing keys

Keys	Function
Common keys	If the edit buffer is not full, pressing a common key inserts a character at the position of the cursor and moves the cursor to the right. The edit buffer can store up to 511 characters. Unless the buffer is full, all common characters that you enter before pressing Enter are saved in the edit buffer.
Backspace	Deletes the character to the left of the cursor and moves the cursor back one character.
Left arrow key (←)	Moves the cursor one character to the left.

Keys	Function
Right arrow key (→)	Moves the cursor one character to the right.
Up arrow key (↑)	Gets the previous history command.
Down arrow key (↓)	Gets the next history command.
Tab	<p>If you press Tab after entering part of a keyword, the system automatically completes the keyword:</p> <ul style="list-style-type: none"> • If a unique match is found, the system substitutes the complete keyword for the incomplete one and displays what you entered in the next line. • If there is more than one match, press Tab multiple times to pick the keyword you want to enter. • If there is no match, the system does not modify what you entered but displays it again in the next line.

Entering a string or text type value for an argument

Generally, a string type argument value can contain any printable character (in the ASCII code range of 32 to 126) other than the question mark (?), quotation mark ("), backward slash (\), and space, and a text type argument value can contain any printable character other than the question mark. However, a specific argument might have more requirements. For more information about the specific requirements for an argument, see the relevant command reference.

Abbreviating commands

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

You can also press **Tab** to complete an incomplete keyword.

Configuring and using command keyword aliases

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

Usage guidelines

- After you successfully execute a command by using a keyword alias, the system saves the keyword, instead of its alias, to the running configuration.
- If a string you entered for a command partially matches an alias and a keyword, the command indicated by the alias is executed. To execute the command indicated by the keyword, enter the complete keyword.
- If a string you entered for a command partially matches multiple aliases, the system displays an error message.
- If you enter a string that partially matches an alias and a keyword and press **Tab**, the keyword indicated by the alias is displayed. Pressing **Tab** again displays the keyword.

Configuration procedure

To configure a command keyword alias:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the command keyword alias function.	command-alias enable	By default, the command keyword alias function is disabled.
3. Configure a command keyword alias.	command-alias mapping <i>cmdkey alias</i>	By default, no command keyword alias is configured. You must enter the <i>cmdkey</i> and <i>alias</i> arguments in their complete form.
4. (Optional.) Display command keyword alias information.	display command-alias	This command is available in any view.

Configuring and using command hotkeys

To facilitate CLI operation, the system defines the hotkeys shown in Table 2 and provides five configurable command hotkeys. Pressing a command hotkey is the same as entering a command.

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

To configure a command hotkey:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Assign a command to a hotkey.	hotkey { ctrl_g ctrl_l ctrl_o ctrl_t ctrl_u } command	By default: <ul style="list-style-type: none">• Ctrl+G is assigned the display current-configuration command.• Ctrl+L is assigned the display ip routing-table command.• Ctrl+O is assigned the undo debugging all command.• No command is assigned to Ctrl+T or Ctrl+U.
3. (Optional.) Display hotkeys.	display hotkey	Available in any view.

Table 2 System-reserved hotkeys

Hotkey	Function
Ctrl+A	Moves the cursor to the beginning of a line.
Ctrl+B	Moves the cursor one character to the left.
Ctrl+C	Stops the current command.
Ctrl+D	Deletes the character at the cursor.
Ctrl+E	Moves the cursor to the end of a line.

Hotkey	Function
Ctrl+F	Moves the cursor one character to the right.
Ctrl+H	Deletes the character to the left of the cursor.
Ctrl+K	Aborts the connection request.
Ctrl+R	Redisplays the current line.
Ctrl+V	Pastes text from the clipboard.
Ctrl+W	Deletes the word to the left of the cursor.
Ctrl+X	Deletes all characters to the left of the cursor.
Ctrl+Y	Deletes all characters to the right of the cursor.
Ctrl+Z	Returns to user view.
Ctrl+]	Terminates the current connection.
Esc+B	Moves the cursor back one word.
Esc+D	Deletes all characters from the cursor to the end of the word.
Esc+F	Moves the cursor forward one word.
Esc+N	Moves the cursor down one line. This hotkey is available before you press Enter .
Esc+P	Moves the cursor up one line. This hotkey is available before you press Enter .
Esc+<	Moves the cursor to the beginning of the clipboard.
Esc+>	Moves the cursor to the ending of the clipboard.

Enabling redisplaying entered-but-not-submitted commands

After you enable redisplaying entered-but-not-submitted commands, when your input is interrupted by system information output, the system redisplay your input after finishing the output so you can continue entering the command line.

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

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

Understanding command-line error messages

After you press **Enter** to submit a command, the command line interpreter first examines the command syntax. If the command passes syntax check, the CLI executes the command. If not, the CLI displays an error message.

Table 3 Common command-line error messages

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

Using the command history function

The system automatically saves commands successfully executed by a login user to two command history buffers: the command history buffer for the user interface and the command history buffer for all user interfaces. Table 4 compares these two types of command history buffers.

Table 4 Comparison between the two types of command history buffers

Item	Command history buffer for a user interface	Command history buffer for all user interfaces
What kind of commands are stored in the buffer?	Commands successfully executed by the current user of the user interface.	Commands successfully executed by all login users.
Cleared when the user logs out?	Yes.	No.
How to view buffered commands?	Use the display history-command command.	Use the display history-command all command.
How to call buffered commands?	<ul style="list-style-type: none"> In Windows 200x or Windows XP HyperTerminal or Telnet, use the up or down arrow key (↑ or ↓) to navigate to a command in the buffer and press Enter to execute the command again. In Windows 9x HyperTerminal, use Ctrl+P and Ctrl+N to do so. 	You cannot call buffered commands.
How to set the buffer size?	Use the history-command max-size size-value command in user interface view to set the buffer size. By default, the buffer can store up to 10 commands.	You cannot set the buffer size. By default, the buffer can store up to 1024 commands.
How to disable the buffer?	Setting the buffer size to 0 disables the buffer.	You cannot disable the buffer.

The system follows these rules when buffering commands:

- Buffering a command in the exact format in which the command was entered. For example, if you enter an incomplete command, the buffered command is also incomplete. If you enter a command with a command keyword alias, the buffered command also uses the alias.
- If you enter a command in the same format multiple times in succession, the system buffers the command only once. If you enter a command multiple times in different formats, the system buffers each command format. For example, **display cu** and **display current-configuration** are buffered as two entries but successive repetitions of **display cu** create only one entry.
- To buffer a new command when a buffer is full, the system deletes the oldest command entry in the buffer.

Controlling the CLI output

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

Pausing between screens of output

If the output being displayed is more than will fit on one screen, the system automatically pauses after displaying a screen. You can use the keys described in "Output controlling keys" to display more information or stop the display.

By default, up to 24 lines can be displayed on a screen. You can change the maximum number of lines that can be displayed on a screen by using the **screen-length** *screen-length* command. For more information about this command, see *Fundamentals Command Reference*.

You can also disable pausing between screens of output for the current session. Then, all output is displayed at one time and the screen is refreshed continuously until the last screen is displayed.

Output controlling keys

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

Disabling pausing between screens of output

To disable pausing between screens of output, execute the following command in user view:

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

Numbering each output line from a display command

You can use the | **by-linenum** option to prefix each **display** command output line with a number for easy identification.

To number each output line from a **display** command:

Task	Command
Number each output line from a display command.	display <i>command</i> by-linenum

For example:

```
# Display information about VLAN 999, numbering each output line.
```

```
<Sysname> display vlan 999 | by-linenum
```

```
1:   VLAN ID: 999
2:   VLAN type: Static
3:   Route interface: Configured
4:   IP address: 192.168.2.1
5:   Subnet mask: 255.255.255.0
6:   Description: For LAN Access
7:   Name: VLAN 0999
8:   Tagged ports:   None
9:   Untagged ports:
10:  Ten-GigabitEthernet 1/0/1
```

Filtering the output from a display command

You can use the | { **begin** | **exclude** | **include** } *regular-expression* option to filter the **display** command output:

- **begin**—Displays the first line matching the specified regular expression and all subsequent lines.
- **exclude**—Displays all lines not matching the specified regular expression.
- **include**—Displays all lines matching the specified regular expression.
- *regular-expression*—A case-sensitive string of 1 to 256 characters, which can contain the special characters described in [Table 5](#).

Table 5 Special characters supported in a regular expression

Characters	Meaning	Examples
^	Matches the beginning of a line.	"^user" matches all lines beginning with "user". A line beginning with "Auser" is not matched.
\$	Matches the end of a line.	"user\$" matches all lines ending with "user". A line ending with "userA" is not matched.
.	Matches any single character.	".s" matches "as" and "bs".
*	Matches the preceding character or string zero, one, or multiple times.	"zo*" matches "z" and "zoo", and "(zo)*" matches "zo" and "zozo".
+	Matches the preceding character or string one or multiple times.	"zo+" matches "zo" and "zoo", but not "z".

Characters	Meaning	Examples
	Matches the preceding or succeeding string.	"def int" matches a string containing "def" or "int".
()	Matches the string in the parentheses, usually used together with the plus sign (+) or asterisk (*).	"(123A)" matches "123A". "408(12)+" matches "40812" and "408121212", but not "408".
\N	Matches the preceding strings in parentheses, with the <i>N</i> th string repeated once.	"(string)\1" matches a string containing "stringstring". "(string1)(string2)\2" matches a string containing "string1string2string2". "(string1)(string2)\1\2" matches a string containing " string1string2string1string2".
[]	Matches a single character in the brackets.	"[16A]" matches a string containing 1, 6, or A; "[1-36A]" matches a string containing 1, 2, 3, 6, or A (- is a hyphen). To match the character "]", put it immediately after "[", for example, []abc]. There is no such limit on "[".
[^]	Matches a single character that is not in the brackets.	"[^16A]" matches a string that contains at least one character other than 1, 6, or A, such as "abc". A match can also contain 1, 6, or A (such as "m16"), but it cannot contain these three characters only (such as 1, 16, or 16A).
{n}	Matches the preceding character <i>n</i> times. The number <i>n</i> must be a nonnegative integer.	"o{2}" matches "food", but not "Bob".
{n,}	Matches the preceding character <i>n</i> times or more. The number <i>n</i> must be a nonnegative integer.	"o{2,}" matches "foooooo", but not "Bob".
{n,m}	Matches the preceding character <i>n</i> to <i>m</i> times or more. The numbers <i>n</i> and <i>m</i> must be nonnegative integers and <i>n</i> cannot be greater than <i>m</i> .	"o{1,3}" matches "fod", "food", and "foooooo", but not "fd".
\<	Matches the beginning of a string. A string that contains the pattern following \< is also a match if the characters preceding the pattern are not digits, letters, or underscores.	"\<do" matches "domain" and "doa".
\>	Matches the end of a string. A string that contains the pattern preceding \> is also a match if the characters following the pattern are not digits, letters, or underscores.	"do\>" matches "undo" and "cdo".
\b	Same as [^A-Za-z0-9_], matches a character that is not a digit, letter, or underscore.	"\ba" matches "a", but not "2a" or "ba".
\B	Same as [A-Za-z0-9_], matches a digit, letter, or underscore.	"\Bt" matches "install", but not "big top".

Characters	Meaning	Examples
\w	Same as \B.	"v\w" matches "vlan" and "service".
\W	Same as \b.	"\Wa" matches "a", but not "2a" or "ba".
\	Escape character. If a special character listed in this table follows \, the specific meaning of the character is removed.	"\\" matches a string containing "\", "\\^" matches a string containing "^", and "\\b" matches a string containing "b".

For example:

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

```
<Sysname> display current-configuration | begin user-interface
user-interface aux 0
  user-role network-operator
#
user-interface vty 0 15
  authentication-mode scheme
  user-role network-operator
#
  ssh server enable
#
return
```

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

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

          Destinations : 12          Routes : 12

Destination/Mask    Proto  Pre  Cost           NextHop           Interface
2.2.2.0/24          OSPF   10   2              1.1.2.2           Ten-GigabitEthernet 1/0/2
```

Use **| include snmp** in the **display current-configuration** command to filter in entries that contain **snmp**.

```
<Sysname> display current-configuration | include snmp
snmp-agent
  snmp-agent community write private
  snmp-agent community read public
  snmp-agent sys-info version all
  snmp-agent target-host trap address udp-domain 192.168.1.26 params securityname public
```

Saving the output from a display command to a file

A **display** command shows certain configuration and operation information of the device. Its output might vary over time or with user configuration or operation. You can save the output to a file for future retrieval or troubleshooting.

Use one of the following methods to save the output from a **display** command:

- Save the output to a separate file. Use this method if you want to use one file for a single **display** command.

- Append the output to the end of a file. Use this method if you want to use one file for multiple **display** commands.

To save the output from a **display** command to a file, use one of the following commands in any view:

Task	Command
Save the output from a display command to a separate file.	display command > filename
Append the output from a display command to the end of a file.	display command >> filename

For example:

Save the VLAN 1 settings to a separate file named **vlan.txt**.

```
<Sysname> display vlan 1 > vlan.txt
```

Verify whether the VLAN 1 settings are saved to file **vlan.txt**.

```
<Sysname> more vlan.txt
```

```
VLAN ID: 1
VLAN type: Static
Route interface: Not configured
Description: VLAN 0001
Name: VLAN 0001
Tagged ports:   None
Untagged ports:
Ten-GigabitEthernet 1/0/2
```

Append the VLAN 999 settings to the end of file **vlan.txt**.

```
<Sysname> display vlan 999 >> vlan.txt
```

Verify whether the VLAN 999 settings are appended to the end of file **vlan.txt**.

```
<Sysname> more vlan.txt
```

```
VLAN ID: 1
VLAN type: Static
Route interface: Not configured
Description: VLAN 0001
Name: VLAN 0001
Tagged ports:   None
Untagged ports:
Ten-GigabitEthernet 1/0/2
```

```
VLAN ID: 999
VLAN type: Static
Route interface: Configured
IP address: 192.168.2.1
Subnet mask: 255.255.255.0
Description: For LAN Access
Name: VLAN 0999
Tagged ports:   None
Untagged ports:
Ten-GigabitEthernet 1/0/2
```

Viewing and managing the output from a display command effectively

You can use the following measures in combination to filter and manage the output from a **display** command:

- Numbering each output line from a display command
- Filtering the output from a display command
- Saving the output from a display command to a file

To use multiple measures to view and manage the output from a **display** command effectively, execute the following command in any view:

Task	Command
View and manage the output from a display command effectively.	display <i>command</i> [[by-linenum] { begin exclude include } <i>regular-expression</i>] [> <i>filename</i> >> <i>filename</i>]

For example:

```
# Save the running configuration to a separate file named test.txt, with each line numbered.
```

```
<Sysname> display current-configuration | by-linenum > test.txt
```

```
# Append lines including "snmp" in the running configuration to the file test.txt.
```

```
<Sysname> display current-configuration | include snmp >> test.txt
```

Saving the running configuration

To make your configuration survive a reboot, save the running configuration to a configuration file by using the **save** command in any view. This command saves all commands that have been successfully executed except for the one-time commands. Typical one-time commands include the **display** commands used for displaying information and the **reset** commands used for clearing information.

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

Login overview

The first time you access the device, you can only log in to the CLI through the console port. After login, you can change console login parameters or configure other access methods including console, Telnet, SSH, and SNMP.

Table 6 Login methods at a glance

Login method	Default settings and minimum configuration requirements
<p data-bbox="272 588 671 631">Logging in to the CLI:</p> <ul style="list-style-type: none"><li data-bbox="272 821 671 886">• Logging in through the console port locally	<p data-bbox="671 642 1437 771">By default, login through the console port is enabled, no username or password is required, and the user role network-admin is assigned. After login, configure password or scheme authentication mode to improve device security.</p> <p data-bbox="671 782 1437 847">By default, login through the console port is enabled and requires a password, but no password is configured.</p> <p data-bbox="671 858 1437 922">To use the console port for login, complete the following configuration tasks:</p> <ul style="list-style-type: none"><li data-bbox="671 933 1437 1019">• Log in through any other method and configure a password for password authentication, or change the authentication mode and configure parameters for the new authentication mode.<li data-bbox="671 1030 1437 1073">• Assign a user role (network-operator by default).
<ul style="list-style-type: none"><li data-bbox="272 1224 671 1267">• Logging in through Telnet	<p data-bbox="671 1084 1437 1127">By default, Telnet login is disabled.</p> <p data-bbox="671 1138 1437 1181">To Log in through Telnet, complete the following configuration tasks:</p> <ul style="list-style-type: none"><li data-bbox="671 1170 1437 1213">• Enable the Telnet server function.<li data-bbox="671 1224 1437 1289">• Assign an IP address to a Layer 3 interface and make sure the interface and the Telnet client can reach each other.<li data-bbox="671 1300 1437 1364">• Configure an authentication mode for VTY login users. By default, password authentication is used but no password is configured.<li data-bbox="671 1375 1437 1397">• Assign a user role to VTY login users (network-operator by default).
<ul style="list-style-type: none"><li data-bbox="272 1558 671 1601">• Logging in through SSH	<p data-bbox="671 1407 1437 1450">By default, SSH login is disabled.</p> <p data-bbox="671 1461 1437 1504">To log in through SSH, complete the following configuration tasks:</p> <ul style="list-style-type: none"><li data-bbox="671 1494 1437 1537">• Enable the SSH server function and configure SSH attributes.<li data-bbox="671 1548 1437 1612">• Assign an IP address to a Layer 3 interface and make sure the interface and the SSH client can reach each other.<li data-bbox="671 1623 1437 1688">• Configure scheme authentication for VTY login users (password authentication by default).<li data-bbox="671 1698 1437 1731">• Assign a user role to VTY login users (network-operator by default).
<p data-bbox="272 1839 671 1882">Accessing the device through SNMP</p>	<p data-bbox="671 1742 1437 1785">By default, SNMP access is disabled.</p> <p data-bbox="671 1795 1437 1860">To access the device through SNMP, complete the following configuration tasks:</p> <ul style="list-style-type: none"><li data-bbox="671 1860 1437 1925">• Assign an IP address to a Layer 3 interface, and make sure the interface and the NMS can reach each other.<li data-bbox="671 1936 1437 1970">• Configure SNMP basic parameters.

Logging in through the console port for the first device access

The first time you access the device, you can only log in to the CLI through the console port.

To log in through the console port, prepare a console terminal (for example, a PC) and make sure the console terminal has a terminal emulation program, for example, HyperTerminal in Windows XP.

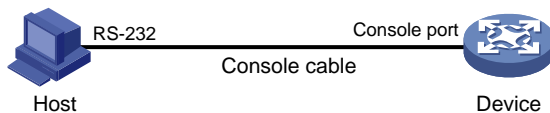
To log in through the console port:

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

! **IMPORTANT:**

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

Figure 2 Connecting a terminal to the console port



3. If the PC is off, turn on the PC.
4. On the PC, launch the terminal emulation program, create a connection that uses the serial port connected to the device, and set the port properties so the port properties match the following console port default settings:
 - **Bits per second**—9600 bps
 - **Flow control**—None
 - **Parity**—None
 - **Stop bits**—1
 - **Data bits**—8

Figure 3 through Figure 5 show the configuration procedure on Windows XP HyperTerminal. On Windows Server 2003, add the HyperTerminal program first, and then follow this procedure to log in to the device. On Windows Server 2008, Windows 7, Windows Vista, or another operating system, obtain a third-party terminal control program first, and then follow the user guide or online help to log in to the device.

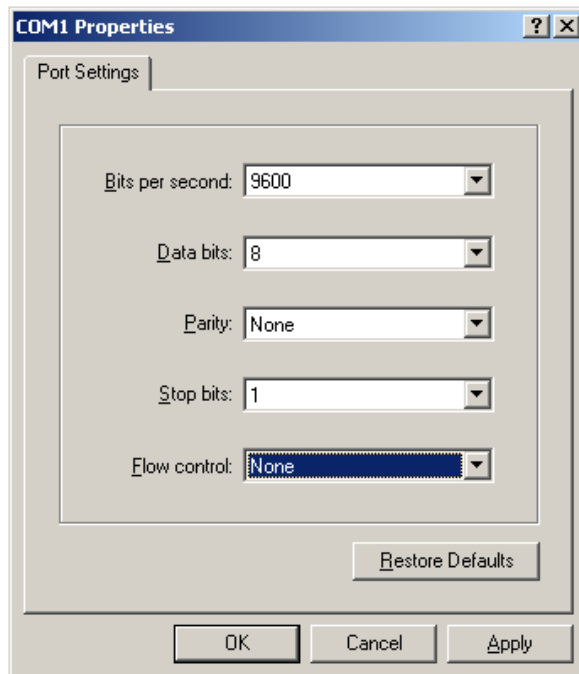
Figure 3 Creating a connection



Figure 4 Specifying the serial port used to establish the connection



Figure 5 Setting the properties of the serial port



5. Power on the device and press **Enter** after the device successfully completes the power-on self test (POST)..
6. At the default user view prompt <HP>, enter commands to configure the device or view the running status of the device. To get help, enter ?.

Logging in to the CLI

By default, you can log in to the CLI only through the console port. To facilitate device management, you can log in to the device through the console port and configure other login methods, including Telnet and SSH.

To prevent illegal access to the CLI and control user behaviors, you can configure login authentication, assign user roles, configure command authorization and command accounting, and use ACLs to filter unauthorized logins.

This chapter describes how to configure and use CLI login methods, including login authentication, user roles, and common user interface settings. For more information about command authorization, command accounting, and unauthorized access filtering, see "[Controlling user access](#)."

CLI overview

CLI user interfaces

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

Users are assigned different user interfaces, depending on their login methods, as shown in [Table 7](#).

Table 7 CLI login method and user interface matrix

User interface	Login method
AUX user interface	Console port.
Virtual type terminal (VTY) user interface	Telnet or SSH.

User interface assignment

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

For a CLI login, the device always picks the lowest numbered user interface from the idle user interfaces available for the type of login. For example, four VTY user interfaces (0 to 3) are configured, of which VTY 0 and VTY 3 are idle. When a user Telnets to the device, the device assigns VTY 0 to the user and uses the settings on VTY 0 to authenticate and manage the user.

User interface identification

Every user interface has an absolute number and a relative number for identification.

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

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

Login authentication modes

You can configure login authentication to prevent illegal access to the device CLI.

The device supports the following login authentication modes:

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

Different login authentication modes require different configurations on the user interfaces, as shown in [Table 8](#).

Table 8 Configuration required for different login authentication modes

Authentication mode	Configuration tasks
None	Set the authentication mode to none .
Password	1. Set the authentication mode to password .
	2. Set a password.
Scheme	3. Set the authentication mode to scheme .
	4. Configure login authentication methods in ISP domain view. For more information, see <i>Security Configuration Guide</i> .

User roles

A user is assigned one or more user roles at login, and a user can access only commands permitted by the assigned user roles. For more information about user roles, see "Configuring RBAC."

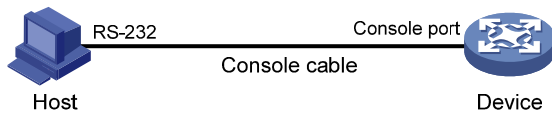
The device assigns user roles based on the login authentication mode and login method:

- If none or password authentication is used, the device assigns user roles according to the user role configuration made on the user interface.
- If scheme authentication is used:
 - For an SSH login user who uses publickey or password-publickey authentication, the device assigns user roles according to the user role configuration made on the user interface.
 - For other users, the device assigns user roles according to the user role configuration made on the AAA module. For remote AAA authentication users, if the AAA server does not assign any user role to a user and the default user role function is disabled, the user cannot log in.

Logging in through the console port locally

You can connect a terminal to the console port of the device to log in and manage the device, as shown in [Figure 6](#). For the login procedure, see "[Logging in through the console port for the first device access](#)."

Figure 6 Logging in through the console port



By default, console login is enabled and does not require authentication. To improve device security, configure the password or scheme authentication mode and assign user roles as required immediately after you log in to the device for the first time.

To configure console login, complete the following tasks:

Task	Remarks
Configuring login authentication: <ul style="list-style-type: none"> Configuring none authentication for console login Configuring password authentication for console login Configuring scheme authentication for console login 	Required. Configure one authentication mode as required.
Configuring common AUX user interface settings	Optional.

The console login configuration is effective only for users who log in after the configuration is made.

Configuring none authentication for console login

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter AUX user interface view.	user-interface aux <i>first-number</i> [<i>last-number</i>]	N/A
3. Enable none authentication mode.	authentication-mode none	By default, the authentication mode is none for the console login.
4. Assign a user role.	user-role <i>role-name</i>	By default, a console login user is assigned the user role network-admin.

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

Configuring password authentication for console login

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter AUX user interface view.	user-interface aux <i>first-number</i> [<i>last-number</i>]	N/A
3. Enable password authentication.	authentication-mode password	By default, the authentication mode is none for the console login
4. Set a password.	set authentication password { hash simple } <i>password</i>	By default, no password is set.

Step	Command	Remarks
5. Assign a user role.	user-role <i>role-name</i>	By default, a console login user is assigned the user role <code>network-admin</code> .

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

Configuring scheme authentication for console login

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter AUX user interface view.	user-interface aux <i>first-number</i> [<i>last-number</i>]	N/A
3. Enable scheme authentication.	authentication-mode <i>scheme</i>	By default, the authentication mode is none for the console login.

To use scheme authentication, you must also configure login authentication methods in ISP domain view. For more information, see *Security Configuration Guide*.

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

Configuring common AUX user interface settings

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

To log in through the console port after the configuration is complete, change the terminal settings on the configuration terminal to match the console port settings on the device.

To configure common settings for an AUX user interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter AUX user interface view.	user-interface aux <i>first-number</i> [<i>last-number</i>]	N/A
3. Set the baud rate.	speed <i>speed-value</i>	By default, the baud rate is 9600 bps.
4. Specify the parity check mode.	parity { even mark none odd space }	The default is none , namely no parity check.
5. Specify the number of stop bits.	stopbits { 1 1.5 2 }	The default is 1. Stop bits indicate the end of a character. The more the stop bits, the slower the transmission.

Step	Command	Remarks
6. Specify the number of data bits for each character.	databits { 5 6 7 8 }	The default is 8. The setting depends on the character coding type. For example, you can set it to 7 if standard ASCII characters are to be sent, and set it to 8 if extended ASCII characters are to be sent.
7. Define a shortcut key for starting a terminal session.	activation-key <i>character</i>	By default, pressing Enter starts the terminal session.
8. Define a shortcut key for terminating tasks.	escape-key { <i>character</i> default }	By default, pressing Ctrl+C terminates a task.
9. Configure the flow control mode.	flow-control { hardware none software }	By default, the flow control mode is none . The switch supports only the none flow control mode.
10. Specify the terminal display type.	terminal type { ansi vt100 }	By default, the terminal display type is ANSI. The device supports two terminal display types: ANSI and VT100. To ensure proper display on the terminal, set the display type of both the device and the terminal to VT100. Otherwise, when a command line has more than 80 characters, an anomaly such as cursor positioning error or abnormal terminal display might occur.
11. Set the maximum number of lines to be displayed on a screen.	screen-length <i>screen-length</i>	By default, a screen displays 24 lines at most. A value of 0 disables pausing between screens of output.
12. Set the size of the command history buffer.	history-command max-size <i>value</i>	By default, the buffer saves 10 history commands at most.
13. Set the session idle-timeout timer.	idle-timeout <i>minutes</i> [<i>seconds</i>]	The default is 10 minutes. If there is no interaction between the device and the user within the idle-timeout interval, the system automatically terminates the user connection on the user interface. If you set the idle-timeout timer to 0, the session will not be aged out.

Logging in through Telnet

You can Telnet to the device to remotely manage the device, or use the device as a Telnet client to Telnet to other devices to manage them.

By default, Telnet login is disabled on the device. To log in to the device through Telnet, you must first log in to the device through any other method, enable the Telnet server, and configure Telnet login authentication on the device.

Configuring Telnet login on the device

Task	Remarks
Configuring login authentication:	
<ul style="list-style-type: none"> Configuring none authentication for Telnet login Configuring password authentication for Telnet login Configuring scheme authentication for Telnet login 	<p>Required.</p> <p>Configure one authentication mode as required.</p>
Configuring common VTY user interface settings	Optional.

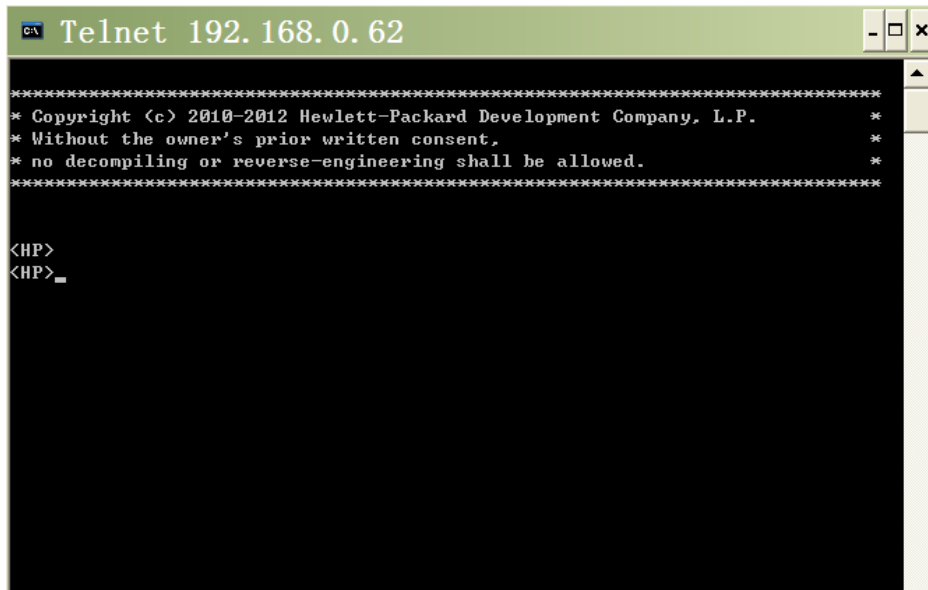
The Telnet login configuration is effective only for users who log in after the configuration is made.

Configuring none authentication for Telnet login

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable Telnet server.	telnet server enable	By default, the Telnet server function is disabled.
3. Enter one or multiple VTY user interface views.	user-interface vty <i>first-number</i> [<i>last-number</i>]	N/A
4. Enable none authentication mode.	authentication-mode none	By default, password authentication is enabled for VTY user interfaces.
5. (Optional.) Assign a user role.	user-role <i>role-name</i>	By default, a VTY user interface user is assigned the user role <code>network-operator</code> .

The next time you attempt to Telnet to the device, you do not need to provide any username or password, as shown in [Figure 7](#). If the maximum number of login users has been reached, your login attempt fails and the message "All user interfaces are used, please try later!" appears.

Figure 7 Telnetting to the device without authentication



Configuring password authentication for Telnet login

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable Telnet server.	telnet server enable	By default, the Telnet server function is disabled.
3. Enter one or multiple VTY user interface views.	user-interface vty <i>first-number</i> [<i>last-number</i>]	N/A
4. Enable password authentication.	authentication-mode password	By default, password authentication is enabled for VTY user interfaces.
5. Set a password.	set authentication password { hash simple } <i>password</i>	By default, no password is set.
6. (Optional.) Assign a user role.	user-role <i>role-name</i>	By default, a VTY user interface user is assigned the user role network-operator.

The next time you attempt to Telnet to the device, you must provide the configured login password, as shown in Figure 8. If the maximum number of login users has been reached, your login attempt fails and the message "All user interfaces are used, please try later!" appears.

Figure 8 Password authentication interface for Telnet login

```
*****
* Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****

Password:
<HP>
<HP>
```

Configuring scheme authentication for Telnet login

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable Telnet server.	telnet server enable	By default, the Telnet server function is disabled.
3. Enter one or multiple VTY user interface views.	user-interface vty <i>first-number</i> [<i>last-number</i>]	N/A
4. Enable scheme authentication.	authentication-mode scheme	By default, password authentication is enabled for VTY user interfaces.

To use scheme authentication, you must also configure login authentication methods in ISP domain view. For more information, see *Security Configuration Guide*.

The next time you attempt to Telnet to the CLI, you must provide the configured login username and password, as shown in [Figure 9](#). If the maximum number of login users has been reached, your login attempt fails and the message "All user interfaces are used, please try later!" appears.

Figure 9 Scheme authentication interface for Telnet login

```

*****
* Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P. *
* Without the owner's prior written consent, *
* no decompiling or reverse-engineering shall be allowed. *
*****

login:
login: admin
Password:
<HP>

```

Configuring common VTY user interface settings

For a VTY user interface, you can specify a command that is to be automatically executed when a user logs in. After executing the specified command and performing the incurred task, the system automatically disconnects the Telnet session. Before you configure this function and save the configuration, make sure you can access the CLI through a different user interface.

Typically, you configure the **auto-execute command telnet** X.X.X.X command on the device so the device redirects a Telnet user to the host at X.X.X.X. In this case, the connection to the current device is closed when the user terminates the Telnet connection to X.X.X.X.

To configure common settings for VTY user interfaces:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter one or multiple VTY user interface views.	user-interface vty <i>first-number [last-number]</i>	N/A
3. Enable the terminal service.	shell	By default, terminal service is enabled.
4. Specify the protocols for the user interfaces to support.	protocol inbound { all ssh telnet }	By default, both Telnet and SSH are supported. This configuration is effective only for users who log in to the user interfaces after the configuration is made.
5. Define a shortcut key for terminating tasks.	escape-key { character default }	By default, pressing Ctrl+C terminates a task.
6. Specify the terminal display type.	terminal type { ansi vt100 }	By default, the terminal display type is ANSI.
7. Set the maximum number of lines to be displayed on a screen.	screen-length screen-length	By default, up to 24 lines is displayed on a screen. A value of 0 disables the function.

Step	Command	Remarks
8. Set the size of command history buffer.	history-command max-size <i>value</i>	By default, the buffer saves 10 history commands.
9. Set the idle-timeout timer.	idle-timeout <i>minutes</i> [<i>seconds</i>]	By default, the idle-timeout interval is 10 minutes for all user interfaces. If there is no interaction between the device and the user within the idle-timeout interval, the system automatically terminates the user connection on the user interface. If you set the idle-timeout timer to 0, the session will not be aged out.
10. Specify a command to be automatically executed when users log in to the user interfaces.	auto-execute command <i>command</i>	By default, no automatically executed command is specified.

Using the device to log in to a Telnet server

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

Figure 10 Telnetting from the device to a Telnet server



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

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Specify the source IPv4 address or source interface for outgoing Telnet packets.	telnet client source { interface <i>interface-type interface-number</i> ip <i>ip-address</i> }	By default, no source IPv4 address or source interface is specified, and the primary IPv4 address of the outbound interface is used as the source address for outgoing Telnet packets.
3. Exit to user view.	quit	N/A

Step	Command	Remarks
4. Use the device to log in to a Telnet server.	<ul style="list-style-type: none"> Log in to an IPv4 Telnet server: telnet <i>remote-host</i> [<i>service-port</i>] [vpn-instance <i>vpn-instance-name</i>] [source { interface <i>interface-type</i> <i>interface-number</i> ip <i>ip-address</i> }] Log in to an IPv6 Telnet server: telnet ipv6 <i>remote-host</i> [-i <i>interface-type interface-number</i>] [<i>port-number</i>] [vpn-instance <i>vpn-instance-name</i>] 	Use either command.

Logging in through SSH

SSH offers a secure approach to remote login. By providing encryption and strong authentication, it protects devices against attacks such as IP spoofing and plain text password interception. For more information, see *Security Configuration Guide*.

You can use an SSH client to log in to the device for remote management, or use the device as an SSH client to log in to an SSH server.

By default, SSH login is disabled on the device. To log in to the device through SSH, you must log in to the device through any other method and configure SSH login on the device first.

Configuring SSH login on the device

This section provides the configuration procedure for when the SSH client authentication method is password. For more information about SSH and publickey authentication configuration, see *Security Configuration Guide*.

To configure SSH login on the device:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create local key pairs.	public-key local create { dsa rsa }	By default, no local key pairs are created.
3. Enable SSH server.	ssh server enable	By default, SSH server is disabled.
4. Create an SSH user and specify the authentication mode.	ssh user <i>username</i> service-type stelnet authentication-type { password { any password-publickey publickey } assign publickey <i>keyname</i> }	By default, no SSH user is configured on the device.
5. Enter one or multiple VTY user interface views.	user-interface vty <i>first-number</i> [<i>last-number</i>]	N/A
6. Enable scheme authentication.	authentication-mode scheme	By default, password authentication is enabled for VTY user interfaces.

Step	Command	Remarks
7. (Optional.) Specify the protocols for the user interfaces to support.	protocol inbound { all ssh telnet }	By default, both Telnet and SSH are supported. This configuration is effective only for users who log in to the user interfaces after the configuration is made.
8. Exit to system view.	quit	N/A
9. (Optional.) Configure common settings for VTY user interfaces.	See " Configuring common VTY user interface settings. "	N/A

Using the device to log in to an SSH server

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

Figure 11 Logging in to an SSH client from the device



Perform the following tasks in user view:

Task	Command
Log in to an IPv4 SSH server.	ssh2 server
Log in to an IPv6 SSH server.	ssh2 ipv6 server

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

Displaying and maintaining CLI login

Execute **display** commands in any view and the other commands in user view.

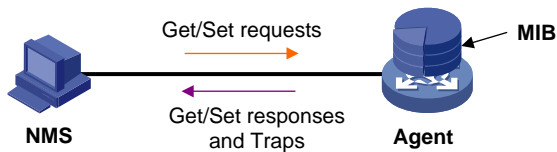
Task	Command	Remarks
Display information about the user interfaces that are being used.	display users	N/A
Display information about all user interfaces the device supports.	display users all	N/A
Display user interface information.	display user-interface [<i>num1</i>] [{ aux vtty } <i>num2</i>] [summary]	N/A

Task	Command	Remarks
Display the source IPv4 address or interface configured for the device to use for outgoing Telnet packets when serving as a Telnet client.	display telnet client	N/A
Release a user interface.	free user-interface { <i>num1</i> { aux vty } <i>num2</i> }	Multiple users can log in to the device to simultaneously configure the device. When necessary, you can execute this command to release some connections. You cannot use this command to release the connection you are using.
Lock the current user interface.	lock	By default, the system does not lock any user interface.
Send messages to user interfaces.	send { all <i>num1</i> { aux vty } <i>num2</i> }	N/A

Accessing the device through SNMP

You can run SNMP on an NMS to access the device MIB and perform GET and SET operations to manage and monitor the device.

Figure 12 SNMP access diagram



The device supports SNMPv1, SNMPv2c, and SNMPv3, and can work with various network management software products, including IMC. However, the device and the NMS must use the same SNMP version. For more information about SNMP, see *Network Management and Monitoring Configuration Guide*.

By default, SNMP access is disabled. To access the device through SNMP, you must log in to the device through any other method and configure SNMP access.

Configuring SNMPv3 access

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the SNMP agent.	snmp-agent	By default, the SNMP agent is disabled.
3. (Optional.) Create or update MIB view information.	snmp-agent mib-view { excluded included } view-name oid-tree [mask mask-value]	By default, the device has four views, all of which are named ViewDefault : <ul style="list-style-type: none"> View 1 includes MIB subtree iso. View 2 does not include subtree snmpUsmMIB. View 3 does not include subtree snmpVacmMIB. View 4 does not include subtree snmpModules.18.
4. Create an SNMPv3 group.	snmp-agent group v3 group-name [authentication privacy] [read-view view-name] [write-view view-name] [notify-view view-name] [acl acl-number acl ipv6 ipv6-acl-number] *	By default, no SNMPv3 group exists.

Step	Command	Remarks
5. Create an SNMPv3 user.	<pre>snmp-agent usm-user v3 user-name group-name [remote { ip-address ipv6 ipv6-address } [vpn-instance vpn-instance-name]] [{ cipher simple } authentication-mode { md5 sha } auth-password [privacy-mode { aes128 des56 } priv-password]] [acl acl-number acl ipv6 ipv6-acl-number] *</pre>	To send informs to an SNMPv3 NMS, you must use the remote ip-address option to specify the IP address of the NMS.

Configuring SNMPv1 or SNMPv2c access

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the SNMP agent.	snmp-agent	By default, the SNMP agent is disabled.
3. (Optional.) Create or update MIB view information.	<pre>snmp-agent mib-view { excluded included } view-name oid-tree [mask mask-value]</pre>	<p>By default, the device has four views, all of which are named ViewDefault:</p> <ul style="list-style-type: none"> View 1 includes MIB subtree iso. View 2 does not include subtree snmpUsmMIB. View 3 does not include subtree snmpVacmMIB. View 4 does not include subtree snmpModules.18.
4. Configure the SNMP access right.	<ul style="list-style-type: none"> (Approach 1) Specify the SNMP NMS access right directly by configuring an SNMP community: <pre>snmp-agent community { read write } community-name [mib-view view-name] [acl acl-number acl ipv6 ipv6-acl-number] *</pre> (Approach 2) Configure an SNMP group and add a user to the SNMP group: <ol style="list-style-type: none"> snmp-agent group { v1 v2c } group-name [read-view view-name] [write-view view-name] [notify-view view-name] [acl acl-number acl ipv6 ipv6-acl-number] * snmp-agent usm-user { v1 v2c } user-name group-name [acl acl-number acl ipv6 ipv6-acl-number] * 	<p>Use either approach.</p> <p>The username in approach 2 is equivalent to the community name used in approach 1, and must be the same as the community name configured on the NMS.</p> <p>By default, no SNMP group or SNMP community exists.</p>

Controlling user access

Use ACLs to prevent unauthorized access and configure command authorization and accounting to monitor and control user behaviors. For more information about ACLs, see *ACL and QoS Configuration Guide*.

Controlling Telnet/SSH logins

Use basic ACLs (2000 to 2999) to filter Telnet and SSH logins by source IP address. Use advanced ACLs (3000 to 3999) to filter Telnet and SSH logins by source and/or destination IP address. Use Ethernet frame header ACLs (4000 to 4999) to filter Telnet and SSH logins by source MAC address.

If an applied ACL does not exist or has no rules, no user login restriction is applied. If the ACL exists and has rules, only users permitted by the ACL can access the device through Telnet or SSH.

Configuration procedures

To control Telnet logins:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Apply an ACL to filter Telnet logins.	<ul style="list-style-type: none">• telnet server acl <i>acl-number</i>• telnet server ipv6 acl { <i>layer2-acl-number</i> ipv6 <i>ipv6-acl-number</i> }	By default, no ACL is used to filter Telnet logins.

To control SSH logins:

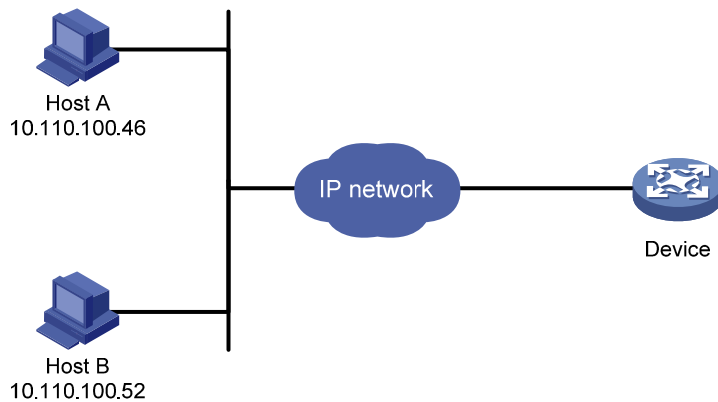
Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Apply an ACL to filter SSH logins.	<ul style="list-style-type: none">• ssh server acl <i>acl-number</i>• ssh server ipv6 acl [ipv6] <i>acl-number</i>	By default, no ACL is used to filter SSH logins. For more information about these two commands, see <i>Security Command Reference</i> .

Configuration example

Network requirements

Configure the device in [Figure 13](#) to permit only Telnet packets sourced from Host A and Host B.

Figure 13 Network diagram



Configuration procedure

Configure an ACL to permit packets sourced from Host A and Host B.

```
<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
```

Apply the ACL to filter Telnet logins.

```
[Sysname] telnet server acl 2000
```

Controlling SNMP access

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

Configuration procedure

To control SNMP access, configure ACLs as required and complete the following configuration:

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

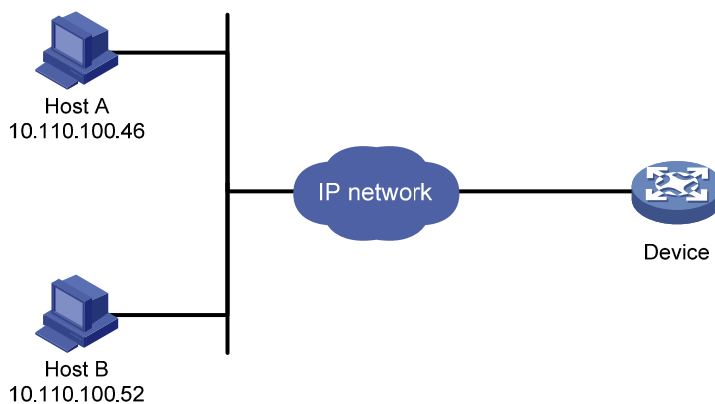
Step	Command	Remarks
2. Apply the ACL to an SNMP community, group, or user.	<ul style="list-style-type: none"> SNMP community: <code>snmp-agent community { read write } community-name [mib-view view-name] [acl acl-number acl ipv6 ipv6-acl-number] *</code> SNMPv1/v2c group: <code>snmp-agent group { v1 v2c } group-name [read-view view-name] [write-view view-name] [notify-view view-name] [acl acl-number acl ipv6 ipv6-acl-number] *</code> SNMPv3 group: <code>snmp-agent group v3 group-name [authentication privacy] [read-view view-name] [write-view view-name] [notify-view view-name] [acl acl-number acl ipv6 ipv6-acl-number] *</code> SNMPv1/v2c user: <code>snmp-agent usm-user { v1 v2c } user-name group-name [acl acl-number acl ipv6 ipv6-acl-number] *</code> SNMPv3 user: <code>snmp-agent usm-user v3 user-name group-name [remote { ip-address ipv6 ipv6-address } [vpn-instance vpn-instance-name]] [{ cipher simple } authentication-mode { md5 sha } auth-password [privacy-mode { aes128 des56 } priv-password]] [acl acl-number acl ipv6 ipv6-acl-number] *</code> 	For more information about SNMP, see <i>Network Management and Monitoring Configuration Guide</i> .

Configuration example

Network requirements

Configure the device in [Figure 14](#) to allow Host A and Host B to access the device through SNMP.

Figure 14 Network diagram



Configuration procedure

Create an ACL to permit packets sourced from Host A and Host B.

```

<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 command authorization

By default, commands are available for a user depending only on that user's user roles. When the authentication mode is scheme, you can configure the command authorization function to further control access to commands.

After you enable command authorization, a command is available for a user only if the user has the commensurate user role and is authorized to use the command by the AAA scheme.

This section provides the procedure for configuring command authorization. To make the command authorization function take effect, you must configure a command authorization method in ISP domain view. For more information, see *Security Configuration Guide*.

Configuration procedure

To configure command authorization:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter user interface view.	user-interface { <i>first-number1</i> [<i>last-number1</i>] { aux vty } <i>first-number2</i> [<i>last-number2</i>] }	N/A
3. Enable scheme authentication.	authentication-mode scheme	By default, the authentication mode is none for the AUX user interface.
4. Enable command authorization.	command authorization	By default, command authorization is disabled, and the commands available for a user only depend on the user role. This command takes effect immediately after it is configured. Configure the command authorization method in ISP domain view before configuring this command.

Configuring command accounting

Command accounting allows the HWTACACS server to record all executed commands that are supported by the device, regardless of the command execution result. This function helps control and monitor user behaviors on the device.

When command accounting is disabled, the accounting server does not record the commands executed by users. If command accounting is enabled but command authorization is not, every executed command is recorded on the HWTACACS server. If both command accounting and command

authorization are enabled, only authorized commands that are executed are recorded on the HWTACACS server.

This section provides only the procedure for configuring command accounting. To make the command accounting function take effect, you must configure a command accounting method in ISP domain view. For more information, see *Security Configuration Guide*.

Configuration procedure

To configure command accounting:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter user interface view.	user-interface { <i>first-number1</i> [<i>last-number1</i>] { aux vty } <i>first-number2</i> [<i>last-number2</i>] }	N/A
3. Enable scheme authentication.	authentication-mode scheme	By default, the authentication mode is none for the AUX user interface.
4. Enable command accounting.	command accounting	By default, command accounting is disabled, and the accounting server does not record the commands executed by users.

Configuring RBAC

Role based access control (RBAC) controls user access to commands and resources based on user role. This chapter describes the basic idea of RBAC and guides you through the RBAC configuration procedure.

Overview

On devices that support multiple users, RBAC is used to assign command and resource access permissions to user roles that are created for different job functions. Users are given permission to access a set of commands and resources based on their user roles. Because user roles are persistent, in contrast to users, separating permissions from users enables easy permission authorization management. When the job responsibilities of a user changes, new users are added, or old users are removed, you only need to change the user roles or assign new user roles.

Permission assignment

Assigning permissions to a user role includes the following:

- Define a set of rules to specify commands accessible or inaccessible to the user role. (See "[User role rules](#).")
- Configure resource access policies to specify which interfaces, VLANs, and VPNs are accessible to the user role. (See "[Resource access policies](#).")

To use a command related to a specific interface, VLAN, or VPN, a user role must have access to both the command and the interface, VLAN, or VPN.

For example, a user role has access to the **qos apply policy** command and access to only interface Ten-GigabitEthernet 1/0/1. With this user role, you can enter the interface view and use the **qos apply policy** command on the interface, but you cannot enter the view of any other interface or use the command on any other interface. If the user role has access to any interface but does not have access to the **qos apply policy** command, you cannot use the command on any interface.

User role rules

User role rules permit or deny access to commands. You can define the following types of rules for different access control granularities:

- **Command rule**—Controls access to a command or a set of commands that match a regular expression.
- **Feature rule**—Controls access to the commands of a feature by command type:
 - **Read**—Commands that display configuration and maintenance information. Examples include the **display** commands and the **dir** command.
 - **Write**—Commands that configure the feature in the system. Examples include the **info-center enable** command and the **debugging** command.
 - **Execute**—Commands that execute specific functions. Examples include the **ping** command and the **ftp** command.
- **Feature group rule**—Controls access to commands of a group of features by command type.

A user role can have multiple rules uniquely identified by rule numbers. The set of permitted commands in these rules are accessible to the user role. If two rules conflict, the one with higher number takes effect. For example, if rule 1 permits the **ping** command, rule 2 permits the **tracert** command, and rule 3 denies the **ping** command, the user role can use the **tracert** command but not the **ping** command.

Resource access policies

Resource access policies control access of user roles to system resources and include the following types:

- **Interface policy**—Controls access to interfaces.
- **VLAN policy**—Controls access to VLANs.
- **VPN instance policy**—Controls access to VPNs.

Resource access policies do not control access to the interface, VLAN, or VPN options in the **display** commands. You can specify these options in the **display** commands if they are permitted by any user role rule.

Predefined user roles

The system provides 18 predefined user roles. All these user roles have access to all system resources (interfaces, VLANs, and VPNs), but their command access permissions (see [Table 9](#)) differ.

Among all the predefined user roles, only the network-admin and level-15 user roles can access the RBAC feature and change the settings including **user-role**, **authentication-mode**, **protocol**, and **set authentication password** in user interface view.

Among all the predefined user roles, level-0 to level-14 users can modify their own permissions for any commands except for the **display history-command all** command.

Table 9 Predefined roles and permissions matrix

User role name	Permissions
network-admin	Accesses all features and resources in the system.
network-operator	Accesses the display commands (except display history-command all) for all features and resources in the system.
level- <i>n</i> (<i>n</i> = 0 to 15)	<ul style="list-style-type: none"> • level-0—Has access to the commands of ping, Tracert, ssh, telnet, and super. Level-0 access rights are configurable. • level-1—Has access to the display commands (except display history-command all) of all features and resources in the system, in addition to all access rights of the user role level-0. Level-1 access rights are configurable. • level-2 to level-8, and level-10 to level-14—Have no access rights by default. Access rights are configurable. • level-9—Has access to all features and resources except RBAC, local users, file management, device management, and the display history-command all command. If you are logged in with a local user account that has a level-9 user role, you can change the password in the local user account. Level-9 access rights are configurable. • level-15—Has the same access rights as the role network-admin. Commands described as accessible to network-admin are also accessible to the Level-15 user role.

Assigning user roles

You assign access rights to users by assigning at least one user role. The users can use the collection of commands and resources accessible to any user role assigned to them. For example, user role A denies access to the **qos apply policy** command and permits access to only interface Ten-GigabitEthernet 1/0/1, and user role B permits access to the **qos apply policy** command and all interfaces. With these two user roles, you can access any interface to use the **qos apply policy** command.

Depending on the authentication method, user role assignment has the following approaches:

- **AAA authorization**—If scheme authentication is used, the AAA module handles user role assignment.
 - If the user passes local authorization, the device assigns the user roles specified in the local user account.
 - If the user passes remote authorization, the remote AAA server assigns the user roles specified on the server to the user. The AAA server can be a RADIUS or HWTACACS server.
- **None-AAA authorization**—If the user uses password authentication or no authentication, the device assigns user roles specified on the user interface. This approach also applies to SSH clients that use publickey or password-publickey authentication. User roles assigned to these SSH clients are specified in their respective local management user accounts.

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

Configuration task list

Tasks at a glance
(Required.) Creating user roles
(Required.) Configuring user role rules
(Optional.) Configuring feature groups
(Optional.) Changing resource access policies
(Optional.) Assigning user roles
(Optional.) Configuring user role switching

Creating user roles

In addition to the predefined user roles, you can create up to 64 custom user roles for granular access control.

To create a user role:

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

Step	Command	Remarks
2. Create a user role and enter user role view.	role name <i>role-name</i>	By default, the system has 18 predefined user roles: network-admin, network-operator, and level-n (where n equals an integer in the range 0 to 15). Among these user roles, only the permissions and description of the user roles level-0 to level-14 are configurable.
3. (Optional.) Configure a description for the user role.	description <i>text</i>	By default, a user role has no description.

Configuring user role rules


Configure command, feature, and feature group rules to permit or deny the access of a user role to specific commands.

You can configure up to 256 rules for a user role, but the total number of user role rules in the system cannot exceed 1024.

If two rules of a user role conflict, the one with a higher rule number has priority.

Any rule modification, addition, or removal for a user role takes effect only on users that are logged in with the user role after the change.


To configure rules for a user role:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter user role view.	role name <i>role-name</i>	N/A
3. Configure a rule.	<ul style="list-style-type: none"> Configure a command rule: rule <i>number</i> { deny permit } command <i>command-string</i> Configure a feature rule: rule <i>number</i> { deny permit } { execute read write } * feature [<i>feature-name</i>] Configure a feature group rule: rule <i>number</i> { deny permit } { execute read write } * feature-group <i>feature-group-name</i> 	<p>Configure at least one command.</p> <p>By default, a user-defined user role has no rules or access to any command.</p> <p>Repeat this step to add up to 256 rules to the user role.</p> <p> IMPORTANT:</p> <p>When you configure feature rules, you can specify only features available in the system and must enter feature names exactly the same as they are displayed, including the case.</p>

Configuring feature groups

Use feature groups to bulk assign command access permissions to sets of features. In addition to the predefined feature groups, you can create up to 64 custom feature groups and assign a feature to multiple feature groups.

To configure a feature group:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a feature group and enter feature group view.	role feature-group name <i>feature-group-name</i>	By default, the system has the following predefined feature groups: <ul style="list-style-type: none">• L2—Includes all Layer 2 commands.• L3—Includes all Layer 3 commands. These two groups are not user configurable.
3. Add a feature to the feature group.	feature <i>feature-name</i>	By default, a feature group has no features.  IMPORTANT: You can specify only features available in the system and must enter feature names exactly the same as they are displayed, including the case.

Changing resource access policies

Every user role has one interface policy, VLAN policy, and VPN instance policy. By default, these policies permit user roles to access any interface, VLAN, and VPN. You can change the policies of user-defined user roles and the predefined level-n user roles to limit their access to interfaces, VLANs, and VPNs. A changed policy takes effect only on users that are logged in with the user role after the change.

Changing the interface policy of a user role

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter user role view.	role name <i>role-name</i>	N/A
3. Enter user role interface policy view.	interface policy deny	By default, the interface policies of user roles permit access to all interfaces. This command disables the access of the user role to any interface.

Step	Command	Remarks
4. (Optional.) Specify a list of interfaces accessible to the user role.	permit interface <i>interface-list</i>	By default, no accessible interfaces are configured. To add more accessible interfaces, repeat this step.

Changing the VLAN policy of a user role

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter user role view.	role name <i>role-name</i>	N/A
3. Enter user role VLAN policy view.	vlan policy deny	By default, the VLAN policies of user roles permit access to all VLANs. This command disables the access of the user role to any VLAN.
4. (Optional.) Specify a list of VLANs accessible to the user role.	permit vlan <i>vlan-id-list</i>	By default, no accessible VLANs are configured. To add more accessible VLANs, repeat this step.

Changing the VPN instance policy of a user role

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter user role view.	role name <i>role-name</i>	N/A
3. Enter user role VPN instance policy view.	vpn-instance policy deny	By default, the VPN policies of user roles permit access to all VPNs. This command disables the access of the user role to any VPN.
4. (Optional.) Specify a list of VPNs accessible to the user role.	permit vpn-instance <i>vpn-instance-name</i> &<1-10>	By default, no accessible VPNs are configured. To add more accessible VPNs, repeat this step.

Assigning user roles

To control user access to the system, you must assign at least one user role. Make sure at least one user role among the user roles assigned by the server exists on the device. User role assignment procedure varies with remote AAA authentication users, local AAA authentication users, and non-AAA authentication users (see "[Assigning user roles](#)"). For more information about AAA authentication, see *Security Configuration Guide*.

Enabling the default user role function

The default user role function assigns the network-operator user role to a local or remote AAA authenticated user if the AAA server has not authorized the user to use any user roles. Without the function, AAA users that have passed authentication cannot access the system if they have no user role authorization.

To enable the default user role function for AAA authentication users:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the default user role function.	role default-role enable	The default user role function is disabled.

Assigning user roles to remote AAA authentication users

For remote AAA authentication users, user roles are configured on the remote authentication server. For information about configuring user roles for RADIUS users, see the RADIUS server documentation. For HWTACACS users, the role configuration must use the **roles="role-1 role-2 ... role-n"** format, where user roles are space separated. For example, configure **roles="level-0 level-1 level-2"** to assign level-0, level-1, and level-2 to an HWTACACS user.

NOTE:

- To be compatible with privilege-based access control, the device automatically converts privilege-based user levels (0 to 15) assigned by an AAA server to RBAC user roles (level-0 to level-15).
- If the AAA server assigns a privilege-based user level and a user role to a user, the user can use the collection of commands and resources accessible to both the user level and the user role.

Assigning user roles to local AAA authentication users

Configure user roles for local AAA authentication users in their local user accounts. Every local user has a default user role. If this default user role is not suitable, delete it.

To assign a user role to a local user:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a local user and enter local user view.	local-user user-name class { manage network }	N/A
3. Authorize the user to have a user role.	authorization-attribute user-role <i>role-name</i>	Repeat this step to assign the user to up to 64 user roles. By default, network-operator is assigned to local users created by a network-admin user or level-15 user.

Assigning user roles to non-AAA authentication users on user interfaces

Specify user roles for the following two types of login users on the user interfaces:

- Users that use password authentication or no authentication.
- SSH clients that use publickey or password-publickey authentication. User roles assigned to these SSH clients are specified in their respective local management user accounts.

For more information about user interfaces, see "Login overview" and "Logging in to the CLI." For more information about SSH, see *Security Configuration Guide*.

To assign a user role to non-AAA authentication users on a user interface:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter user interface view.	user-interface { <i>first-num1</i> [<i>last-num1</i>] { aux vty } <i>first-num2</i> [<i>last-num2</i>] }	N/A
3. Specify a user role on the user interface.	user-role <i>role-name</i>	Repeat this step to specify up to 64 user roles on a user interface. By default, network-admin is specified on the AUX user interface, and network-operator is specified on any other user interface.

Configuring user role switching

You can switch to a different user role without reconnecting to the device. This operation does not change the user role settings in the user account that you have been logged in with, and it is effective only on the current login. The next time you are logged in with the user account, the original user role settings take effect.

Configuration guidelines

- To enable VTY users to switch the user role, you must configure user role switching authentication. [Table 10](#) describes the available authentication modes and configuration requirements.
- Local password authentication is available for switching to any user role, but remote AAA authentication is available only for switching to a level-n user role.
 - If HWTACACS authentication is used, use a user account that has the target user role level or a user role level higher than the target user role for role switching. For example, if the user account **test** has the user role **level-3**, you can use this user account to switch the user role among **level-0**, **level-1**, **level-2**, and **level-3**. In this approach, you must enter the correct username and password to pass authentication.
 - If RADIUS authentication is used, you must create a user account for each level-n user role in the **\$enabn\$** format or the **\$enabn\$@domain-name** format, where *n* represents the user role level.

In this approach, the username you enter is ignored. You can pass authentication as long as the password is correct.

- If you execute the **quit** command after switching to a user role, you are logged out of the current user interface.

Table 10 Authentication modes for user role switching

Keywords	Authentication mode	Description
local	Local password authentication only (local-only)	The device uses the locally configured switching password for authentication. An AUX user can switch the user role without authentication in the local password authentication.
scheme	Remote AAA authentication through HWTACACS or RADIUS (remote-only)	The device sends the username and password to the HWTACACS or RADIUS server for remote authentication. To use this mode, you must perform the following configuration tasks: <ul style="list-style-type: none"> • Configure the required HWTACACS or RADIUS scheme and configure the ISP domain to use the scheme for the user. For more information, see <i>Security Configuration Guide</i>. • Add the user account and password on the HWTACACS or RADIUS server.
local scheme	Local password authentication first and then remote AAA authentication (local-then-remote)	Local password authentication is performed first. If no switching password is configured, the device performs AAA authentication.
scheme local	Remote AAA authentication first and then local password authentication (remote-then-local)	AAA authentication is performed first. If the remote HWTACACS or RADIUS server does not respond or the AAA configuration on the device is invalid, local password authentication is performed.

Configuring user role switching authentication

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set an authentication mode.	super authentication-mode { local scheme } *	By default, local-only authentication applies.
3. Set a local authentication password for switching to a user role.	super password [role rolename] { hash simple } password	Use this step for local password authentication. By default, no switching password is configured. If you do not specify the role rolename option, the command sets the password for network-admin.

Switching the user role

A VTY user must pass authentication before switching to a user role.

Perform the following task in user view:

Task	Command	Remarks
Switch the user role.	super [<i>rolename</i>]	The user role switching fails after three consecutive unsuccessful password attempts.

Displaying RBAC settings

Execute **display** commands in any view.

Task	Command
Display user role information.	display role [name <i>role-name</i>]
Display user role feature information.	display role feature [name <i>feature-name</i> verbose]
Display user role feature group information.	display role feature-group [name <i>feature-group-name</i>] [verbose]

RBAC configuration example for local AAA authentication users

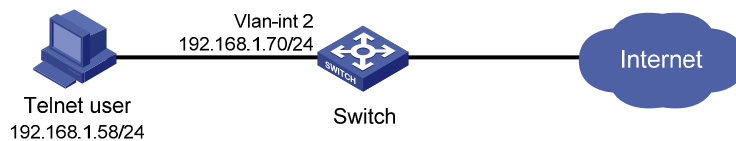
Network requirements

The switch in [Figure 15](#) performs local AAA authentication for the Telnet user at 192.168.1.58. This Telnet user has the username **user1@bbb** and is assigned the user role **role1**.

Configure role1 to have the following permissions:

- Executes the read commands of any feature.
- Configures no VLANs except VLANs 10 to 20.

Figure 15 Network diagram



Configuration procedure

Assign an IP address to VLAN interface 2, the interface connected to the Telnet user.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

Enable Telnet server.

```

[Switch] telnet server enable

# Enable scheme authentication on the user interfaces for Telnet users.
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
[Switch-ui-vty0-15] quit

# Enable local authentication and authorization for the ISP domain bbb.
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login local
[Switch-isp-bbb] quit

# Create the user role role1.
[Switch] role name role1

# Configure rule 1 to permit the user role to access read commands of all features.
[Switch-role-role1] rule 1 permit read feature

# Configure rule 2 to permit the user role to create VLANs and access commands in VLAN view.
[Switch-role-role1] rule 2 permit command system-view ; vlan *

# Change the VLAN policy to permit the user role to configure only VLANs 10 to 20.
[Switch-role-role1] vlan policy deny
[Switch-role-role1-vlanpolicy] permit vlan 10 to 20
[Switch-role-role1-vlanpolicy] quit
[Switch-role-role1] quit

# Create a management local user named user1 and enter its view.
[Switch] local-user user1 class manage

# Set a plaintext password aabbcc for the user.
[Switch-luser-manage-user1] password simple aabbcc

# Set the service type to Telnet.
[Switch-luser-manage-user1] service-type telnet

# Assign role1 to the user.
[Switch-luser-manage-user1] authorization-attribute user-role role1

# To make sure that the user has only the permissions of role1, remove the user from the default user role
network-operator.
[Switch-luser-manage-user1] undo authorization-attribute user-role network-operator
[Switch-luser-manage-user1] quit

```

Verifying the configuration

```

# Telnet to the switch, and enter the username and password to access the user interface. (Details not
shown.)

# Verify that you can create VLANs 10 to 20. This example uses VLAN 10.
<Switch> system-view
[Switch] vlan 10
[Switch-vlan10] quit

# Verify that you cannot create any VLANs other than VLANs 10 to 20. This example uses VLAN 30.

```

```
[Switch] vlan 30
Permission denied.
```

Verify that you can use all read commands of any feature. This example uses **display clock**.

```
[Switch] display clock
09:31:56 UTC Sat 01/01/2011
[Switch] quit
```

Verify that you cannot use the write or execute commands of any feature.

```
<Switch> debugging role all
Permission denied.
<Switch> ping 192.168.1.58
Permission denied.
```

RBAC configuration example for RADIUS authentication users

Network requirements

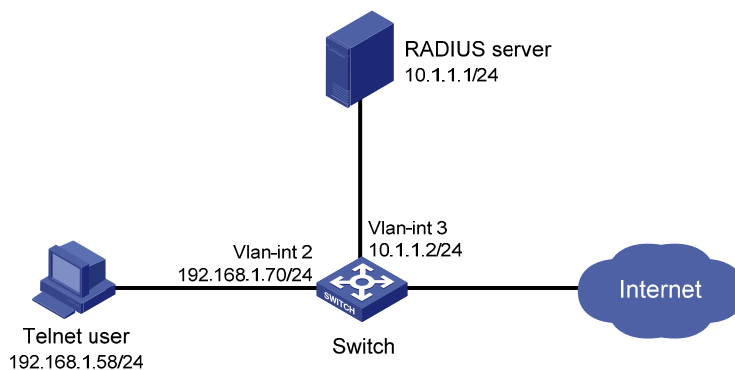
The switch in [Figure 16](#) uses the FreeRADIUS server at 10.1.1.1/24 to provide AAA service for login users, including the Telnet user at 192.168.1.58. This Telnet user uses the username **hello@bbb** and is assigned the user role **role2**.

This user role has the following permissions:

- Performs all the commands in ISP view.
- Performs read and write commands of the features **arp** and **radius**.
- Has no access to read commands of the feature **acl**.
- Configures VLANs 1 to 20 and interfaces Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/24.

The switch and the FreeRADIUS server use the shared key **expert** and authentication port 1812. The switch delivers usernames with their domain names to the server.

Figure 16 Network diagram



Configuration procedure

Make sure that the settings on the switch and the RADIUS server match.

1. Configure the switch:

Assign VLAN interface 2 an IP address from the same subnet as the Telnet user.

```
<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
```

Assign VLAN interface 3 an IP address from the same subnet as the RADIUS server.

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
```

Enable Telnet server.

```
[Switch] telnet server enable
```

Enable scheme authentication on the user interfaces for Telnet users.

```
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
[Switch-ui-vty0-15] quit
```

Create the RADIUS scheme **rad** and enter its view.

```
[Switch] radius scheme rad
```

Specify the primary server address 10.1.1.1 and the service port 1812 in the scheme.

```
[Switch-radius-rad] primary authentication 10.1.1.1 1812
```

Set the shared key to **expert** in the scheme for the switch to authenticate to the server.

```
[Switch-radius-rad] key authentication simple expert
[Switch-radius-rad] quit
```

Specify the scheme **rad** as the authentication and authorization schemes for the ISP domain **bbb**.

! IMPORTANT:

The authorization scheme must be the same as the authentication scheme to ensure successful authorization, because RADIUS does not separate authorization from authentication and sends authorization attributes in authentication responses.

```
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] quit
```

Create the feature group **fgroup1**.

```
[Switch] role feature-group name fgroup1
```

Add the features **arp** and **radius** to the feature group.

```
[Switch-featuregrp-fgroup1] feature arp
[Switch-featuregrp-fgroup1] feature radius
[Switch-featuregrp-fgroup1] quit
```

Create the user role **role2**.

```
[Switch] role name role2
```

```

# Configure rule 1 to permit the user role to use all commands available in ISP view.
[Switch-role-role2] rule 1 permit command system-view ; domain *
# Configure rule 2 to permit the user role to use read and write commands of all features in
fgroup1.
[Switch-role-role2] rule 2 permit read write feature-group fgroup1
# Configure rule 3 to disable access to the read commands of the acl feature.
[Switch-role-role2] rule 3 deny read feature acl
# Configure rule 4 to permit the user role to create VLANs and use all commands available in
VLAN view.
[Switch-role-role2] rule 4 permit command system-view ; vlan *
# Configure rule 5 to permit the user role to enter interface view and use all commands available
in interface view.
[Switch-role-role2] rule 5 permit command system-view ; interface *
# Configure the user role VLAN policy to disable configuration of any VLAN except VLANs 1 to
20.
[Switch-role-role2] vlan policy deny
[Switch-role-role2-vlanpolicy] permit vlan 1 to 20
[Switch-role-role2-vlanpolicy] quit
# Configure the user role interface policy to disable configuration of any interface except
Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/24.
[Switch-role-role2] interface policy deny
[Switch-role-role2-ifpolicy] permit interface ten-gigabitethernet 1/0/1 to
ten-gigabitethernet 1/0/24
[Switch-role-role2-ifpolicy] quit
[Switch-role-role2] quit

```

2. Configure the RADIUS server:

```

# Add either of the user role attributes to the dictionary file of the FreeRADIUS server.
Cisco-AVPair = "shell:roles=\"role2\""
Cisco-AVPair = "shell:roles*\"role2\""
# Configure the settings required for the FreeRADIUS server to communicate with the switch.
(Details not shown.)

```

Verifying the configuration

```

# Telnet to the switch, and enter the username and password to access the user interface. (Details not
shown.)
# Verify that you can use all commands available in ISP view.
<Switch> system-view
[Switch] domain abc
[Switch-isp-abc] authentication login radius-scheme abc
[Switch-isp-abc] quit
# Verify that you can use all read and write commands of the features radius and arp. Take radius as an
example.
[Switch] radius scheme rad
[Switch-radius-rad] primary authentication 2.2.2.2
[Switch-radius-rad] display radius scheme rad

```

...

Output of the RADIUS scheme is omitted.

Verify that you cannot configure any VLAN except VLANs 1 to 20. Take VLAN 10 and VLAN 30 as examples.

```
[Switch] vlan 10
[Switch-vlan10] quit
[Switch] vlan 30
Permission denied.
```

Verify that you cannot configure any interface except Ten-GigabitEthernet 1/0/1 to Ten-GigabitEthernet 1/0/24. Take Ten-GigabitEthernet 1/0/2 and Ten-GigabitEthernet 1/0/25 as examples.

```
[Switch] vlan 10
[Switch-vlan10] port ten-gigabitethernet 1/0/2
[Switch-vlan10] port ten-gigabitethernet 1/0/25
Permission denied.
```

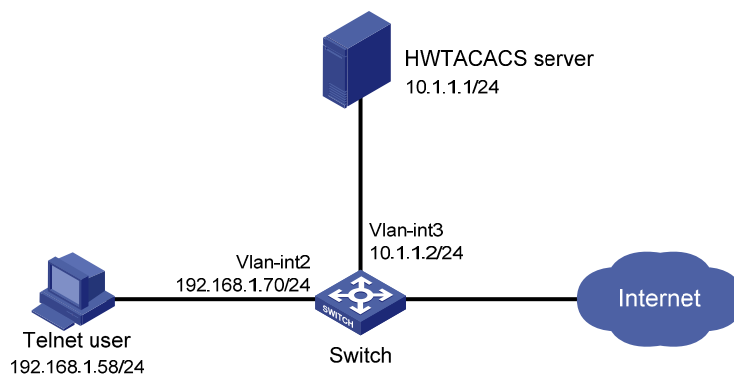
RBAC configuration example for HWTACACS authentication users

Network requirements

The switch in [Figure 17](#) uses local authentication for login users, including the Telnet user at 192.168.1.58. This Telnet user uses the username **test@bbb** and is assigned the user role **level-0**.

Configure the remote-then-local authentication mode for user role switching. The switch uses the HWTACACS server to provide authentication for user role switching among level-0 and level-3. If the AAA configuration is invalid or the HWTACACS server does not respond, the switch performs local authentication.

Figure 17 Network diagram



Configuration procedure

1. Configure the switch:
 - # Assign an IP address to VLAN-interface 2, the interface connected to the Telnet user.

```

<Switch> system-view
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.1.70 255.255.255.0
[Switch-Vlan-interface2] quit
# Assign an IP address to VLAN-interface 3, the interface connected to the HWTACACS server.
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ip address 10.1.1.2 255.255.255.0
[Switch-Vlan-interface3] quit
# Enable Telnet server.
[Switch] telnet server enable
# Enable scheme authentication on the user interfaces for Telnet users.
[Switch] user-interface vty 0 15
[Switch-ui-vty0-15] authentication-mode scheme
[Switch-ui-vty0-15] quit
# Enable remote-then-local authentication for user role switching.
[Switch] super authentication-mode scheme local
# Create the HWTACACS scheme hwtac and enter its view.
[Switch] hwtacacs scheme hwtac
# Specify the primary authentication server address 10.1.1.1 and the service port 49 in the
scheme.
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
# Set the shared key to expert in the scheme for the switch to authenticate to the server.
[Switch-hwtacacs-hwtac] key authentication simple expert
# Exclude the ISP domain name from the username sent to the HWTACACS server.
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
# Create ISP domain bbb and enter its view.
[Switch] domain bbb
# Configure ISP domain bbb to use local authentication for login users.
[Switch-isp-bbb] authentication login local
# Configure ISP domain bbb to use local authorization for login users.
[Switch-isp-bbb] authorization login local
# Apply the HWTACACS scheme hwtac to the ISP domain.
[Switch-isp-bbb] authentication super hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
# Create a management local user named test and enter its view. Set the service type to Telnet,
and set the password to aabbcc.
[Switch] local-user test class manage
[Switch-luser-manage-test] service-type telnet
[Switch-luser-manage-test] password simple aabbcc
# Assign level-0 to the user.
[Switch-luser-manage-test] authorization-attribute user-role level-0
# Delete the default user role network admin.
[Switch-luser-manage-test] undo authorization-attribute user-role network-operator

```

```
[Switch-luser-manage-test] quit
# Set the switching password to 654321 for the user role level-3.
[Switch] super password role level-3 simple 654321
[Switch] quit
```

2. Configure the HWTACACS server:

This example uses ACSv4.0.

- a. Add a user account **test**.
- b. Access the **Advanced TACACS+ Settings** page.
- c. Select **Level 3** for the **Max Privilege for any AAA Client** option.
- d. Select the **Use separate password** option, and specify **enabpass** as the password.

Figure 18 Configuring advanced TACACS+ settings

Verifying the configuration

1. Telnet to the switch, and enter the username **test@bbb** and password **aabbcc** to access the user interface. Verify that you have access to diagnostic commands.

```
<Switch> telnet 192.168.1.70
Trying 192.168.1.70 ...
```

```

Press CTRL+K to abort
Connected to 192.168.1.59 ...
*****
* Copyright (c) 2004-2012 Hewlett-Packard Development Company, L.P..      *
* Without the owner's prior written consent,                               *
* no decompiling or reverse-engineering shall be allowed.                 *
*****

login: test@bbb
Password:
<Switch>

```

2. Switch the user role:

Use the super password to switch the user role. When the system prompts for a username and password, enter the username **test@bbb** and password **enabpass**.

```
<Switch> super level-3
```

```
Username: test@bbb
```

```
Password:
```

The following output shows that you have switched the user role to level-3.

```
User privilege role is level-3, and only those commands that authorized to the role
can be used.
```

If the ACS server does not respond, enter the local authentication password **654321** at the prompt.

```
Invalid configuration or no response from the authentication server.
```

```
Change authentication mode to local.
```

```
Password:
```

```
User privilege role is level-3, and only those commands that authorized to the role
can be used.
```

The output shows that you have switched the user role to level-3.

Troubleshooting RBAC

This section describes several typical RBAC problems and their solutions.

Local users have more access permissions than intended

Symptom

A local user can use more commands than should be permitted by the assigned user roles.

Analysis

The local user might have been assigned to user roles without your knowledge. For example, the local user is automatically assigned a default user role when you create it.

Solution

Use the **display local-user** command to examine the local user accounts for undesirable user roles, and delete them.

Login attempts by RADIUS users always fail

Symptom

Attempts by a RADIUS user to log in to the network access device always fail, even though the network access device and the RADIUS server can communicate with one another and all AAA settings are correct.

Analysis

RBAC requires that a login user have at least one user role. If the RADIUS server does not authorize the login user to use any user role, the user cannot log in to the device.

Solution

Resolve the problem in one of the following ways:

- Configure the **role default-role enable** command so a RADIUS user can log in with the default user role when no user role is assigned by the RADIUS server.
- Add the user role authorization attributes on the RADIUS server.

Configuring FTP

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

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

FTP supports the following transfer modes:

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

By default, the FTP server uses ASCII mode.

FTP can operate in either of the following modes:

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

FTP operation mode varies depending on the FTP client program.

The device can act as the FTP server or FTP client. Make sure the FTP server and the FTP client can reach each other before establishing the FTP connection.

Figure 19 FTP application scenario



Using the device as an FTP server

Perform the configuration tasks in this section to configure the device as an FTP server.

Configuring basic parameters

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable the FTP server.	ftp server enable	By default, the FTP server is disabled.
3. (Optional.) Use an ACL to control access to the FTP server.	ftp server acl { acl-number ipv6 acl-number6 }	By default, no ACL is used for access control.

Step	Command	Remarks
4. (Optional.) Configure the idle-timeout interval.	ftp timeout <i>minutes</i>	The default idle-timeout interval is 30 minutes. If no data is transferred between the FTP server and FTP client within the idle-timeout interval, the connection is terminated.

Configuring authentication and authorization

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

The following authentication modes are available:

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

The following authorization modes are available:

- **Local authorization**—The device assigns authorized directories to FTP clients based on the locally configured authorization attributes.
- **Remote authorization**—A remote authorization server assigns authorized directories on the device to FTP clients.

For information about configuring authentication and authorization, see *Security Configuration Guide*.

Manually releasing FTP connections

Task	Command
Manually release FTP connections.	<ul style="list-style-type: none"> • Release the FTP connection established using a specific user account: free ftp user <i>username</i> • Release the FTP connection to a specific IP address: free ftp user-ip [ipv6] <i>client-address</i> [port <i>port-num</i>]

Displaying and maintaining the FTP server

Execute **display** commands in any view.

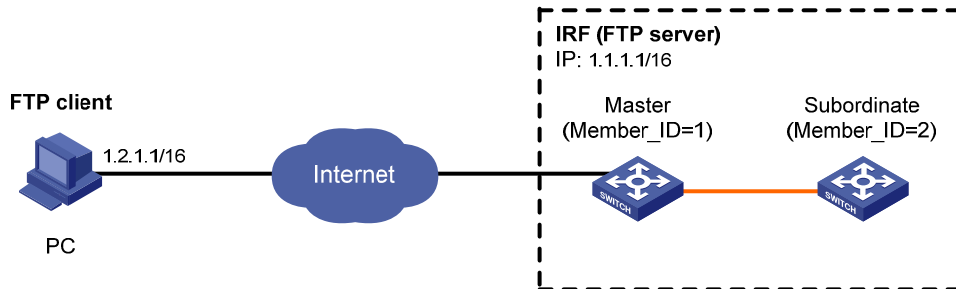
Task	Command
Display FTP server configuration and status information.	display ftp-server
Display detailed information about online FTP users.	display ftp-user

FTP server configuration example

Network requirements

Create a local user account with username **abc** and password **123456** on the FTP server. Use the user account to log in to the FTP server from the FTP client, upload the file **temp.bin** from the FTP client to the FTP server, and download the configuration file **config.cfg** from the FTP server to the FTP client for backup.

Figure 20 Network diagram



Note: The orange line represents an IRF connection.

Configuration procedure

1. Configure IP addresses as shown in Figure 20, and make sure the IRF fabric and the PC can reach each other. (Details not shown.)
2. Configure the FTP server:

Examine the storage space on the member devices for insufficiency. If the free space is insufficient, use the **delete/unreserved file-url** command to delete unused files. (Details not shown.)

Create a local user account **abc**, set the password to **123456**, the user role to **network-admin**, the working directory to the root directory of the Flash, and the service type to FTP. (To set the working directory to the Flash root directory of the subordinate member, replace **flash:/** in the **authorization-attribute** command with **slot2#flash:/**.)

```
<Sysname> system-view
[Sysname] local-user abc class manage
[Sysname-luser-abc] password simple 123456
[Sysname-luser-abc] authorization-attribute user-role network-admin work-directory flash:/
[Sysname-luser-abc] service-type ftp
[Sysname-luser-abc] quit
```

Enable the FTP server.

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

3. Perform FTP operations from the FTP client:

Log in to the FTP server at 1.1.1.1 using the username **abc** and password **123456**.

```
c:\> ftp 1.1.1.1
Connected to 1.1.1.1. (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.
# Use the ASCII mode to download the configuration file config.cfg from the FTP server to the PC
for backup.
ftp> ascii
200 TYPE is now ASCII
ftp> get config.cfg back-config.cfg
# Use the binary mode to upload the file temp.bin from the PC to the Flash root directory of the
master.
ftp> binary
200 TYPE is now 8-bit binary
ftp> put temp.bin
# Exit FTP.
ftp> bye

```

Using the device as an FTP client

Perform the configuration in this section to use the device as an FTP client.

Establishing an FTP connection

To access the FTP server, you must establish a connection from the FTP client to the FTP server.

To establish an IPv4 FTP connection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Specify a source IP address for outgoing FTP packets.	ftp client source { interface <i>interface-type interface-number</i> ip <i>source-ip-address</i> }	By default, no source IP address is specified, and the primary IP address of the output interface is used as the source IP address.
3. Return to user view.	quit	N/A
4. Log in to the FTP server.	<ul style="list-style-type: none"> (Approach 1) Log in to the FTP server directly in user view: ftp <i>server-address</i> [<i>service-port</i>] [vpn-instance <i>vpn-instance-name</i>] [source { interface { <i>interface-name</i> <i>interface-type interface-number</i> } ip <i>source-ip-address</i> }] (Approach 2) Log in to the FTP server in FTP client view: <ol style="list-style-type: none"> ftp open <i>server-address</i> [<i>service-port</i>] 	Use either approach. The source IP address specified in the ftp command takes precedence over the one set by the ftp client source command.

To establish an IPv6 FTP connection:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Specify the source IPv6 address for FTP packets sent by the FTP client.	ftp client ipv6 source { interface <i>interface-type interface-number</i> ipv6 <i>source-ipv6-address</i> }	By default, no source IPv6 address is specified. The source address is automatically selected as defined in RFC 3484.
3. Return to user view.	quit	N/A
4. Log in to the FTP server.	<ul style="list-style-type: none"> Log in to the FTP server directly in user view: ftp ipv6 <i>server-address</i> [<i>service-port</i>] [vpn-instance <i>vpn-instance-name</i>] [source { interface <i>interface-type interface-number</i> ipv6 <i>source-ipv6-address</i> }] [-i <i>interface-type interface-number</i>] Log in to the FTP server in FTP client view: <ol style="list-style-type: none"> ftp ipv6 open <i>server-address</i> [<i>service-port</i>] 	Use either approach. The source IP address specified in the ftp ipv6 command takes precedence over the one set by the ftp client ipv6 source command.

Managing directories on the FTP server

Task	Command
Display directory and file information on the FTP server.	<ul style="list-style-type: none"> Display the detailed information of a directory or file on the FTP server: dir [<i>remotefile</i> [<i>localfile</i>]] Display the name of a directory or file on the FTP server: ls [<i>remotefile</i> [<i>localfile</i>]]
Change the working directory on the FTP server.	cd { <i>directory</i> <i>..</i> <i>/</i> }
Return to the upper level directory on the FTP server.	cdup
Display the working directory that is being accessed.	pwd
Create a directory on the FTP server.	mkdir <i>directory</i>
Remove the specified working directory on the remote FTP server.	rmdir <i>directory</i>

Working with files on the FTP server

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

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

To work with files on an FTP server, execute the following commands in FTP client view:

Task	Command	Remarks
Display directory or file information on the FTP server.	<ul style="list-style-type: none"> • Display the detailed information of a directory or file on the FTP server: dir [<i>remotefile</i> [<i>localfile</i>]] • Display the name of a directory or file on the FTP server: ls [<i>remotefile</i> [<i>localfile</i>]] 	N/A
Delete the specified file on the FTP server permanently.	delete <i>remotefile</i>	N/A
Set the file transfer mode to ASCII.	ascii	The default file transfer mode is ASCII.
Set the file transfer mode to binary.	binary	The default file transfer mode is ASCII.
Set the FTP operation mode to passive.	passive	The default mode is passive.
Display or change the local working directory of the FTP client.	lcd [<i>directory</i> /]	N/A
Upload a file to the FTP server.	put <i>localfile</i> [<i>remotefile</i>]	N/A
Download a file from the FTP server.	get <i>remotefile</i> [<i>localfile</i>]	N/A
Add the content of a file on the FTP client to a file on the FTP server.	append <i>localfile</i> [<i>remotefile</i>]	N/A
Specify the retransmit marker.	restart <i>marker</i>	Use this command together with the put , get , or append command.
Update the local file.	newer <i>remotefile</i>	N/A
Get the missing part of a file.	reget <i>remotefile</i> [<i>localfile</i>]	N/A
Rename the file.	rename [<i>oldfilename</i> [<i>newfilename</i>]]	N/A

Switching to another user account

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

To switch to another user account, execute the following command in user view:

Task	Command
Switch to another user account.	user <i>username</i> [<i>password</i>]

Maintaining and troubleshooting the FTP connection

Task	Command	Remarks
Display FTP commands on the FTP server.	rhelp	N/A
Display FTP commands help information on the FTP server.	rhelp <i>protocol-command</i>	N/A
Display FTP server status.	rstatus	N/A
Display the detailed information of a specified directory or file on the FTP server.	rstatus <i>remotefile</i>	N/A
Display FTP connection status.	status	N/A
Display the system information of the FTP server.	system	N/A
Enable or disable FTP operation information display.	verbose	By default, this function is enabled.
Enable or disable FTP client debugging.	debug	By default, FTP client debugging is disabled.
Clear the reply information in the buffer.	reset	N/A

Terminating the FTP connection

Task	Command	Remarks
Terminate the connection to the FTP server without exiting FTP client view.	<ul style="list-style-type: none">• disconnect• close	Use either command in FTP client view.
Terminate the connection to the FTP server and return to user view.	<ul style="list-style-type: none">• bye• quit	Use either command in FTP client view.

Displaying command help information

To display command help information after you log in to the server:

Task	Command	Remarks
Display command help information	<ul style="list-style-type: none"> • help [<i>command-name</i>] • ? [<i>command-name</i>] 	Use either command.

Displaying and maintaining FTP client

Execute the **display** command in any view.

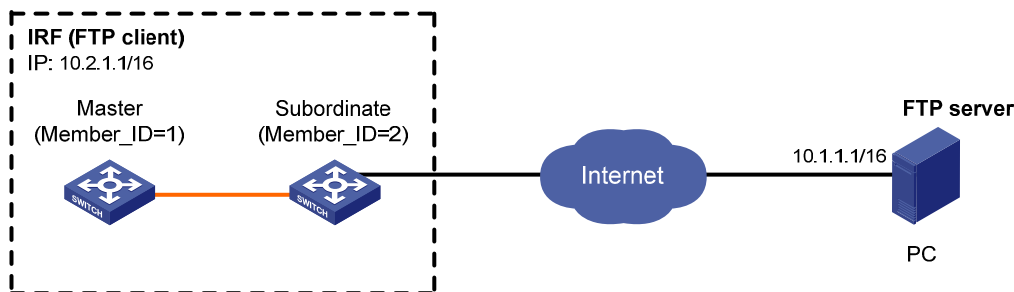
Task	Command
Display source IP address information on the FTP client	display ftp client source

FTP client configuration example

Network requirements

- Use the IRF fabric that comprises two member devices as the FTP client and the PC as the FTP server.
- Log in to the FTP server from the FTP client using the user account with the username **abc** and password **123456** (which has been created on the PC).
- Download the file **temp.bin** from the FTP server to the FTP client, and upload the configuration file **config.cfg** from the FTP client to the FTP server for backup.

Figure 21 Network diagram



Note: The orange line represents an IRF connection.

Configuration procedure

Configure IP addresses as shown in Figure 21 and make sure the IRF fabric and PC can reach each other. (Details not shown.)

Examine the storage space on the member devices for insufficiency. If the free space is insufficient, use the **delete/unreserved file-url** command to delete unused files. (Details not shown.)

Log in to the FTP server at 10.1.1.1 using the username **abc** and password **123456**.

```
<Sysname> ftp 10.1.1.1
Connected to 10.1.1.1 (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
Remote system type is MSDOS.
ftp>

# Set the file transfer mode to binary.
ftp> binary
200 TYPE is now 8-bit binary

# Download the file temp.bin from the PC to the Flash root directory of the master device.
ftp> get temp.bin
local: temp.bin remote: temp.bin
150 Connecting to port 47457
226 File successfully transferred
23951480 bytes received in 95.399 seconds (251.0 kbyte/s)

# Download the file temp.bin from the PC to the Flash root directory of the subordinate member (with member ID of 2).
ftp> get temp.bin slot2#flash:/temp.bin

# Set the transfer mode to ASCII and upload the configuration file config.cfg from the IRF fabric to the PC for backup.
ftp> ascii
200 TYPE is now ASCII
ftp> put config.cfg back-config.cfg
local: config.cfg remote: back-config.cfg
150 Connecting to port 47461
226 File successfully transferred
3494 bytes sent in 5.646 seconds (618.00 kbyte/s)
ftp> bye
221-Goodbye. You uploaded 2 and downloaded 2 kbytes.
221 Logout.
<Sysname>
```


Configuring TFTP

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

The device can only operate as a TFTP client. You can upload a file from the device to the TFTP server or download a file from the TFTP server to the device. If you download a file with a file name that exists in the target directory, the device deletes the existing file and saves the new one. If file download fails due to network disconnection or other reasons, the original file cannot be restored. Therefore, use a nonexistent file name instead.

Figure 22 TFTP application scenario



Configuring the device as an IPv4 TFTP client

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Use an ACL to control the client's access to TFTP servers.	fttp-server acl <i>acl-number</i>	By default, no ACL is used for access control.
3. Specify the source IP address for TFTP packets sent by the TFTP client.	fttp client source { interface <i>interface-type interface-number</i> ip <i>source-ip-address</i> }	By default, no source IP address is specified, and the primary IP address of the output interface is used as the source IP address.
4. Return to user view.	quit	N/A
5. Download or upload a file in an IPv4 network.	fttp server-address { get put } <i>source-filename</i> [<i>destination-filename</i>] [vpn-instance <i>vpn-instance-name</i>] [source { interface <i>interface-type interface-number</i> ip <i>source-ip-address</i> }]	The source IP address specified in this command takes precedence over the one set by the fttp client source command. Use this command in user view.

Configuring the device as an IPv6 TFTP client

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Use an ACL to control the client's access to TFTP servers.	tftp-server ipv6 acl <i>acl-number</i>	By default, no ACL is used for access control.
3. Specify the source IPv6 address for TFTP packets sent by the TFTP client.	tftp client ipv6 source { interface <i>interface-type interface-number</i> ipv6 <i>source-ip-address</i> }	By default, no source IPv6 address is specified. The source address is automatically selected as defined in RFC 3484.
4. Return to user view.	quit	N/A
5. Download or upload a file in an IPv6 network.	tftp ipv6 <i>tftp-ipv6-server</i> [-i <i>interface-type interface-number</i>] { get put } <i>source-filename</i> [<i>destination-filename</i>] [vpn-instance <i>vpn-instance-name</i>] [source { interface <i>interface-type interface-number</i> ipv6 <i>source-ipv6-address</i> }]	The source IP address specified in this command takes precedence over the one set by the tftp client ipv6 source command. Use this command in user view.

Managing the file system

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

! IMPORTANT:

- Before managing storage media, files, and directories, make sure you know the possible impacts.
- A file or directory whose name starts with a period (.) is considered a hidden file or directory. Do not give a common file or directory a name that starts with a period.
- Some system files and directories are hidden. For proper system operation, do not modify or delete hidden files or directories.

File name formats

When you specify a file, enter the file name in one of the formats shown in Table 11. When you specify a directory, follow the rules for the *drive* and *path* arguments.

Table 11 File name formats

Format	Description	Example
<i>file-name</i>	Specifies a file in the current working directory.	a.cfg indicates a file named a.cfg in the current working directory. This working directory might be on the master device or a subordinate device.
<i>[path/]file-name</i>	Specifies a file in a specific folder in the current working directory. The <i>path</i> argument represents the path to the file. If the file is in a single-level folder, specify the folder name for the argument. If the file is in a nested folder, separate each folder name by a forward slash (/).	<ul style="list-style-type: none">• test/a.cfg indicates a file named a.cfg in the test folder in the current working directory.• test/subtest/a.cfg indicates a file named a.cfg in the subtest subfolder of the test folder in the current working directory.
<i>drive:/[path]/file-name</i>	Specifies a file in a specific storage medium on the device. The <i>drive</i> argument represents the storage medium name. The storage medium on the master is flash. The storage medium on a subordinate device is slotn#flash, where <i>n</i> represents the member ID of the subordinate device, for example, slot2#flash. To view the correspondence between a member device and its member ID, use the display irf command.	<ul style="list-style-type: none">• flash:/test/a.cfg indicates a file named a.cfg under the test folder in the root directory of the master's Flash memory.• slot2#flash: a.cfg indicates a file named a.cfg in the root directory of the Flash on the member device 2.

Managing files

CAUTION:

To avoid file system corruption, do not install or remove storage media or perform master/subordinate switchover during file operations.

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

You can create a file by copying, downloading, or using the **save** command. For more information about downloading a file, see "Configuring FTP" and "Configuring TFTP." For more information about the **save** command, see *Fundamentals Command Reference*.

Before you rename, compress, decompress, delete, or move a file on a USB disk, or copy a file to a USB disk, make sure the disk is not write protected.

Displaying file information

Perform this task in user view.

Task	Command
Display folder or file information.	dir [/all] [file-url /all-filestems]

Displaying the contents of a text file

Perform this task in user view.

Task	Command
Display the contents of a text file.	more file-url

Renaming a file

Perform this task in user view.

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

Copying a file

Perform this task in user view.

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

Moving a file

Perform this task in user view.

Task	Command
Move a file.	<code>move fileurl-source fileurl-dest</code>

Compressing/decompressing a file

Perform the following tasks in user view:

Task	Command
Compress a file.	<code>gzip filename</code>
Decompress a file.	<code>gunzip filename</code>

Deleting/restoring a file

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

Files in the recycle bin occupy storage space. To release the occupied space, execute the **reset recycle-bin** command in user view. To save storage space, periodically empty the recycle bin with the **reset recycle-bin** command.

Perform the following tasks in user view:

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

ⓘ IMPORTANT:

Do not use the **delete** command to delete files from the recycle bin. To delete files from the recycle bin, use the **reset recycle-bin** command.

Deleting files from the recycle bin

The Flash memory has a recycle bin named **.trash**. To view which files or directories are in the recycle bin, use either of the following methods:

- Enter the storage medium and execute the **dir/all .trash** command.
- Execute the **cd .trash** command to enter the recycle bin folder and then execute the **dir** command.

To delete files from a recycle bin, perform the following task in user view:

Task	Command
Delete files from the recycle bin.	<code>reset recycle-bin [/force]</code>

Managing directories

△ CAUTION:

To avoid file system corruption, do not install or remove storage media or perform master/subordinate switchover during directory operations.

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

Before you create or remove a directory on a USB disk, make sure the disk is not write protected.

Displaying the current working directory

Perform this task in user view.

Task	Command
Display the current working directory.	<code>pwd</code>

Changing the current working directory

Perform this task in user view.

Task	Command
Change the current working directory.	<code>cd { directory .. / }</code>

Creating a directory

Perform this task in user view.

Task	Command
Create a directory.	<code>mkdir directory</code>

Removing a directory

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

Removing a directory permanently deletes all its files in the recycle bin, if any.

Perform this task in user view.

Task	Command
Remove a directory.	<code>rmdir directory</code>

Managing storage media

Before you repair or format a USB disk, make sure the disk is not write protected.

Repairing a storage medium

If part of a storage medium is inaccessible, use the **fixdisk** command to examine the medium for any damage and repair the medium.

Before repairing a storage medium, make sure no other users are accessing the medium. Otherwise, the repair operation fails.

Perform this task in user view.

Task	Command
Repair a storage medium.	fixdisk <i>medium-name</i>

Formatting a storage medium

CAUTION:

After a storage medium is formatted, all files and directories on it are erased and cannot be restored.

Perform this task in user view.

Task	Command
Format a storage medium.	format <i>medium-name</i>

Setting the operation mode for files and folders

The device supports the following file and folder operation modes:

- **alert**—The system warns you about operations that might cause problems such as file corruption and data loss. To avoid operation mistakes, use the **alert** mode.
- **quiet**—The system does not prompt for confirmation.

To set the operation mode for files and folders:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the operation mode for files and folders.	file prompt { alert quiet }	The default mode is alert .

Managing configuration files

You can use the CLI or the Boot menu to manage configuration files. This chapter describes the CLI approach to configuration file management.

Overview

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

Configuration types

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

Factory defaults

The device is shipped with some basic settings called "factory defaults." These default settings make sure the device can start up and run normally when it has no configuration file or the configuration file is corrupted.

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

To view factory defaults, use the **display default-configuration** command.

Startup configuration

The device uses startup configuration to configure software features during startup. After the device starts up, you can specify a different configuration file to be loaded at the next startup. This configuration file is called the "next-startup configuration file." The configuration file that has been loaded is called the "current startup configuration file."

If no next-startup configuration file exists, the device boots with the factory defaults.

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

- Execute the **display startup** command. To view detailed file contents, use the **more** command.
- After the device reboots, execute the **display current-configuration** command before making any configuration.

Running configuration

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

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

To view the running configuration, use the **display current-configuration** command.

Next-startup configuration file redundancy

You can specify one main next-startup configuration file and one backup next-startup configuration file for redundancy.

At startup, the device tries to start up with the main configuration file. If the main configuration file is corrupted or unavailable, the device tries the backup configuration file. If the backup configuration file is corrupted or unavailable, the device starts up with the factory defaults.

For reliability, do not specify one configuration file as both the main and backup configuration files.

Configuration file formats

Configuration files you specify for saving configuration must use the .cfg extension. A .cfg configuration file is a human-readable text file. When you save configuration to a .cfg file, the device automatically saves the configuration to an .mdb user-inaccessible binary file that has the same name as the .cfg file. The device loads an .mdb file faster than loading a .cfg file.

Startup configuration file selection

At startup, the device uses the following procedure to identify the configuration file to load:

1. Searches for a valid .cfg next-startup configuration file.
2. If one is found, searches for an .mdb file that has the same name and content as the .cfg file.
3. If an .mdb file has the same name and content as the .cfg file, starts up with the .mdb file. If none is found, starts up with the .cfg file.

Unless otherwise stated, the term "configuration file" in this document refers to a .cfg configuration file.

Configuration file content organization and format

ⓘ IMPORTANT:

To run on the device, a configuration file must meet the content and format requirements of the device. To avoid any configuration loading problem at startup, use a configuration file created on the device. If you edit the configuration file, make sure all edits are compliant with the requirements of the device.

A configuration file must meet the following requirements:

- All commands are saved in their complete form.
- Commands are sorted in sections by command view, typically in this order: system view, interface view, protocol views, and user interface view.
- Two adjacent sections are separated by a comment line that starts with a pound sign (#).
- The configuration file ends with the word **return**.

The following is a sample configuration file excerpt:

```
#
  version 7.1.035, ESS 2205
#
  sysname HP
#
  ftp server enable
#
  telnet server enable
#
  irf mac-address persistent timer
  irf auto-update enable
```

```
irf link-delay 0
irf member 2 priority 1
```

Enabling configuration encryption

Configuration encryption enables the device to automatically encrypt a startup configuration file when saving the running configuration. This function has the following approaches:

- **Private key approach**—Only the encrypting device can decrypt the encrypted configuration file.
- **Public key approach**—Any device running the same software version as the encrypting device can decrypt the encrypted configuration file.

ⓘ IMPORTANT:

Do not move or copy a private-key-encrypted configuration file between IRF member devices. Doing so can cause a decryption failure, because the member devices use different private keys..

To enable configuration encryption:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable configuration encryption.	configuration encrypt { private-key public-key }	By default, configuration encryption is disabled. Configuration is saved unencrypted.

Saving the running configuration

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

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

- **Fast mode**—Use the **save** command without the **safely** keyword. In this mode, the device directly overwrites the target next-startup configuration file. If a reboot or power failure occurs during this process, the next-startup configuration file is lost. You must specify a new startup configuration file after the device reboots (see "[Specifying a next-startup configuration file](#)").
- **Safe mode**—Use the **save** command with the **safely** keyword. Safe mode is slower than fast mode, but more secure. In safe mode, the system saves configuration in a temporary file and starts overwriting the target next-startup configuration file after the save operation is complete. If a reboot or power failure occurs during the save operation, the next-startup configuration file is still retained.

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

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

Task	Command
Save the running configuration to a configuration file without specifying the file as a next-startup configuration file.	save file-url

Task	Command
Save the running configuration to a configuration file and specify the file as a next-startup configuration file.	<code>save [safely] [backup main] [force]</code>

Configuring configuration rollback

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

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

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

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

Configuration task list

Tasks at a glance
(Required.) Configuring configuration archive parameters
(Required.) Perform either task: <ul style="list-style-type: none"> • Enabling automatic configuration archiving • Manually archiving the running configuration
(Required.) Performing a configuration rollback

Configuring configuration archive parameters

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

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

After you change the file directory or file name prefix, or reboot the device, the old configuration archives are regarded as common configuration files, the configuration archive counter resets, and the **display archive configuration** command no longer displays them. The serial number for new configuration archives starts at 1.


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

Configuration guidelines

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

Configuration procedure

To configure configuration archive parameters:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the directory and file name prefix for archiving the running configuration.	archive configuration location <i>directory filename-prefix</i> <i>filename-prefix</i>	Do not include member ID information in the directory name. By default, no path or file name prefix is set for configuration archives, and the system does not regularly save configuration.  IMPORTANT: The undo form of this command disables both manual and automatic configuration archiving, restores the default settings for the archive configuration interval and archive configuration max commands, and deletes all saved configuration archives.
3. (Optional.) Set the maximum number of configuration archives.	archive configuration max <i>file-number</i>	The default number is 5. Change the setting depending on the amount of storage available on the device.

Enabling automatic configuration archiving

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

- If the device configuration does not change frequently, manually archive the running configuration as needed.
- If the device configuration changes frequently, configure automatic archiving with an interval longer than 1440 minutes (24 hours).

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

To enable automatic configuration archiving:

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

Step	Command	Remarks
2. Enable automatic configuration archiving and set the archiving interval.	archive configuration interval <i>minutes</i>	By default, this function is disabled. To view configuration archive names and their archiving time, use the display archive configuration command.

Manually archiving the running configuration

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

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

Perform the following task in user view:

Task	Command
Manually archive the running configuration.	archive configuration

Performing a configuration rollback

To avoid a rollback failure, follow these guidelines:

- Make sure the replacement configuration file is created by using the configuration archive function or the **save** command on the local device.
- If the configuration file is not created on the local device, make sure the configuration file content format is fully compatible with the local device.
- The replacement configuration file is not encrypted.

To perform a configuration rollback:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Roll the running configuration back to the configuration defined by a configuration file.	configuration replace file <i>filename</i>	The specified configuration file must not be encrypted.

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

- A command cannot be undone because prefixing the **undo** keyword to the command does not result in a valid **undo** command. For example, if the **undo** form designed for the **A [B] C** command is **undo A C**, the configuration rollback function cannot undo the **A B C** command, because the system does not recognize the **undo A B C** command.

- A command (for example, a hardware-dependent command) cannot be deleted, overwritten, or undone due to system restrictions.
- The commands in different views are dependent on each other.
- Commands or command settings that the device does not support cannot be added to the running configuration.

Specifying a next-startup configuration file

△ CAUTION:

In an IRF fabric, use the **undo startup saved-configuration** command with caution. This command can cause an IRF split after the IRF fabric or an IRF member reboots.

You can specify a .cfg configuration file as a main or backup next-startup configuration file when using the **save [safely] [backup | main] [force]** command to save the running configuration.

Alternatively, you can execute the **startup saved-configuration *cfgfile* [backup | main]** command to specify a configuration file as the main or backup next-startup configuration file. When performing this task, follow these guidelines:

- Make sure the specified configuration file is valid and saved to the root directory of each member device's storage medium.
- If neither **backup** nor **main** is specified, this command sets the configuration file as the main next-startup configuration file.
- Even though the main and backup next-startup configuration files can be the same one, specify them as separate files for high availability.
- The **undo startup saved-configuration** command changes the attribute of the main or backup next-startup configuration file to NULL instead of deleting the file.

To specify a next-startup configuration file, perform the following task in user view:

Task	Command	Remarks
Specify a next-startup configuration file.	startup saved-configuration <i>cfgfile</i> [backup main]	Use the display startup command and the display saved-configuration command in any view to verify the configuration.

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

Before performing this task, make sure the server is reachable and enabled with TFTP service, and you have read and write permissions.

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

Step	Command	Remarks
1. (Optional.) Verify that a next-startup configuration file has been specified in user view.	display startup	If no next-startup configuration file has been specified, the backup operation will fail.
2. Back up the next-startup configuration file to a TFTP server in user view.	backup startup-configuration to <i>tftp-server [dest-filename]</i>	N/A

Restoring the main next-startup configuration file from a TFTP server

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

Before restoring the next-startup configuration file, make sure the server is reachable, the server is enabled with TFTP service, and you have read and write permissions.

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

Step	Command
1. Restore the main next-startup configuration file from a TFTP server in user view.	restore startup-configuration from <i>tftp-server src-filename</i>
2. (Optional.) Verify that the specified configuration file has been set as the main next-startup configuration file.	display startup display saved-configuration

Deleting a next-startup configuration file

CAUTION:

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

You can delete the main, the backup, or both.

To delete a file that is set as both main and backup next-startup configuration files, you must execute both the **reset saved-configuration backup** command and the **reset saved-configuration main** command. Whichever command is executed first, the system removes the specific file attribute instead of deleting the file. For example, if the **reset saved-configuration backup** command is executed first, the backup next-startup configuration file setting is set to NULL, but the file is still used as the main file. To delete the file, you must execute the **reset saved-configuration main** command.

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

- After you upgrade system software, the file no longer matches the new system software.
- The file has been corrupted or is not fully compatible with the device.

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

Perform the following task in user view:

Task	Command	Remarks
Delete next-startup configuration files.	reset saved-configuration [backup main]	If neither backup nor main is specified, this command deletes the main next-startup configuration file.

Displaying and maintaining configuration files

Execute **display** commands in any view.

Task	Command
Display information about configuration rollback.	display archive configuration
Display the running configuration.	display current-configuration [configuration [<i>module-name</i>] interface [<i>interface-type</i> [<i>interface-number</i>]]]
Display the factory defaults.	display default-configuration
Display the contents of the main next-startup configuration file.	display saved-configuration
Display names of the configuration files used at this startup and the next startup.	display startup
Display the valid configuration in the current view.	display this

Upgrading software

This chapter describes types of software and how to upgrade software from the CLI in the non-ISSU approach. For a comparison of all software upgrade methods, see "[Upgrade methods](#)."

Overview

Software upgrade enables you to have new features and fix bugs. Before performing an upgrade, use the release notes for the new software version to verify software and hardware compatibility and evaluate upgrade impacts.

Software types

The following software types are available:

- **Boot ROM image**—A .bin file that comprises a basic section and an extended section. The basic section is the minimum code that bootstraps the system. The extended section enables hardware initialization and provides system management menus. You can use these menus to load application software and the startup configuration file or manage files when the device cannot correctly start up.
- **Comware image**—Includes the following image subcategories:
 - **Boot image**—A .bin file that contains the Linux operating system kernel. It provides process management, memory management, file system management, and the emergency shell.
 - **System image**—A .bin file that contains the minimum feature modules required for device operation and some basic features, including device management, interface management, configuration management, and routing.
 - **Patch packages**—Irregularly released packages for fixing bugs without rebooting the device. A patch package does not add new features or functions.

Comware software images that have been loaded are called "current software images."

Comware images specified to load at the next startup are called "startup software images."

Boot ROM image, boot image, and system image are required for the system to work. These images might be released separately or as a whole in one .ipe package file. If an .ipe file is used, the system automatically decompresses the file, loads the .bin boot and system images and sets them as startup software images. Typically, the Boot ROM and startup software images for the device are released in an .ipe file named **main.ipe**.

Software file naming conventions

This document uses **boot.bin** and **system.bin** to represent boot and system image names, whereas the actual software image name format is *chassis_software_platform_version_image_type_release*, for example, 5920_5900-cmw710-boot-e2107.bin and 5920_5900-cmw710-system-e2107.bin.

Comware image redundancy and loading procedure

You can specify two sets of Comware software images: one main and one backup.

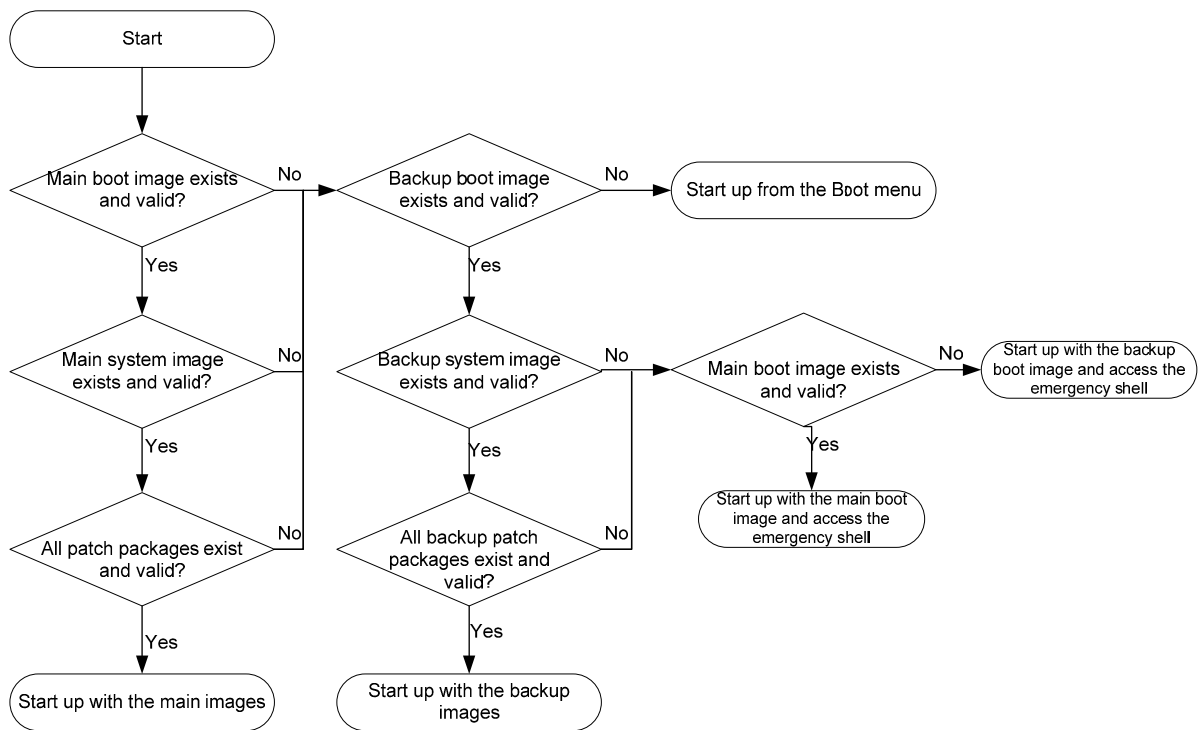
The system always attempts to start up with the main images. If any main image does not exist or is invalid, the system tries the backup images. Figure 23 shows the entire Comware image loading procedure.

This procedure assumes that the main image set and the backup image set have patch packages. If an image set does not have patch packages, the system can use the image set to start up after the boot image and the system image passes verification.

If neither the main boot image nor the backup boot image exists or is valid, connect to the console port and re-power on the device to access the Boot menu for loading a boot image. For more information about downloading and loading a boot image, see the specific release notes.

After accessing the emergency shell, connect to the console port and load a system image so you can access the Comware system. For more information about using the emergency shell, see "Using the emergency shell."

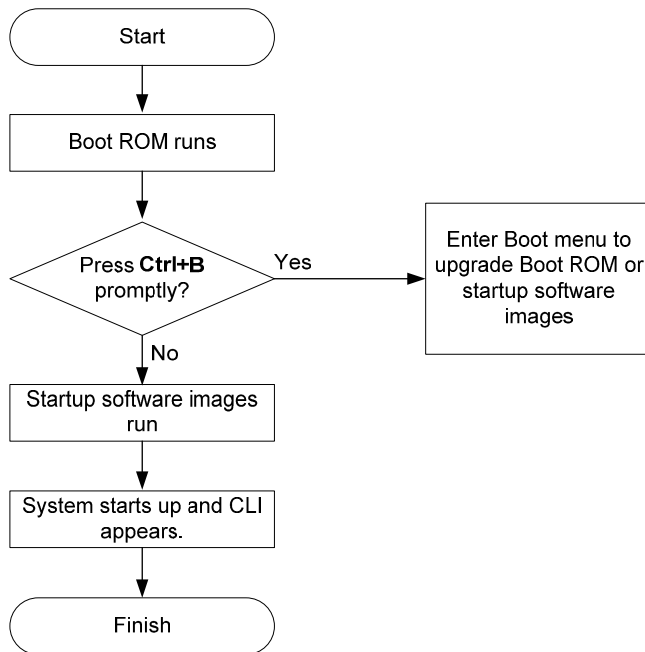
Figure 23 Comware image loading procedure



System startup process

Upon power-on, the Boot ROM image runs to initialize hardware, and then the startup software images run to start up the entire system, as shown in Figure 24. To access the Boot menu, you must press **Ctrl+B** within 1 second at the prompt.

Figure 24 System startup process



Upgrade methods

Upgrading method	Software types	Remarks
Upgrading from the CLI:		
Non-ISSU approach	<ul style="list-style-type: none"> • Boot ROM image • Comware images (excluding patches) 	You must reboot the entire device to complete the upgrade. This approach causes service interruption.
ISSU approach	Comware images	<p>The ISSU approach enables a software upgrade without service interruption.</p> <p>Use this approach for an IRF fabric.</p> <p>For more information about ISSU, see "Performing ISSU."</p>
Upgrading from the Boot menu	<ul style="list-style-type: none"> • Boot ROM image • Comware software images 	<p>Use this method when the device cannot correctly start up.</p> <p>! IMPORTANT:</p> <p>Upgrade an IRF fabric from the CLI rather than the Boot menu.</p> <p>The Boot menu approach requires that you upgrade the member devices one by one and has a larger impact on services than the CLI approach.</p>

This chapter covers only the non-ISSU approach to upgrading software from the CLI.

Non-ISSU upgrade procedure summary

To upgrade software in the non-ISSU approach:

1. Download the upgrade software image file.
2. (Optional.) Preload the Boot ROM image to the Boot ROM.
If a Boot ROM upgrade is required, you can perform this task to shorten the subsequent upgrade time. This task helps avoid upgrade problems caused by unexpected electricity failure.
If you skip this task, the device automatically upgrades the Boot ROM when upgrading the startup software images.
The Boot ROM image preloaded into the Boot ROM does not affect the device running status.
3. Specify the image file as the startup software image file.
4. If you are upgrading a standalone device, reboot the device. If you are upgrading an IRF fabric, reboot the entire IRF fabric.
5. Verify the upgrade.

Preparing for the upgrade

1. Use the **display version** command to verify the current Boot ROM image version and startup software version.
2. Use the release notes for the upgrade software version to evaluate the upgrade impact on your network and verify the following items:
 - Software and hardware compatibility
 - Version and size of the upgrade software
 - Compatibility of the upgrade software with the current Boot ROM image
3. Use the **dir** command to verify that all IRF member devices have sufficient Flash memory for the upgrade images, and use the **delete** command to delete unused files. For more information, see "Managing the file system."
4. Configure FTP and TFTP settings.
5. Use FTP or TFTP to download the upgrade image file to the root directory of Flash memory on the master device.

For more information about FTP and TFTP configuration and operations, see "Configuring FTP" or "Configuring TFTP."

Preloading the Boot ROM image to Boot ROM

Step	Command	Remarks
1.	Load the upgrade Boot ROM image from the root directory of Flash memory to the Normal area of Boot ROM. bootrom update file <i>file-url</i> slot <i>slot-number-list</i>	Specify the downloaded software image file for the <i>file-url</i> argument. The new Boot ROM image takes effect at a reboot.

Specifying the startup image file and completing the upgrade

Perform this task in user view.

Step	Command	Remarks
1. Specify the upgrade file as the main startup image file for the master device.	Approach 1: boot-loader file <i>ipe-filename</i> slot <i>slot-number</i> { backup main } Approach 2: boot-loader file boot <i>boot-package</i> system <i>system-package</i> slot <i>slot-number</i> { backup main }	Use either command. You can also specify a backup startup image file. In approach 1, the file name must take the <i>storage-medium:/base-filename.ipe</i> format, for example, <i>flash:/startup.ipe</i> . In approach 2, all file names must take the <i>storage-medium:/base-filename.bin</i> format, for example, <i>flash:/startup-boot.bin</i> .

Step	Command	Remarks
2. Specify main startup images for each subordinate device.	<p>Approach 1: boot-loader file <i>ipe-filename</i> slot <i>slot-number</i> { backup main }</p> <p>Approach 2: boot-loader file boot <i>boot-package</i> system <i>system-package</i> slot <i>slot-number</i> { backup main }</p> <p>Approach 3: boot-loader update slot <i>slot-number</i></p>	<p>Use one of the approaches. For more information about the upgrade methods provided by these commands, see <i>Fundamentals Command Reference</i>.</p> <p>Skip this step if you have only one device.</p> <p>In approach 3:</p> <ul style="list-style-type: none"> • If the master device has started up with main startup images, its main startup images are synchronized to the subordinate devices, regardless of whether any change has been made to this set of startup images. • If the master device has started up with backup startup images, its backup startup images are synchronized to the subordinate devices, regardless of whether any change has been made to this set of startup images. • Startup image synchronization fails if any software image being synchronized is not available or has been corrupted. • If a patch installation or software upgrade has been performed in ISSU approach, use the install commit command to update the set of main startup images on the master device before software synchronization for startup image consistency among IRF member devices.
3. Save the running configuration.	save	This step makes sure any configuration you have made can survive a reboot.
4. Reboot the IRF fabric.	reboot	At startup, each device reads the preloaded Boot ROM image to RAM, loads the startup images in the file, and sets the images as both current software images and startup software images.
5. (Optional.) Verify the software image settings.	display boot-loader [slot <i>slot-number</i>]	Verify that the current software images are the same as the startup software images.

Displaying and maintaining software image settings

Execute **display** commands in any view.

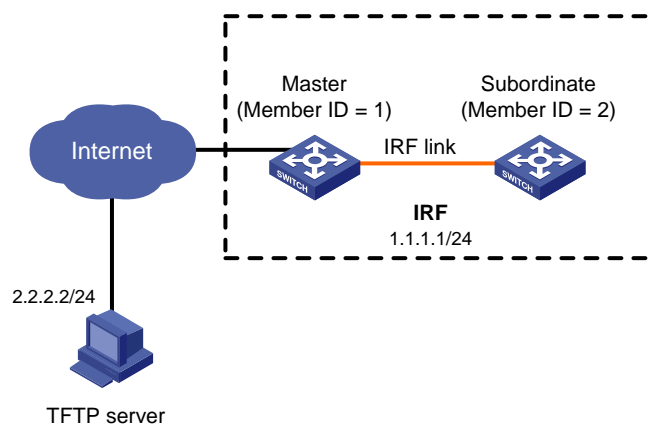
Task	Command
Display current software images and startup software images.	display boot-loader [slot slot-number]

Non-ISSU software upgrade example

Network requirements

Use the file **startup-a2105.ipe** to upgrade software images for the IRF fabric in [Figure 25](#).

Figure 25 Network diagram



Configuration procedure

Configure IP addresses and routes to make sure the device and the TFTP server can reach each other. (Details not shown.)

Complete TFTP settings on both the device and the TFTP server. (Details not shown.)

Display information about the current software images.

```
<Sysname> display version
```

Use TFTP to download the image file **startup-a2105.ipe** from the TFTP server to the root directory of Flash memory on the master device.

```
<Sysname> tftp 2.2.2.2 get startup-a2105.ipe
```

(Optional.) Back up the image file to **startup-a2105-backup.ipe**. Skip this step if the Flash memory does not have sufficient space.

```
<Sysname> copy startup-a2105.ipe startup-a2105_backup.ipe
```

Specify **startup-a2105.ipe** as the main startup image file for all IRF member devices.

```
<Sysname> boot-loader file flash:/startup-a2105.ipe slot 1 main
<Sysname> boot-loader file flash:/startup-a2105.ipe slot 2 main
# Specify startup-a2105-backup.ipe as the backup startup image file for all IRF member devices.
<Sysname> boot-loader file flash:/startup-a2105-backup.ipe slot 1 backup
<Sysname> boot-loader file flash:/startup-a2105-backup.ipe slot 2 backup
# Verify the startup image settings.
<Sysname> display boot-loader
# Reboot the IRF fabric to complete the upgrade.
<Sysname> reboot
# Verify that the IRF fabric is running the correct software.
<Sysname> display version
```


ISSU overview

The In-Service Software Upgrade (ISSU) function enables a fast software upgrade without (or with the least) service interruption. During an ISSU, you can perform version rollback and use **display** commands to view the version compatibility and upgrade status.

ISSU is implemented on the basis of the following design advantages:

- Image separation. The software of the device includes a boot image, a system image, and some patch images (if any). You can upgrade these images separately.
- Support for hotfix. By installing patch images, you can fix system bugs without rebooting the device.
- Hardware redundancy. When the master needs to reboot for an upgrade, a subordinate member in the IRF fabric can take over to ensure service continuity.

For more information about images, see "Upgrading software."

ISSU methods

Before an ISSU, you can use the **display version comp-matrix file** command to view the compatibility between the old and new software versions and the recommended ISSU method for the upgrade (indicated by the **Upgrade Way** field). Different ISSU methods require different upgrade procedures and have different impact on the current services.

Table 12 shows the ISSU methods available for different scenarios.

Table 12 ISSU methods

ISSU method	Application scenario	Value of the Upgrade Way field output by the display command
Incremental upgrade	Service-level	Service Upgrade
	File-level	File Upgrade
ISSU reboot	Upgrade to a compatible version	ISSU Reboot
Reboot	Upgrade to a compatible version	Reboot
Incompatible upgrade	Upgrade to an incompatible version	Incompatible upgrade

ISSU methods for a compatible version

The following are ISSU methods for a compatible version:

- Incremental upgrade
An incremental upgrade analyzes the differences between the new and old software versions and upgrades only the different parts. An incremental upgrade takes the least time and imposes the least effect on the device.
Incremental upgrade methods include:

- **Service-level incremental upgrade**—This method involves only the upgraded service modules. The other service modules provide services normally during the upgrade.
- **File-level incremental upgrade**—This method involves only hidden system program files. The system operates and provides services normally during the upgrade.
- ISSU reboot

An ISSU reboot upgrade saves the current system information (including the operation data, configuration data, hardware data, and status information) to the memory and uses the new software to reboot the CPU. During an ISSU reboot upgrade, the data forwarding plane of the system keeps forwarding packets. After startup, the CPU continues to provide services on the basis of the saved system information. For services that require regular protocol message exchanges to maintain connections, this method starts protocol agents to satisfy the requirements.

Compared with an incremental upgrade, an ISSU reboot upgrade affects all modules that use the CPU and takes a longer time. An ISSU reboot upgrade is usually performed when the new and old software versions are partially compatible.
- Reboot

This method reboots member devices to load the new software:

 - When the IRF fabric has more than one member and both the master and the subordinate members need to be rebooted for the upgrade, to implement in-service upgrade, upgrade subordinate members first and make sure one upgraded subordinate member will become the master when you upgrade the master.
 - When the IRF fabric has only one member, service interruption is unavoidable during the upgrade, and you can upgrade the IRF fabric by using the reboot upgrade procedure described in this chapter or that described in "Upgrading software."

ISSU method for an incompatible version

Only one method is available for an ISSU to an incompatible version, the incompatible upgrade method. This method reboots member devices to load the new software:

- When the IRF fabric has more than one member and both the master and the subordinate members need to be rebooted for the upgrade, to implement in-service upgrade, upgrade subordinate members first and make sure one upgraded subordinate member will become the master when you upgrade the master.
- When the IRF fabric has only one member, service interruption is unavoidable during the upgrade, and you can upgrade the IRF fabric by using the incompatible upgrade procedure described in this chapter or that described in "Upgrading software."

ISSU command series

To perform an ISSU, you can use either of the **install** series commands or the **issu** series commands. Table 13 compares these two series of commands.

Table 13 Comparison between the two series of commands

Item	issu series commands	install series commands
Required compatibility between the old and new software versions	Compatible or incompatible.	Compatible.

Item	issu series commands	install series commands
Support installing and uninstalling patches?	No.	Yes.

ISSU prerequisites

- Read the software release notes to determine which software images need to be upgraded, whether these software images are compatible with one another, and whether these software images are compatible with the software images running on the device. Then, based on the compatibility, determine the command series to use.
- Make sure the storage media on the IRF members have sufficient free space for the new image files.
- Use the **display device** command to examine the operation status of the system and make sure the system is operating properly. If there is any problem with the system, troubleshoot the system before performing an ISSU.
- Use the **save** command to save the running configuration.
- Use FTP or TFTP to download or upload the software image files or the IPE file to the root directory of the master's storage medium. Before a subordinate member is upgraded, the system will ask you whether you want to copy the files to the subordinate member. For more information about FTP and TFTP, see "Configuring FTP" and "Configuring TFTP."

ISSU restrictions and guidelines

- Before an ISSU:
 - Disable BFD for protocols including LDP, RSVP, OSPF, ISIS, RIP, BGP, VRRP, and NQA. Otherwise, services might be interrupted during the upgrade.
 - Make sure the LACP timeout interval is the long timeout interval (the **lacp period short** command is not configured) on all member ports of the dynamic aggregation groups. Otherwise, traffic forwarding might be interrupted during the upgrade.
 - To upgrade the IRF fabric to a compatible version by using the reboot method, configure the IRF bridge MAC address persistence by using the **irf mac-address persistent timer** command or **irf mac-address persistent always** command.
 - If you want to upgrade the IRF fabric to an incompatible version and the IRF bridge MAC address is the MAC address of a member device for which the **issu load** command is required, configure the **irf mac-address persistent always** command.
 - Log in to the device through the console port. If you are using Telnet or SSH, you might be disconnected from the device before the ISSU is completed.
 - To achieve better service continuity, equip the IRF fabric with multiple member devices, connect the member devices into a ring topology, and make sure they are all operating properly. When the IRF fabric has only one member and the reboot or ISSU reboot method is used, service interruption is unavoidable.
 - Make sure nothing is wrong with the hardware and no hardware upgrade is going on. Otherwise, an upgrade failure or system exception might occur.
- During an ISSU:
 - Do not reboot the device, and make sure the network topology is stable.
 - Do not execute any command that is not relevant to the ISSU process.

- Make sure you are the only one who is logged in to the device and no other administrators will log in during the upgrade.
- Do not modify, delete, or rename any boot or system image.
- The **issu** series configuration commands and the **install** series configuration commands are mutually exclusive. You can use only one series of configuration commands for one ISSU process. However, you can use the **install** series displaying and maintaining commands with the **issu** series configuration commands.
- To configure the device after an ISSU, you must relog in to the device.

To perform an ISSU reboot upgrade, also notice the following restrictions and guidelines when the IRF fabric has only one member device:

- Disable MSTP. Otherwise, the network topology might change during the upgrade, resulting in traffic interruption.
- Disable LAGG. During an ISSU reboot, only static aggregation is supported, and traffic on dynamic aggregate interfaces might not be serviced.
- Disable CFD. Otherwise, the CFD CC function will be disabled during an ISSU reboot, resulting in network traffic abnormality.
- Disable DLD. Otherwise, the peer device might consider a link a unidirectional link and shut down the port because it cannot receive probe packets.
- Disable loop detection. Otherwise, the peer device might mistakenly enable a port that was blocked or shut down due to a loop, resulting in traffic abnormality.
- After an ISSU reboot, the following protocols might need to perform a recalculation because the peer device is timed out, resulting in service interruption:
 - Multicast protocols, including PIM, IGMP/MLD, and IGMP snooping/MLD snooping.
 - Routing protocols, including OSPF, ISIS, and BGP.
 - MPLS protocols, including LDP and RSVP.
 - FCoE protocols, including FIP and FSPF.

Performing an ISSU by using issu series commands

- Before performing an ISSU, read "ISSU prerequisites" and "" ISSU restrictions and guidelines."

The ISSU procedure varies depending on whether the IRF fabric has a single or multiple members.

Performing an ISSU for a multi-member IRF fabric

Before upgrade, use the **display version comp-matrix file** { **boot filename** | **system filename** } * or the **display version comp-matrix file ipe** *ipe-filename* command to display the compatibility between the new and old images and the upgrade methods to be used:

- If a new image is on the **Version compatibility list**, the new and old images are compatible.
- If a new image is not on the **Version compatibility list**, the new and old images are incompatible.

To perform an ISSU for a compatible version, execute the following commands:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. (Optional.) Display automatic-rollback timer information.	display issu rollback-timer	Estimate the time the upgrade will take. If the upgrade might not be able to be completed before the timer expires, adjust the timer.
3. (Optional.) Set the automatic rollback timer.	issu rollback-timer <i>minutes</i>	By default, the automatic-rollback interval is 45 minutes. This timer is started when you execute the issu run switchover command. If you do not execute the issu accept or issu commit command before this timer expires, the system automatically rolls back to the original software configuration.
4. Return to user view.	quit	N/A
5. Upgrade a subordinate member and configure the upgrade images as the main startup software images for the subordinate member.	<ul style="list-style-type: none">• Approach 1: issu load file { boot filename system filename } * slot <i>slot-number</i>• Approach 2: issu load file ipe <i>ipe-filename</i> slot <i>slot-number</i>	Specify the member ID of a subordinate member to be upgraded for the slot slot-number option. To upgrade multiple subordinate members, use the command multiple times.
6. Perform a master/subordinate switchover.	issu run switchover	N/A

Step	Command	Remarks
7. (Optional.) Accept the upgrade and delete the automatic-rollback timer.	issu accept	N/A
8. Complete the ISSU process or roll back to the original software configuration.	<ul style="list-style-type: none"> To complete the ISSU process, upgrade the unupgraded subordinate members (including the original master) using the following command: issu commit slot slot-number To roll back to the original software configuration: issu rollback 	<p>After using the issu commit command to upgrade one subordinate member, you must wait for the subordinate member to restart up and join the IRF fabric before upgrading another subordinate member. After all members are upgraded, the ISSU process ends and the ISSU status transitions to Init.</p> <p>During this ISSU process, you can use the issu rollback command at any point to roll back to the original software configuration. For more information about rollback, see <i>Fundamentals Command Reference</i>.</p>

To perform an ISSU for an incompatible version, execute the following commands in user view:

Step	Command	Remarks
1. Upgrade subordinate members and configure the upgrade images as the main startup software images for the subordinate members.	<ul style="list-style-type: none"> Approach 1: issu load file { boot filename system filename } * slot slot-number<1-9> Approach 2: issu load file ipe ipe-filename slot slot-number<1-9> 	<p>Specify the member IDs of the subordinate members to be upgraded for the slot slot-number<1-9> option.</p> <p>If the member devices of the IRF fabric are connected into a ring topology, HP recommends you specify a half of the subordinate members for this command to reduce service interruption. Make sure the specified subordinate members are physically connected.</p>
2. Complete the ISSU process or roll back to the original software configuration.	<ul style="list-style-type: none"> To complete the ISSU process, perform a master/subordinate switchover to upgrade all unupgraded members: issu run switchover To roll back to the original software configuration: issu rollback 	<p>After all members are upgraded, the ISSU process ends and the ISSU status transitions to Init.</p> <p>During this ISSU process, automatic rollback is not supported, but you can use the issu rollback command at any point to manually roll back to the original software configuration. For more information about rollback, see <i>Fundamentals Command Reference</i>.</p>

Performing an ISSU for a single-member IRF fabric

Before upgrade, use the **display version comp-matrix file { boot filename | system filename } *** or the **display version comp-matrix file ipe ipe-filename** command to display the compatibility between the new and old images and the upgrade methods to be used. If a new image is on the **Version compatibility**

list and the value of the **Upgrade Way** field is **Service Upgrade** or **File Upgrade**, the new and old images are compatible and an incremental upgrade applies.

To perform an incremental upgrade to a compatible version, execute the following commands in user view:

Step	Command	Remarks
1. Upgrade the member and configure the upgrade images as the main startup software images for the member.	<ul style="list-style-type: none"> Approach 1: issu load file { boot <i>filename</i> system <i>filename</i> } * slot <i>slot-number</i> Approach 2: issu load file ipe <i>ipe-filename</i> slot <i>slot-number</i> 	Specify the member ID of the only member for the slot <i>slot-number</i> option.
2. Complete the ISSU process or roll back to the original software configuration.	<ul style="list-style-type: none"> To complete the ISSU process: issu commit slot <i>slot-number</i> To roll back to the original software configuration: issu rollback 	Specify the member ID of the only member for the slot <i>slot-number</i> option. After the issu commit command is completed, the ISSU process ends and the ISSU status transitions to Init. During this ISSU process, automatic rollback is not supported, but you can use the issu rollback command to manually roll back to the original software configuration. For more information about rollback, see <i>Fundamentals Command Reference</i> .

To perform a reboot upgrade or ISSU reboot upgrade to a compatible version, or an ISSU for an incompatible version, execute one of the following commands in user view:

Task	Command	Remarks
Upgrade the member and configure the upgrade images as the main startup software images for the member.	<ul style="list-style-type: none"> Approach 1: issu load file { boot <i>filename</i> system <i>filename</i> } * slot <i>slot-number</i> Approach 2: issu load file ipe <i>ipe-filename</i> slot <i>slot-number</i> 	Specify the member ID of the only member for the slot <i>slot-number</i> option. This single command starts and finishes the ISSU process. After this command is completed, the ISSU process ends and the ISSU status transitions to Init. No rollback can be performed during the ISSU process.

NOTE:

For a single-member IRF fabric, device reboot and service interruption are unavoidable during a reboot upgrade or incompatible upgrade. Using the **boot-loader file** command as described in "Upgrading software" can achieve the same effect and has the same impact. The only difference is that the **boot-loader file** command reboots the device but the **boot-loader file** command does not. You must reboot the device when you use the **boot-loader file** command.

Displaying and maintaining ISSU

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display version compatibility information.	display version comp-matrix
Display ISSU status information.	display issu state
Display automatic-rollback timer information.	display issu rollback-timer
Display active software images.	display install active [slot <i>slot-number</i>] [verbose]
Display inactive software images.	display install inactive [slot <i>slot-number</i>] [verbose]
Display main startup software images.	display install committed [slot <i>slot-number</i>] [verbose]
Display backup startup software images.	display install backup [slot <i>slot-number</i>] [verbose]
Display ongoing ISSU activate, deactivate, and rollback operations.	display install job
Display ISSU logs.	display install log [<i>log-id</i>] [verbose]
Display software image file information.	display install package { <i>filename</i> all } [verbose]
Display the software images included in an IPE file.	display install ipe-info <i>ipe-file</i>
Display all software image files that include a specific component or file.	display install which { component <i>name</i> file <i>filename</i> } [slot <i>slot-number</i>]
Clear ISSU logs.	reset install log-history oldest <i>log-number</i>

Performing an ISSU by using install series commands

- Before performing an ISSU, read "ISSU prerequisites" and "" ISSU restrictions and guidelines."

Obtaining the software images issued in an IPE file

1. Download or upload the IPE file to the root directory of the master's storage medium by using FTP or TFTP.
2. Use the **display install ipe-info** command to view which software images are included in the IPE file.
3. Decompress the IPE file by using the following command in user view:

Task	Command
Decompress an IPE file.	install add <i>ipe-file medium-name:</i>

Installing or upgrading software images

When shipped, the device is installed with a boot image and a system image. To upgrade the device software, you might need to perform one or more of the following tasks:

- Upgrade the boot image.
- Upgrade the system image.
- Install patch images.

All these tasks can be implemented by using the **install activate** command. If you use this command for an image that does not exist on the device, you install the image. If you use this command for an image that already exists on the device, you upgrade the image.

To install or upgrade a boot image or a system image, execute the following commands in user view:

Step	Command	Remarks
1. (Optional.) Check for the ISSU method to be used for the upgrade and the possible impact of the upgrade.	install activate { boot filename system filename } * slot slot-number test	N/A
2. Activate the images.	install activate { boot filename system filename } * slot slot-number	An image takes effect only after it is activated.
3. (Optional.) Confirm the software changes.	install commit	To keep activated images effective after a reboot, you must confirm the software changes.

To install or upgrade patch images, execute the following commands in user view:

Step	Command	Remarks
1. Activate the patch images.	install activate patch <i>filename slot slot-number</i>	An image takes effect only after it is activated.
2. (Optional.) Confirm the software changes.	install commit	To keep activated images effective after a reboot, you must confirm the software changes.

Uninstalling patch images

You can uninstall patch images from the device. Boot and system images cannot be uninstalled.

Uninstalled images are not active but are still saved on the storage medium. To permanently remove the images from the device, execute the **install remove** command.

To uninstall an image, deactivate it and then confirm the software change. If you do not confirm the deactivation, the deactivated image will become active after a reboot.

To uninstall patch images, execute the following commands in user view:

Step	Command
1. Deactivate patch images.	install deactivate patch <i>filename slot slot-number</i>
2. (Optional.) Confirm the software changes.	install commit

Rolling back the software configuration

Every time you activate or deactivate a software image for an incremental upgrade, the system creates a rollback point to record the current software configuration. Before you execute the **install commit** command to confirm the software changes (executing this command also removes all rollback points), you can roll back the software configuration to a rollback point to cancel all software image upgrade-related operations performed after the rollback point. You can also roll back the software configuration to the original software configuration, the software configuration before you perform an ISSU.

For an incremental upgrade, up to 50 rollback points are supported. After the limit is reached, the oldest rollback points are deleted to make room for newly created rollback points.

For ISSU reboot upgrades and reboot upgrades, the system does not record and maintain any rollback point, and you can roll back the software configuration only to the original software configuration.

Patch images do not support rollback.

To make a rollback take effect after a reboot, you must confirm the rollback operation using the **install commit** command.

To roll back the software configuration, execute the following commands in user view:

Step	Command	Remarks
1. Roll back the software configuration to an earlier rollback point or the original software configuration.	install rollback to { <i>point-id</i> original }	To view available rollback points, use the display install rollback command.
2. (Optional.) Confirm the software changes.	install commit	N/A

Aborting a software activate/deactivate operation

When the system is activating or deactivating a software image for an incremental upgrade, you can use this feature to abort the operation. Then, the system runs with the software images that it used before the activate or deactivate operation.

To abort a software activate or deactivate operation for an incremental upgrade, use the following command in user view:

Task	Command
Abort a software activate or deactivate operation.	install abort [<i>job-id</i>]

Verifying the software change confirmation status and software image integrity and consistency

If some software images are not integral or some activated/deactivated software images are not confirmed, a switchover might not occur as expected, and the IRF members might run different versions of software images after a reboot or even cannot restart up correctly.

To solve the problem, download and install the software images again to ensure software integrity, or use the **install activate**, **install deactivate**, and **install commit** commands as appropriate to guarantee software image consistency.

To check the integrity and consistency of software images, execute the following command in user view:

Task	Command
Verify the software change confirmation status and software image integrity and consistency.	install verify

Removing inactive software images

You can remove inactive software images from the device.

ⓘ IMPORTANT:

Removing a software image deletes the image file from the device permanently. This operation can neither be reverted by using the **install rollback to** command nor be aborted by using the **install abort** command.

To remove inactive software images, execute one of the following commands as appropriate in user view:

Task	Command
Remove inactive software images.	install remove [slot <i>slot-number</i>] { <i>package</i> inactive }

Displaying and maintaining ISSU

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display active software images.	display install active [slot <i>slot-number</i>] [verbose]
Display inactive software images.	display install inactive [slot <i>slot-number</i>] [verbose]
Display main startup software images.	display install committed [slot <i>slot-number</i>] [verbose]
Display backup startup software images.	display install backup [slot <i>slot-number</i>] [verbose]
Display ongoing ISSU activate, deactivate, and rollback operations.	display install job
Display ISSU logs.	display install log [<i>log-id</i>] [verbose]
Display software image file information.	display install package { <i>filename</i> all } [verbose]
Display the software images included in an IPE file.	display install ipe-info <i>ipe-file</i>
Display rollback point information.	display install rollback [<i>point-id</i>]
Display all software image files that include a specific component or file.	display install which { component <i>name</i> file <i>filename</i> } [slot <i>slot-number</i>]
Clear ISSU logs.	reset install log-history oldest <i>log-number</i>
Clear ISSU rollback points.	reset install rollback oldest <i>point-id</i>

Managing the device

This chapter describes how to monitor the operating status of the device, configure the running parameters (such as the device name, system time, and the temperature alarm thresholds), and reboot the device.

You can perform the configuration tasks in this chapter in any order.

Configuring the device name

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

To configure the device name:

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

Setting the system time

The system time is determined by the UTC time, local time zone, and daylight saving time. You can use the **display clock** command to view the system time.

A correct system time setting is essential to network management and communication. Before you run the device on the network, set the system time correctly or configure NTP to synchronize the system time to a trusted time source. If you perform both configuration tasks, the device uses the system time of the trusted time source. For more information about NTP, see *Network Management and Monitoring Configuration Guide*.

Powering off or rebooting a HP 5920 or HP 5900 switch does not affect the system time.

To set the system time:

Step	Command	Remarks
1. Set the UTC time.	clock datetime <i>time date</i>	Execute this command in user view. The default UTC time is 00:00:00 on 01/01/2011.
2. Enter system view.	system-view	N/A
3. Set the local time zone.	clock timezone <i>zone-name</i> { add minus } <i>zone-offset</i>	The default local time zone is the UTC time zone.

Step	Command	Remarks
4. Set the daylight saving time	clock summer-time <i>name start-time start-date end-time end-date add-time</i>	By default, daylight saving time is disabled.

Enabling displaying the copyright statement

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

```
*****
* Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.          *
* Without the owner's prior written consent,                                *
* no decompiling or reverse-engineering shall be allowed.                  *
*****
```

To enable displaying the copyright statement:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enable displaying the copyright statement.	copyright-info enable	By default, this function is enabled.

Configuring banners

Banners are messages that the system displays when a user logs in.

Banner types

The system supports the following banners:

- **Legal banner**—Appears after the copyright or license statement. To continue login, the user must enter **Y** or press **Enter**. To quit the process, the user must enter **N**. **Y** and **N** are case-insensitive.
- **Message of the Day (MOTD) banner**—Appears after the legal banner and before the login banner.
- **Login banner**—Appears only when password or scheme authentication has been configured.
- **Shell banner**—Appears after a user logs in.

Banner input modes

Use one of the following methods to configure a banner:

- Single-line input.

Input the entire banner in the same line as the command. The start and end delimiters for the banner can be any printable character but must be the same and not included in the banner. The input text, including the command keywords and the delimiters cannot exceed 510 characters. In

this mode, do not press **Enter** before you input the end delimiter. For example, you can configure the shell banner "Have a nice day." as follows:

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

- Multiple-line input.

Input message text in multiple lines. In this approach, the message text can be up to 2000 characters. Use one of the following methods to implement multi-line input mode:

- **Method 1**—Press **Enter** after the last command keyword. At the system prompt, enter the banner and end the last line with the delimiter character %. For example, you can configure the banner "Have a nice day. Please input the password." as follows:

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

- **Method 2**—After you type the last command keyword, type any single printable character as the start delimiter for the banner and press **Enter**. At the system prompt, type the banner and end the last line with the same delimiter. For example, you can configure the banner "Have a nice day. Please input the password." as follows:

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

- **Method 3**—After you type the last command keyword, type the start delimiter and part of the banner and press **Enter**. At the system prompt, enter the rest of the banner and end the last line with the same delimiter. For example, you can configure the banner "Have a nice day. Please input the password." as follows:

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

Configuration procedure

To configure banners:

Step	Command
1. Enter system view.	system-view
2. Configure the legal banner.	header legal text
3. Configure the MOTD banner.	header motd text
4. Configure the login banner.	header login text
5. Configure the shell banner.	header shell text

Setting the operating mode

In different operating mode, the device supports different features and might have different specifications for the supported features. For example, the FC and FCOE functions are supported only when the device is operating in advanced mode.

Change to the operating mode takes effect after a reboot.

To set the operating mode of the device:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the operating mode.	system-working-mode { advance standard }	By default, the device operates in standard mode.

Rebooting the device

△ CAUTION:

A reboot can interrupt network services.

To avoid configuration loss, use the **save** command to save the running configuration before a reboot. For more information about the **save** command, see *Fundamentals Command Reference*.

Before a reboot, use the **display startup** and **display boot-loader** commands to verify that you have correctly specified the startup configuration file and startup software images. If the main startup software images are corrupted or missing, you must respecify a set of main startup software images before using the **reboot** command to reboot the device. Otherwise, the device cannot start up. For more information about the two **display** commands, see *Fundamentals Command Reference*.

Reboot the device using one of the following methods:

- Power off and then power on the device. This method might cause data loss, and is the least-preferred method.
- Immediately reboot the device at the CLI.
- Schedule a reboot at the CLI, so the device automatically reboots at the specified time or after the specified period of time.

Reboot at the CLI enables easy remote device maintenance.

Configuration guidelines

The automatic reboot configuration is effective on all member devices, and will be canceled if a master/subordinate switchover occurs.

If you execute the **scheduler reboot at** or **scheduler reboot delay** command multiple times, the most recent configuration takes effect.

For data security, the device does not reboot while it is performing file operations.

Rebooting devices immediately at the CLI

To immediately reboot the device, execute one of the following commands as appropriate in user view:

Task	Command
Reboot an IRF member device or all IRF member devices.	reboot [slot <i>slot-number</i>]

Scheduling a device reboot

To schedule a reboot, execute either of the following commands in user view:

Task	Command	Remarks
Specify the reboot date and time.	scheduler reboot at <i>time</i> [<i>date</i>]	By default, no reboot date or time is specified.
Specify the reboot delay time.	scheduler reboot delay <i>time</i>	By default, no reboot delay time is specified.

Scheduling a task

You can schedule the device to automatically execute a command or a set of commands without administrative interference.

You can configure a one-time schedule or a periodic schedule. A one-time schedule is not saved to the configuration file, and is lost when the device reboots. A periodic schedule is saved to the startup configuration file and will be automatically executed periodically.

Configuration guidelines

- To make sure a task schedule can be executed as expected, make sure the system time is correct. If the system time is incorrect, reconfigure the system time or configure NTP. For more information about NTP, see *Network Management and Monitoring Configuration Guide*.
- Make sure all commands in a schedule are compliant to the command syntax. The system does not check the syntax when you assign a command to a job.
- A schedule cannot contain any of these commands: **telnet**, **ftp**, **ssh2**, and **monitor process**.
- A schedule does not support user interaction. If a command requires a yes or no answer, the system always assumes that a **Y** or **Yes** is entered. If a command requires a character string input, the system assumes that the default character string (if any) is entered, or a null string is entered.
- A schedule is executed in the background, and no output (except for logs, traps, and debug information) is displayed for the schedule.

Configuration procedure

To configure a one-time schedule for the device:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a job.	scheduler job <i>job-name</i>	By default, no job exists.
3. Assign a command to the job.	command <i>id command</i>	By default, no command is assigned to a job. You can assign multiple commands to a job. A command with a smaller ID will be executed first.
4. Exit to system view.	quit	N/A
5. Create a schedule.	scheduler schedule <i>schedule-name</i>	By default, no schedule exists.
6. Assign a job to a schedule.	job <i>job-name</i>	By default, no job is assigned to a schedule. You can assign multiple jobs to a schedule. The jobs will be executed concurrently.
7. Specify an execution time table for the one-time schedule.	<ul style="list-style-type: none"> Specify the execution date and time: time at <i>time date</i> Specify the execution days and time: time once at <i>time</i> [month-date <i>month-day</i> week-day <i>week-day</i>&<1-7>] Specify the execution delay time: time once delay <i>time</i> 	Configure one command as required. By default, no execution time is specified for a schedule. Executing commands clock datetime , clock summer-time , and clock timezone does not change the execution time table that is already configured for a schedule.

To configure a periodic schedule for the device:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Create a job.	scheduler job <i>job-name</i>	By default, no job exists.
3. Assign a command to the job.	command <i>id command</i>	By default, no command is assigned to a job. You can assign multiple commands to a job. A job with a smaller ID will be executed first.
4. Exit to system view.	quit	N/A
5. Create a schedule.	scheduler schedule <i>schedule-name</i>	By default, no schedule exists.

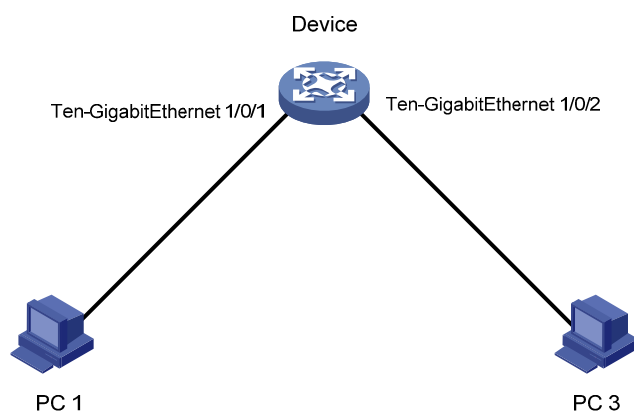
Step	Command	Remarks
6. Assign a job to a schedule.	<code>job job-name</code>	By default, no job is assigned to a schedule. You can assign multiple jobs to a schedule. The jobs will be executed concurrently.
7. Specify an execution time table for the periodic schedule	<ul style="list-style-type: none"> Execute the schedule at an interval from the specified time on: time repeating at time [month-date [<i>month-day</i> last] week-day <i>week-day</i>&<1-7>] Execute the schedule at the specified time on every specified day in a month or week: time repeating [at time [<i>date</i>]] interval <i>interval-time</i> 	Configure either command. By default, no execution time is specified for a schedule. Executing commands clock datetime , clock summer-time , and clock timezone does not change the execution time table that is already configured for a schedule.

Schedule configuration example

Network requirements

To save energy, configure the device to enable interfaces Ten-GigabitEthernet 1/0/1 and Ten-GigabitEthernet 1/0/2 at 8:00 a.m. every Monday through Friday and disable the interfaces at 18:00 every Monday through Friday.

Figure 26 Network diagram



Scheduling procedure

```

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

```

# Configure a job for disabling interface Ten-GigabitEthernet 1/0/1.
[Sysname] scheduler job shutdown-Ten-GigabitEthernet1/0/1
[Sysname-job-shutdown-Ten-GigabitEthernet1/0/1] command 1 system-view
[Sysname-job-shutdown-Ten-GigabitEthernet1/0/1] command 2 interface
ten-gigabitEthernet1/0/1
[Sysname-job-shutdown-Ten-GigabitEthernet1/0/1] command 3 shutdown
[Sysname-job-shutdown-Ten-GigabitEthernet1/0/1] quit

# Configure a job for enabling interface Ten-GigabitEthernet 1/0/1.
[Sysname] scheduler job start-Ten-GigabitEthernet1/0/1
[Sysname-job-start-Ten-GigabitEthernet1/0/1] command 1 system-view
[Sysname-job-start-Ten-GigabitEthernet1/0/1] command 2 interface
ten-gigabitEthernet1/0/1
[Sysname-job-start-Ten-GigabitEthernet1/0/1] command 3 undo shutdown
[Sysname-job-start-Ten-GigabitEthernet1/0/1] quit

# Configure a job for disabling interface Ten-GigabitEthernet 1/0/2.
[Sysname] scheduler job shutdown-Ten-GigabitEthernet1/0/2
[Sysname-job-shutdown-Ten-GigabitEthernet1/0/2] command 1 system-view
[Sysname-job-shutdown-Ten-GigabitEthernet1/0/2] command 2 interface
ten-gigabitEthernet1/0/2
[Sysname-job-shutdown-Ten-GigabitEthernet1/0/2] command 3 shutdown
[Sysname-job-shutdown-Ten-GigabitEthernet1/0/2] quit

# Configure a job for enabling interface Ten-GigabitEthernet 1/0/2.
[Sysname] scheduler job start-Ten-GigabitEthernet1/0/2
[Sysname-job-start-Ten-GigabitEthernet1/0/2] command 1 system-view
[Sysname-job-start-Ten-GigabitEthernet1/0/2] command 2 interface
ten-gigabitEthernet1/0/2
[Sysname-job-start-Ten-GigabitEthernet1/0/2] command 3 undo shutdown
[Sysname-job-start-Ten-GigabitEthernet1/0/2] quit

# Configure a periodic schedule for enabling the interfaces at 8:00 a.m. every Monday through Friday.
[Sysname] scheduler schedule START-pc1/pc2
[Sysname-schedule-START-pc1/pc2] job start-Ten-GigabitEthernet1/0/1
[Sysname-schedule-START-pc1/pc2] job start-Ten-GigabitEthernet1/0/2
[Sysname-schedule-START-pc1/pc2] time repeating at 8:00 week-day mon tue wed thu fri
[Sysname-schedule-START-pc1/pc2] quit

# Configure a periodic schedule for disabling the interfaces at 18:00 every Monday through Friday.
[Sysname] scheduler schedule STOP-pc1/pc2
[Sysname-schedule-STOP-pc1/pc2] job shutdown-Ten-GigabitEthernet1/0/1
[Sysname-schedule-STOP-pc1/pc2] job shutdown-Ten-GigabitEthernet1/0/2
[Sysname-schedule-STOP-pc1/pc2] time repeating at 18:00 week-day mon tue wed thu fri
[Sysname-schedule-STOP-pc1/pc2] quit

```

Verifying the scheduling

```

# Display the configuration information of all jobs.
[Sysname] display scheduler job
Job name: shutdown-Ten-GigabitEthernet1/0/1

```

```
system-view
interface ten-gigabitethernet1/0/1
shutdown
```

Job name: shutdown-Ten-GigabitEthernet1/0/2

```
system-view
interface ten-gigabitethernet1/0/2
shutdown
```

Job name: start-Ten-GigabitEthernet1/0/1

```
system-view
interface ten-gigabitethernet1/0/1
undo shutdown
```

Job name: start-Ten-GigabitEthernet1/0/2

```
system-view
interface ten-gigabitethernet1/0/2
undo shutdown
```

Display the schedule information.

```
[Sysname] display scheduler schedule
```

```
Schedule name      : START-pc1/pc2
Schedule type      : Run on every Mon Tue Wed Thu Fri at 08:00:00
Start time         : Wed Sep 28 08:00:00 2011
Last execution time : Wed Sep 28 08:00:00 2011
Last completion time : Wed Sep 28 08:00:03 2011
Execution counts   : 1
```

```
-----
Job name                Last execution status
start-Ten-GigabitEthernet1/0/1      Successful
start-Ten-GigabitEthernet1/0/2      Successful
```

```
Schedule name      : STOP-pc1/pc2
Schedule type      : Run on every Mon Tue Wed Thu Fri at 18:00:00
Start time         : Wed Sep 28 18:00:00 2011
Last execution time : Wed Sep 28 18:00:00 2011
Last completion time : Wed Sep 28 18:00:01 2011
Execution counts   : 1
```

```
-----
Job name                Last execution status
shutdown-Ten-GigabitEthernet1/0/1    Successful
shutdown-Ten-GigabitEthernet1/0/2    Successful
```

Display schedule log information.

```
[Sysname] display scheduler logfile
```

```
Job name      : start-Ten-GigabitEthernet1/0/1
Schedule name : START-pc1/pc2
Execution time : Wed Sep 28 08:00:00 2011
```

```

Completion time : Wed Sep 28 08:00:02 2011
----- Job output -----
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface ten-gigabitEthernet1/0/1
[Sysname-Ten-GigabitEthernet1/0/1]undo shutdown

Job name          : start-Ten-GigabitEthernet1/0/2
Schedule name     : START-pc1/pc2
Execution time    : Wed Sep 28 08:00:00 2011
Completion time   : Wed Sep 28 08:00:02 2011
----- Job output -----
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface ten-gigabitEthernet1/0/2.
[Sysname-Ten-GigabitEthernet1/0/2]undo shutdown

Job name          : shutdown-Ten-GigabitEthernet1/0/1
Schedule name     : STOP-pc1/pc2
Execution time    : Wed Sep 28 18:00:00 2011
Completion time   : Wed Sep 28 18:00:01 2011
----- Job output -----
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface ten-gigabitEthernet1/0/1
[Sysname-Ten-GigabitEthernet1/0/1]shutdown

Job name          : shutdown-Ten-GigabitEthernet1/0/2
Schedule name     : STOP-pc1/pc2
Execution time    : Wed Sep 28 18:00:00 2011
Completion time   : Wed Sep 28 18:00:01 2011
----- Job output -----
<Sysname>system-view
System View: return to User View with Ctrl+Z.
[Sysname]interface ten-gigabitEthernet1/0/2
[Sysname-Ten-GigabitEthernet1/0/2]shutdown

```

Configuring the preferred airflow direction

Two models of fans are available for the device. One model has air flow from the port side to the power supply side. The other model has air flow from the power supply side to the port side. Select the correct model and configure the preferred airflow direction consistent with the airflow direction of the ventilation system in the equipment room.

You can configure the preferred airflow direction for the device. If a fan tray is not operating correctly or the device detects that an installed fan tray has a different airflow direction than the configured one, the system sends out traps and logs. You must replace the wrong fan tray with a correct tray.

To configure the preferred airflow direction:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Configure the preferred airflow direction.	fan prefer-direction slot <i>slot-number</i> { power-to-port port-to-power }	The default preferred airflow direction is from the power supply side to the port side.

Setting the port status detection timer

Some protocols shut down ports under specific conditions. For example, MSTP shuts down a BPDU guard-enabled port when the port receives a BPDU. After a port is shut down this way, the device starts the detection timer. If the port is still down when the detection timer expires, the device automatically brings up the port and restores the port's actual physical status.

To set the port status detection timer:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Set the port status detection timer.	shutdown-interval <i>time</i>	The default setting is 30 seconds.

Setting memory usage thresholds

To ensure proper operation and improve memory utilization, the system monitors the amount of free memory space in real time. When a threshold is crossed, the system generates an alarm notification or an alarm-removed notification and sends it to affected service modules or processes so they can take responsive actions.

The system supports the following levels of thresholds:

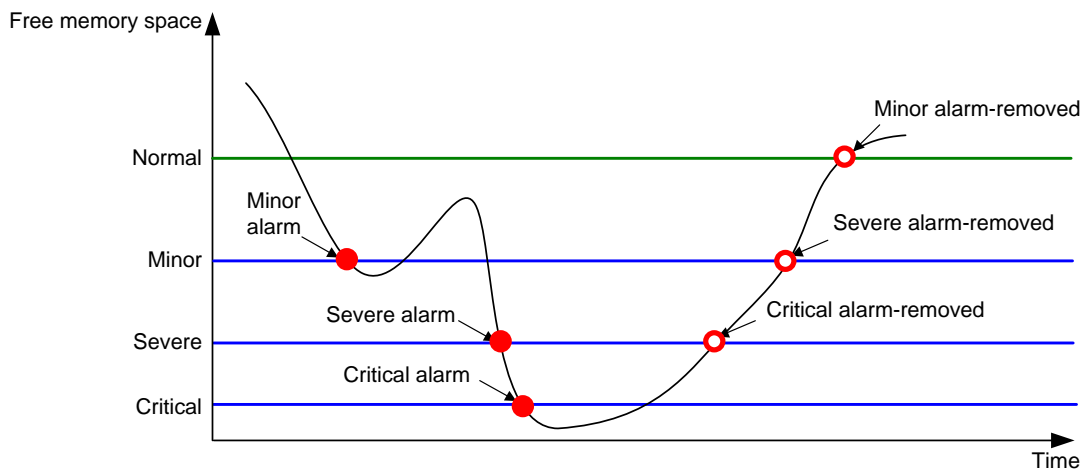
- Normal state threshold.
- Minor alarm threshold.
- Severe alarm threshold.
- Critical alarm threshold.

Figure 27 shows the triggering conditions for memory alarm notifications and memory alarm-removed notifications:

Notification	Triggering condition	Remarks
Minor alarm notification	The amount of free memory space goes down to or below the minor alarm threshold for the first time.	After generating and sending a minor alarm notification, the system does not generate and send any additional minor alarm notifications until the first minor alarm is canceled.

Notification	Triggering condition	Remarks
Severe alarm notification	The amount of free memory space goes down to or below the severe alarm threshold for the first time.	After generating and sending a severe alarm notification, the system does not generate and send any additional severe alarm notifications until the first severe alarm is canceled.
Critical alarm notification	The amount of free memory space goes down to or below the critical alarm threshold for the first time.	After generating and sending a critical alarm notification, the system does not generate and send any additional critical alarm notifications until the first critical alarm is canceled.
Critical alarm-removed notification	The amount of free memory space goes up to or above the severe alarm threshold.	N/A
Severe alarm-removed notification	The amount of free memory space goes up to or above the minor alarm threshold.	N/A
Minor alarm-removed notification	The amount of free memory space goes up to or above the normal state threshold.	N/A

Figure 27 Memory alarm notification and alarm-removed notification



To set memory usage thresholds:

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

Step	Command	Remarks
		The defaults are as follows:
2.	Set memory usage thresholds.	<ul style="list-style-type: none"> • Minor alarm threshold—96 MB. • Severe alarm threshold—64 MB. • Critical alarm threshold—48 MB. • Normal state threshold—128 MB.
	memory-threshold [slot slot-number] minor minor-value severe severe-value critical critical-value normal normal-value	

Configuring the temperature alarm thresholds

You can set a lower temperature threshold, warning temperature threshold, and alarming temperature threshold to monitor the temperature of the device through its temperature sensors. The device also supports a shutdown temperature threshold, which is not configurable.

When the temperature drops below the lower temperature threshold or reaches the warning temperature threshold, the device logs the event and sends out a log message and a trap.

When the temperature reaches the alarming temperature threshold, the device logs the event and notifies users by repeatedly sending log messages and traps and by setting the LEDs on the device panel.

When the temperature reaches the shutdown temperature threshold, the device logs the event, notifies users of the temperature, and shuts down.

To configure the temperature alarm thresholds:

Step	Command	Remarks
1.	Enter system view.	N/A
2.	Configure the temperature alarm thresholds for a member device.	<p>The warning and alarming thresholds must be higher than the lower temperature threshold.</p> <p>The alarming threshold must be higher than the warning threshold.</p> <p>For the default temperature alarm thresholds, see Table 14.</p>
	temperature-limit slot slot-number hotspot sensor-number lowerlimit warninglimit [alarmlimit]	

Table 14 Default temperature alarm thresholds

Airflow direction	Sensor	Lower temperature threshold	Warning temperature threshold	Alarming temperature threshold	Shutdown temperature threshold	
HP 5900AF-48XG-4	Power-to-port	hotspot 1	0	50	55	N/A
		hotspot 2	0	58	63	N/A
QSFP+	Port-to-power	hotspot 1	0	61	66	N/A

Airflow direction	Sensor	Lower temperature threshold	Warning temperature threshold	Alarming temperature threshold	Shutdown temperature threshold
Switch(J C772A)	hotspot 2	0	58	63	N/A
HP 5920AF-24XG Switch(J G296A)	Power-to-port hotspot 1 to hotspot 4	0	62	77	N/A
	Port-to-power				N/A

Disabling all USB interfaces

HP 5920 & 5900 switches provide USB interfaces. You can use USB interfaces to upload or download files. By default, all USB interfaces are enabled. You can disable USB interfaces as needed.

To disable all USB interfaces:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Disable all USB interfaces.	usb disable	By default, all USB interfaces are enabled.

Verifying and diagnosing transceiver modules

Verifying transceiver modules

You can use one of the following methods to verify the genuineness of a transceiver module:

- Display the key parameters of a transceiver module, including its transceiver type, connector type, central wavelength of the transmit laser, transfer distance, and vendor name.
- Display its electronic label. The electronic label is a profile of the transceiver module and contains the permanent configuration, including the serial number, manufacturing date, and vendor name. The data is written to the storage component during device debugging or testing.

To verify transceiver modules, execute the following commands in any view:

Task	Command	Remarks
Display key parameters of transceiver modules.	display transceiver interface [<i>interface-type interface-number</i>]	N/A
Display transceiver modules' electrical label information.	display transceiver manuinfo interface [<i>interface-type interface-number</i>]	This command cannot display information for some transceiver modules.

Diagnosing transceiver modules

The device provides the alarm and digital diagnosis functions for transceiver modules. When a transceiver module fails or is not operating correctly, you can check the alarms present on the transceiver module to identify the fault source or you can examine the key parameters monitored by the digital diagnosis function, including the temperature, voltage, laser bias current, TX power, and RX power.

To diagnose transceiver modules, execute the following command in any view:

Task	Command	Remarks
Display alarms present on transceiver modules.	display transceiver alarm interface [<i>interface-type interface-number</i>]	N/A
Display the current measured values of the digital diagnosis parameters for transceiver modules.	display transceiver diagnosis interface [<i>interface-type interface-number</i>]	This command cannot display information for some transceiver modules.

Displaying and maintaining device management configuration

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display system version information.	display version
Display the system time, date, local time zone, and daylight saving time.	display clock
Display the copyright statement.	display copyright
Display CPU usage statistics.	display cpu-usage [<i>slot slot-number</i> [<i>cpu cpu-number</i>]]
Display historical CPU usage statistics in a chart.	display cpu-usage history [<i>job job-id</i>] [<i>slot slot-number</i> [<i>cpu cpu-number</i>]]
Display hardware information.	display device [<i>usb</i>] [<i>slot slot-number</i> <i>verbose</i>]
Display the electronic label data for the device.	display device manuinfo [<i>slot slot-number</i>]
Display the electronic label data for the specified fan.	display device manuinfo slot <i>slot-number fan fan-id</i>
Display the electronic label data for the specified power supply.	display device manuinfo slot <i>slot-number power power-id</i>
Display the operating statistics for multiple feature modules.	display diagnostic-information [<i>hardware</i> <i>infrastructure</i> <i>I2</i> <i>I3</i> <i>service</i>]
Display device temperature statistics.	display environment [<i>slot slot-number</i>]
Display the operating states of fans.	display fan [<i>slot slot-number</i> [<i>fan-id</i>]]
Display memory usage statistics.	display memory [<i>slot slot-number</i>]

Task	Command
Display memory usage thresholds.	display memory-threshold [<i>slot slot-number</i>]
Display power supply information.	display power [<i>slot slot-number</i> [<i>power-id</i>]]
Display job configuration information.	display scheduler job [<i>job-name</i>]
Display job execution log information.	display scheduler logfile
Display the automatic reboot schedule.	display scheduler reboot
Display schedule information.	display scheduler schedule [<i>schedule-name</i>]
Display the current system working mode.	display system-working-mode
Display the startup software image upgrade history records of the master.	display version-update-record
Clear the startup software image upgrade history records of the master.	reset version-update-record
Clear job execution log information.	reset scheduler logfile

Using the emergency shell

At startup, the device tries to locate and load the Comware startup software images, which includes a boot image, a system image, and some patch images (if any). If the boot image is OK but the system image or a patch image is missing or corrupted, the device enters emergency shell mode.

After the device enters emergency shell mode, you can log in through the console port and get and load a system image to start the Comware system. After the Comware system is started, you can load patch images as described in "Upgrading software" or "Performing an ISSU by using install series commands." This chapter describes how to get and load the system image in emergency shell mode.

If more than one member exists on the device, each member starts up independently. If one member enters emergency shell mode, log in to that member through its console port to load a system image for it.

For more information about software images, see "Upgrading software." For more information about how to log in through the console port, see "Logging in through the console port for the first device access."

Managing the file system

The emergency shell provides some basic file system management commands for managing the files on the device's storage media. You can use these commands to manage the file system.

! IMPORTANT:

- A file deleted by using the **delete** command cannot be restored.
- The **format** command permanently deletes all files and folders from a storage medium, and the deleted files and folders cannot be restored.

To manage the file system, execute the following commands in user view:

Task	Command	Remarks
Display files or folders.	dir [/all] [file-url]	N/A
Create a folder on a storage medium.	mkdir <i>directory</i>	The parent folder must already exist. For example, to create folder flash:/test/mytest , the parent folder test must already exist on the Flash. The name for the new folder must be unique under the parent folder.
Display the current path.	pwd	N/A
Copy a file.	copy <i>fileurl-source</i> <i>fileurl-dest</i>	N/A
Move a file.	move <i>fileurl-source</i> <i>fileurl-dest</i>	The target folder must have enough space for the file.
Display the contents of a file.	more <i>file-url</i>	N/A

Task	Command	Remarks
Permanently delete a file.	delete <i>file-url</i>	N/A
Delete a folder.	rmdir <i>directory</i>	To delete a folder, first delete all files and child folders in the folder.
Format a storage medium.	format <i>device</i>	N/A

Obtaining a system image from an FTP/TFTP server

If the required system image is saved on an FTP or TFTP server, configure the management Ethernet interface and obtain the system image as described in the following sections.

The version of the system image must match that of the boot image. Before obtaining a system image, check the version of the boot image by using the **display version** command and the version of the system image by reading the release notes.

Configuring the management Ethernet interface

To use FTP, TFTP, SSH, and Telnet services in emergency shell mode, you must configure an IP address for the management Ethernet interface and activate the port at first. If the servers are on a different network, you must also specify a gateway for the management Ethernet interface.

To configure the management Ethernet interface on an IPv4 network:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter management Ethernet interface view.	interface m-eth0	N/A
3. Assign an IPv4 address to the port.	ip address <i>ip-address</i> { <i>mask-length</i> <i>mask</i> }	By default, the management Ethernet interface has no IPv4 address.
4. Specify an IPv4 gateway for the port.	ip gateway <i>ip-address</i>	By default, the management Ethernet interface has no IPv4 gateway configured.
5. Activate the port.	undo shutdown	By default, the management Ethernet interface is active.
6. Return to system view.	quit	N/A

To configure the management Ethernet interface on an IPv6 network:

Step	Command	Remarks
1. Enter system view.	system-view	N/A
2. Enter management Ethernet interface view.	interface m-eth0	N/A

Step	Command	Remarks
3. Assign an IPv6 address to the port.	ipv6 address <i>ipv6-address prefix-length</i>	By default, the management Ethernet interface has no IPv6 address.
4. Specify an IPv6 gateway for the port.	ipv6 gateway <i>ipv6-address</i>	By default, the management Ethernet interface has no IPv6 gateway configured.
5. Activate the port.	undo shutdown	By default, the management Ethernet interface is active.
6. Return to system view.	quit	N/A

Checking the connectivity to a server

After completing network parameter configuration, you can use the **ping** command to check the connectivity between the device and the intended FTP or TFTP server.

To check the connectivity between the device and a server on an IPv4 network, execute the following command in any view:

Task	Command
Check the connectivity to an IPv4 address	ping [<i>-c count</i> <i>-s size</i>] * <i>ip-address</i>

To check the connectivity between the device and a server on an IPv6 network, execute the following command in any view:

Task	Command
Check the connectivity to an IPv6 address	ping ipv6 [<i>-c count</i> <i>-s size</i>] * <i>ipv6-address</i>

Accessing the server

In emergency shell mode, the device can:

- Operate as an FTP or TFTP client to download software packages from an FTP or TFTP server.
- Operate as an FTP or TFTP client to upload software packages to an FTP or TFTP server.
- Operate as a Telnet or SSH client so you can log in to a server to, for example, view and manage files on the server.

To access a remote IPv4 server, execute one of the following commands as appropriate in user view:

Task	Command
Use FTP to download a file from or upload a file to an IPv4 server.	ftp <i>server-ipv4-address</i> user <i>username</i> password <i>password</i> { get <i>remote-file</i> <i>local-file</i> put <i>local-file</i> <i>remote-file</i> }
Use TFTP to download a file from or upload a file to an IPv4 server.	tftp <i>server-ipv4-address</i> { get <i>remote-file</i> <i>local-file</i> put <i>local-file</i> <i>remote-file</i> }
Telnet to an IPv4 server.	telnet <i>server-ipv4-address</i>
Use SSH to connect to an IPv4 server.	ssh2 <i>server-ipv4-address</i>

To access a remote IPv6 server, execute one of the following commands to obtain a system image in user view:

Task	Command
Use FTP to download a file from or upload a file to an IPv6 server.	ftp ipv6 <i>server-ipv6-address</i> user <i>username</i> password <i>password</i> { get <i>remote-file</i> <i>local-file</i> put <i>local-file</i> <i>remote-file</i> }
Use TFTP to download a file from or upload a file to an IPv6 server.	tftp ipv6 <i>server-ipv6-address</i> { get <i>remote-file</i> <i>local-file</i> put <i>local-file</i> <i>remote-file</i> }
Telnet to an IPv6 server.	telnet ipv6 <i>server-ipv6-address</i>
Use SSH to connect to an IPv6 server.	ssh2 ipv6 <i>server-ipv6-address</i>

Loading the system image

! IMPORTANT:

The version of the system image must match that of the boot image. Before loading a system image, use the **display version** and **display install package** commands to check the version information of the boot image and system image.

When you load the system image, the system modifies the main startup software image set to include only the boot image and system image so the device can reboot normally.

To load the system image, execute the following command in user view:

Task	Command
Load a system image.	install load <i>system-package</i>

Rebooting the device

To reboot the device, execute one of the following commands as appropriate in user view:

Task	Command
Reboot the current member device.	reboot

Displaying device information in emergency shell mode

Execute **display** commands in any view.

Task	Command
Display copyright information.	display copyright
Display software package information.	display install package <i>package</i>

Task	Command
Display management Ethernet interface information.	display interface m-eth0
Display IPv4 routing information.	display ip routing-table
Display IPv6 routing information.	display ipv6 routing-table
Display boot image version information.	display version

Emergency shell usage example

Network requirements

The device has only the boot image (boot.bin) and enters emergency shell after startup. The device and PC can reach each other.

Use the TFTP client service on the device to download system image system.bin from the PC and start the Comware system on the device.

Figure 28 Network diagram



Usage procedure

Check which files are stored and how much space is available on the storage medium of the device.

```

<boot> dir
Directory of flash:/
 0  drw-      5954  Apr 26 2012 21:06:29  logfile
 1  -rw-      1842  Apr 27 2012 04:37:17  boot.bin
 2  -rw-      1518  Apr 26 2012 12:05:38  startup.cfg
 3  -rw-      2045  May 04 2012 15:50:01  backcfg.cfg
  
```

```
524288 KB total (513248 KB free)
```

The output shows that the boot image **boot.bin** is present but the matching system image **system.bin** is not, and the available space is 513248 KB, enough for saving the system image **system.bin**.

Check the version information of the boot image.

```

<boot> display version
HP Comware Software, Version 7.1.035, ESS 2206P05002
Copyright (c) 2010-2012 Hewlett-Packard Development Company, L.P.
HP 5900AF-48XG-4QSFP+ Switch uptime is 0 weeks, 0 days, 0 hours, 13 minutes
Last reboot reason : User reboot
  
```

```

Boot image: flash:/5900_5920-cmw710-boot-e2206p05002.bin
Boot image version: 7.1.035P02, ESS 2206P05002
System image: flash:/5900_5920-cmw710-system-e2206p05002.bin
  
```

System image version: 7.1.035, ESS 2206P05002

Slot 2

HP 5900AF-48XG-4QSFP+ Switch with 2 Processors

Last reboot reason : User reboot

2048M bytes SDRAM

4M bytes Nor Flash Memory

512M bytes Nand Flash Memory

Config Register points to Nand Flash

Configure an IP address and a gateway for the management Ethernet interface.

```
<boot> system-view
```

```
[boot] interface m-eth0
```

```
[boot-m-eth0] ip address 1.1.1.1 16
```

```
[boot-m-eth0] ip gateway 1.1.1.2
```

Test the connectivity between the device and the TFTP server.

```
<boot> ping 1.2.1.1
```

```
PING 1.2.1.1(1.2.1.1):56 data bytes
```

```
64 bytes from 1.2.1.1:seq=0 ttl=64 time=0.160 ms
```

```
64 bytes from 1.2.1.1:seq=1 ttl=64 time=0.062 ms
```

```
64 bytes from 1.2.1.1:seq=2 ttl=64 time=0.061 ms
```

```
64 bytes from 1.2.1.1:seq=3 ttl=64 time=0.065 ms
```

```
64 bytes from 1.2.1.1:seq=4 ttl=64 time=0.063 ms
```

```
--- 1.2.1.1 ping statistics ---
```

```
5 packets transmitted,5 packets received,0% packet loss
```

```
round-trip min/avg/max = 0.061/0.082/0.160 ms
```

Download the file `system.bin` from the TFTP server.

```
<boot> tftp 1.2.1.1 get system.bin flash:/system.bin
```

Check whether the version of `system.bin` matches that of `boot.bin`.

```
<boot> display install package flash:/system.bin
```

```
flash:/ system.bin
```

```
 [Package]
```

```
 Vendor: HP
```

```
 Product: 5900_5920
```

```
 Service name: system
```

```
 Platform version: 7.1.035
```

```
 Product version: ESS 2206P05002
```

```
 Supported board: mpu
```

Load the system image to start the Comware system.

```
<boot> install load flash:/system.bin
```

```
Check package flash:/system.bin ...
```

```
Extracting package ...
```

```
Loading...
```

```
User interface aux0 is available.
```

Press ENTER to get started.

Automatic configuration

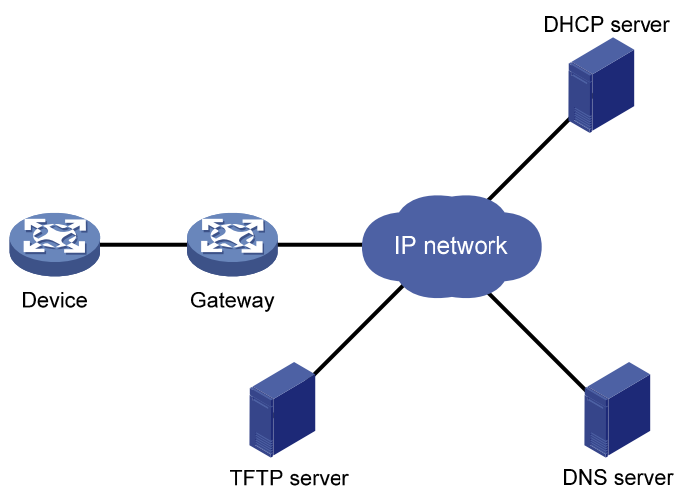
With the automatic configuration feature, the device can automatically obtain a set of configuration settings from some servers when it starts up without a configuration file. This feature simplifies network configuration, facilitates centralized management, and reduces maintenance workload.

Automatic configuration cannot be used for automatic IRF fabric setup.

Understanding automatic configuration

The automatic configuration feature requires the cooperation of the following servers: a DHCP server, a TFTP server, and a DNS server, as shown in Figure 29.

Figure 29 Typical automatic configuration network diagram



When the device is powered on without a configuration file, it automatically starts the automatic configuration process to try to obtain a set of configuration settings. If one attempt fails, the device waits for two minutes and then automatically starts the process again for another attempt. The device continues to make attempts until it gets a set of configuration settings or it is powered off.

Overall automatic configuration process

Overall, the automatic configuration process includes the following steps:

1. The device selects an interface for automatic configuration.
If there are Ethernet interfaces in up state (for example, the management Ethernet interface), the device prefers the VLAN interface of the default VLAN.
2. After finding an interface for automatic configuration, the device enables the DHCP client on the interface and tries to locate a DHCP server and obtain a set of parameters for automatic configuration, which might include a temporary IP address, a host name, a configuration file name, a TFTP server domain name, a TFTP server IP address, and a DNS server IP address. For more information, see "Automatic-configuration parameter acquisition process."

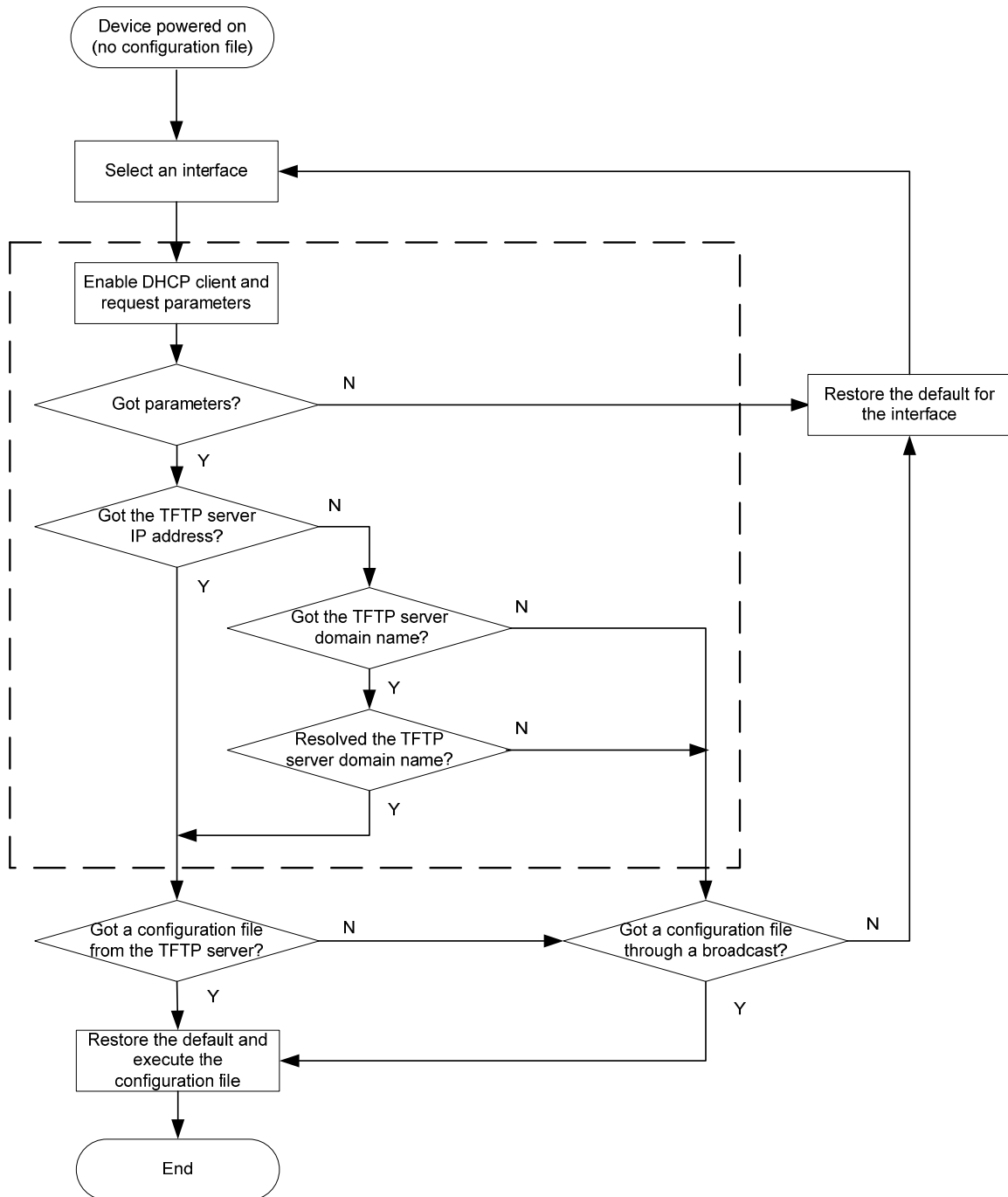
3. After getting automatic configuration parameters, the device tries to download a configuration file from a TFTP server. For more information, see "Configuration file acquisition process."
4. If the device gets a configuration file, it deletes its temporary settings to restore the factory defaults and then executes the configuration file. Otherwise, the device deletes its temporary settings, select another interface for automatic configuration, and repeats Step 2 to Step 4.

ⓘ **IMPORTANT:**

- To ensure quick and successful automatic configuration of a device, connect only the interface used for automatic configuration to the network.
 - The configuration file is deleted after being executed. After the device completes the automatic configuration process, save the configuration by using the **save** command. Otherwise, the device has to perform automatic configuration again after reboot. For more information about the **save** command, see *Fundamentals Command Reference*.
-

Figure 30 shows the automatic configuration workflow.

Figure 30 Automatic configuration workflow



Automatic-configuration parameter acquisition process

After the device finds an interface for automatic configuration, it enables the DHCP client on the interface. Then, the DHCP client broadcasts a DHCP request to locate a DHCP server and request configuration settings. The DHCP request contains DHCP Option 55, which indicates the configuration settings the device requires, including the configuration file name, the TFTP server domain name, the TFTP server IP address, and the DNS server IP address.

After the device obtains an IP address, it resolves the received DHCP reply to examine the following fields:

- **Option 67** or the **file** field—Carries the configuration file name. The device resolves Option 67 first. If Option 67 does not contain the configuration file name, the device resolves the **file** field.
- **Option 12**—Carries the host name. This host name might be used to determine the configuration file name, which is in the format *host name.cfg*.
- **Option 150**—Carries the TFTP server IP address. If this option contains a valid TFTP server IP address, the device starts the configuration file acquisition process. Otherwise, the device resolves Option 66.
- **Option 66**—Carries the TFTP server domain name. If Option 150 does not contain a TFTP server IP address, the device resolves this option for a TFTP server domain name and tries to communicate with the DNS server indicated by Option 6 to get the TFTP server IP address.
- **Option 6**—Carries the DNS server IP address.

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

Configuration file acquisition process

During the automatic-configuration parameter acquisition process, the device might or might not get a TFTP server IP address:

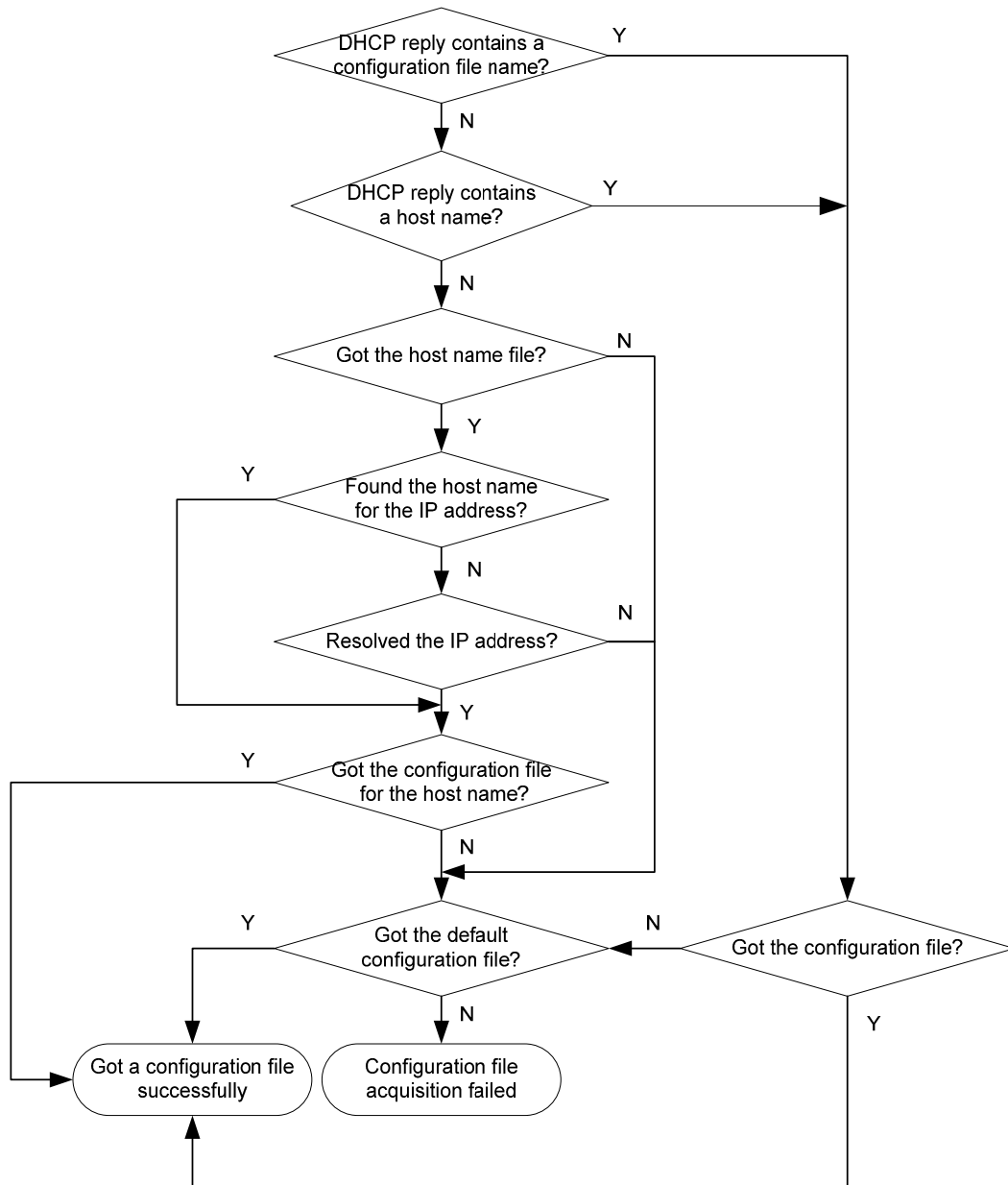
- If the device gets a TFTP server IP address, it starts the configuration file acquisition process by unicasting a request to the TFTP server.
- If not, the device starts the configuration file acquisition process by broadcasting a request. In this case, the device resolves only the first reply.

As shown in Figure 31, the device determines what to request from the TFTP server based on whether or not it got a configuration file name during the automatic-configuration parameter acquisition process:

- If the device got a configuration file name, it requests the specified configuration file.
- If not, it requests a configuration file named in the format *host name.cfg* from the TFTP server, where *host name* represents the host name of the device. If the device got no host name during the automatic-configuration parameter acquisition process, it first requests the host name file **network.cfg**, which contains mappings between IP addresses and host names. If the device fails to get the host name file or the file contains no entry for the device's temporary IP address, it tries to communicate with a DNS server to resolve the temporary IP address to a host name. After the device gets the host name, it tries to obtain the configuration file for the host name.

If the device fails to get a configuration file specific for itself, it requests the default configuration file *device.cfg* from the TFTP server.

Figure 31 Configuration file acquisition process



Deploying and configuring servers for automatic configuration

To implement automatic configuration, you do not need to perform any configuration on the device. However, you must deploy DHCP, TFTP, and DNS servers and properly configure the servers to cooperate with the device as follows:

- **DHCP server**—Assigns the device a set of parameters for automatic configuration, which might include a temporary IP address, a host name, a configuration file name, a TFTP server domain name, a TFTP server IP address, and a DNS server IP address. For more information about the DHCP server, see *Layer 3—IP Services Configuration Guide*.

- **TFTP server**—Stores files needed for device automatic configuration, including the configuration files and host name files. For more information about the TFTP server, see "Configuring TFTP."
- **DNS server**—Resolves the device's temporary IP address to its host name so the device can request a configuration file named in the format *host name.cfg* from the TFTP server. The DNS server might also need to resolve the TFTP server domain name to the TFTP server IP address. For more information about the DNS server, see *Layer 3—IP Services Configuration Guide*.

If the DHCP server, the TFTP server, the DNS server, and the device are not in the same network segment, configure the DHCP relay agent on the gateway, and configure routing protocols to make sure the servers have routes to the device and vice versa.

DHCP server configuration guidelines

DHCP server configuration requirements vary depending on whether the devices use the same configuration file:

- If all devices that need to be automatically configured share the same configuration file, configure the dynamic address allocation mechanism on the DHCP server. To allow these devices to have some different configurations, you can put the configurations that the devices share to the configuration file and provide a way for device administrators to change the configurations after the devices start up. For example, you can configure a configuration file that enables the Telnet service and creates a local user so administrators can Telnet to their devices to perform specific configurations after their devices start up.
- If different devices need different configurations, configure the static address and parameter allocation mechanism on the DHCP server so the server assigns pre-configured IP addresses and parameters to the devices. With this method, you can configure all configuration items required for each device on the DHCP server.

Before you configure a static binding for a device, you must obtain the client ID of the device. To do so, ask the device administrator to turn on the device and, after the device starts up, execute the **display dhcp server ip-in-use** command on the DHCP server to view the client ID of the device.

After you complete the static binding configuration, ask the device administrator to turn off the device and then turn on it again so the device gets the IP address and configuration parameters you configured for it.

TFTP server configuration guidelines

You must configure the configuration files and host name files required for device automatic configuration on the TFTP server, including the default configuration file named *device.cfg*.

To use the host name file **network.cfg**, configure a configuration file for each device on the TFTP server, name the file in the format *host name.cfg*, and configure a mapping entry in the format **ip host** *host-name ip-address* for the host name file. For example, you can configure the following entries for the host name file:

```
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
```

If a device resides in a network different than the TFTP server, configure the UDP helper function on the gateway so the gateway changes the broadcast TFTP request from the device to a unicast packet and forwards the unicast packet to the TFTP server. For more information about UDP helper, see *Layer 3—IP Services Configuration Guide*.

Configuring Tcl

Comware V7 provides a built-in tool command language (Tcl) interpreter. You can execute Tcl commands on the device.

From user view, you can use the **tclsh** command to enter Tcl configuration view, where you can execute the following commands:

- All Tcl 8.5 commands.
- Comware commands. In this case, the Tcl configuration view is equivalent to the user view. You can use Comware commands in Tcl configuration view in the same way that you do in user view.

Restrictions and benefits

Unlike Comware commands, which support features such as online help and history command buffering, Tcl commands have the following restrictions:

- No online help information is provided for Tcl commands.
- You cannot press **Tab** to complete a partly-input Tcl command.
- Successfully executed Tcl commands are not saved to command history buffers.

However, Tcl commands provide the following benefits:

- Tcl environment variables can be applied to Comware commands.
- You can enter multiple Comware commands separated by semi-colons to execute the commands in the order they are entered.

For more information about Comware command usage, see "Using the CLI."

Entering Tcl configuration view from user view

Task	Command
Enter Tcl configuration view from user view.	tclsh

Returning from Tcl configuration view to user view

Task	Command
Return from Tcl configuration view to user view.	tclquit

Support and other resources

Contacting HP

For worldwide technical support information, see the HP support website:

<http://www.hp.com/support>

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

<http://www.hp.com/go/wwalerts>

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Related information

Documents

To find related documents, browse to the Manuals page of the HP Business Support Center website:

<http://www.hp.com/support/manuals>

- For related documentation, navigate to the Networking section, and select a networking category.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Websites

- HP.com <http://www.hp.com>
- HP Networking <http://www.hp.com/go/networking>
- HP manuals <http://www.hp.com/support/manuals>
- HP download drivers and software <http://www.hp.com/support/downloads>
- HP software depot <http://www.software.hp.com>
- HP Education <http://www.hp.com/learn>

Conventions

This section describes the conventions used in this documentation set.





Command conventions

Convention	Description
Boldface	Bold text represents commands and keywords that you enter literally as shown.
<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
Boldface	Window names, button names, field names, and menu items are in bold text. For example, the New User window appears; click OK .
>	Multi-level menus are separated by angle brackets. For example, File > Create > Folder .

Symbols

Convention	Description
 WARNING	An alert that calls attention to important information that if not understood or followed can result in personal injury.
 CAUTION	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
 TIP	An alert that provides helpful information.

Network topology icons



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



Represents a routing-capable device, such as a router or Layer 3 switch.



Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.

Port numbering in examples

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

Index

? (CLI online help access), 2

AAA

- default user role function, 44

- RBAC AAA authorization, 40

- RBAC local AAA authentication user configuration, 47

- RBAC user role local AAA authentication assignment, 44

- RBAC user role remote AAA authentication assignment, 44

abbreviating command, 4

accessing

- device through SNMP, 31

accessing CLI online help, 2

accounting

- command accounting configuration, 36

- user access control, 33

ACL

- command accounting, 36

- command authorization, 35, 36

- SNMP access control, 34

- SSH login control, 33

- Telnet login control, 33

- user access control, 33

active (PORT) FTP operating mode, 57

airflow direction configuration, 111

alias (command keyword), 4

archiving configuration

- automatic, 77

- manual, 78

argument

- CLI string/text type argument value entry, 4

ASCII transfer mode, 57

assigning

- RBAC local AAA authentication user role, 44

- RBAC non-AAA authentication user role, 45

- RBAC remote AAA authentication user role, 44

- RBAC user role, 43

authenticating

- console login none authentication, 20

- console login password authentication, 20

- console login scheme authentication, 21

- FTP basic server server authentication, 58

- none CLI authentication mode, 19

- password CLI authentication mode, 19

- RBAC HWTACACS authentication user configuration, 52

- RBAC local AAA authentication user configuration, 47

- RBAC RADIUS authentication user configuration, 49

- RBAC user role local AAA authentication assignment, 44

- RBAC user role remote AAA authentication assignment, 44

- RBAC user role switching authentication configuration, 46

- scheme CLI authentication mode, 19

- Telnet login none authentication, 23

- Telnet login password authentication, 24

- Telnet login scheme authentication, 25

authorizing

- command authorization configuration, 35, 36

- FTP basic server server authorization, 58

- user access control, 33

- automatic configuration, 125
 - configuration file acquisition process, 128
 - DHCP server configuration guideline, 130
 - network diagram, 125
 - overall process, 125
 - parameter acquisition process, 127
 - TFTP server configuration guideline, 130
- AUX
 - CLI local console port login, 19
 - common user interface settings, 21
 - console login none authentication, 20
 - console login password authentication, 20
 - console login scheme authentication, 21
 - login management overview, 14
- backup next-startup configuration file
 - deleting, 80
 - specifying, 79
- backup software image set, 82
- banner
 - configuration, 103, 104
 - incoming type, 103
 - legal type, 103
 - login type, 103
 - MOTD type, 103
 - multiple-line input mode, 103
 - shell type, 103
 - single-line input mode, 103
- binary transfer mode, 57
- boot loader
 - displaying software image settings, 88
- Boot ROM
 - preloading software image to Boot ROM, 85
 - preparing for upgrade, 85
 - software image type, 82
 - system startup process, 83
- upgrade methods, 84
- changing
 - file system current working directory, 71
 - RBAC resource access policies, 42
 - RBAC user role interface policy, 42
 - RBAC user role VLAN policy, 43
 - RBAC user role VPN instance policy, 43
- checking server connectivity, 120
- CLI
 - command abbreviation, 4
 - command entry, 3
 - command history function use, 7
 - command hotkey use, 5
 - command keyword alias configuration, 4
 - command keyword alias use, 4
 - command keyword hotkey configuration, 5
 - command redisplay, 6
 - command-line error messages, 6
 - common AUX user interface settings, 21
 - console none authentication, 20
 - console password authentication, 20
 - console port login procedure, 15
 - console scheme authentication, 21
 - disabling pause in screen output, 8
 - display command output filtering, 9
 - display command output line numbering, 9
 - display command output management, 13
 - display command output save to file, 11
 - display command output viewing, 13
 - displaying login, 29
 - emergency shell file system management, 118
 - emergency shell system software image retrieval, 119
 - emergency shell use, 118, 122
 - enter system view from user view, 2
 - file system current working directory change, 71

- file system current working directory display, 71
- file system directory creation, 71
- file system directory management, 71
- file system directory removal, 71
- file system file information display, 69
- file system file management, 69
- file system file/folder operation mode, 72
- file system storage media formatting, 72
- file system storage media management, 72
- file system storage media repair, 72
- local console port login, 19
- login authentication modes, 19
- login management overview, 14
- login overview, 18
- maintaining login, 29
- online help access, 2
- output control, 8
- pausing screen output, 8
- return to upper-level view from any view, 2
- return to user view, 2
- running configuration save, 13
- string/text type argument value entry, 4
- undo command form, 3
- use, 1
- user interfaces, 18
- user roles, 19
- view hierarchy, 1

command

- accounting, 36
- authorization, 35, 36
- CLI command abbreviation, 4
- CLI command entry, 3
- CLI command history function use, 7
- CLI command hotkey configuration, 5
- CLI command hotkey use, 5
- CLI command keyword alias configuration, 4
- CLI command keyword alias use, 4
- CLI command redisplay, 6
- CLI string/text type argument value entry, 4
- CLI undo command form, 3

command language (Tcl), 131

command line interface. *Use* CLI

completing

- software upgrade, 86

compressing file, 70

Comware

- image loading procedure, 82
- image redundancy, 82

configuration

- automatic configuration, 125
- saving running configuration, 75
- types, 73

configuration (device)

- factory default, 73
- running, 73
- startup, 73

configuration archive

- automatic, 77
- configuration guidelines, 77
- configuring archive parameters, 76
- enabling automatic archiving, 77
- manual archiving, 78

configuration encryption

- enabling, 75
- private key approach, 75
- public key approach, 75

configuration file

- automatic configuration, 125
- content, 74
- displaying, 81

- encryption, 75
- file extension, 73, 74
- format, 74
- management, 73
- overview, 73
- redundancy, 73
- saving running configuration, 75
- specifying next-startup file, 79
- startup file selection, 74
- configuration file management
 - configuration file content, 74
 - configuration file format, 74
 - configuration types, 73
 - displaying configuration files, 81
 - specifying next-startup configuration file, 79
- configuration management
 - automatic configuration archiving, 77
 - configuration archive, 76
 - configuration rollback, 76
 - enabling configuration encryption, 75
 - manual configuration archiving, 78
 - performing configuration rollback, 78
 - saving running configuration, 75
- configuration redundancy
 - backing up to TFTP server, 79
 - restoring from TFTP server, 80
- configuration rollback, 99
 - automatic configuration archiving, 77
 - configuring, 76
 - configuring archive parameters, 76
 - how it works, 76
 - manual configuration archiving, 78
 - performing, 78
 - task list, 76
- configuration view
 - entering from user view, 131
 - returning to user view, 131
- configuring
 - airflow direction, 111
 - banner, 103, 104
 - CLI local console port login, 19
 - command accounting, 36
 - command authorization, 35, 36
 - command keyword alias, 4
 - command keyword hotkey, 5
 - common AUX user interface settings, 21
 - common VTY user interface settings, 26
 - configuration archive parameters, 76
 - configuration rollback, 76
 - console login none authentication, 20
 - console login password authentication, 20
 - console login scheme authentication, 21
 - device as IPv4 TFTP client, 66
 - device as IPv6 TFTP client, 66
 - device management parameters, 102
 - device name, 102
 - FTP, 57
 - FTP basic server parameters, 57
 - FTP client, 64
 - FTP server, 59
 - FTP server authentication, 58
 - FTP server authorization, 58
 - management Ethernet interface, 119
 - RBAC, 38, 40
 - RBAC feature group, 42
 - RBAC for HWTACACS authentication user (on switch), 52
 - RBAC for RADIUS authentication user, 49
 - RBAC local AAA authentication user, 47
 - RBAC user role rules, 41
 - RBAC user role switching, 45

- RBAC user role switching authentication, 46
- server for automatic configuration, 129
- SNMPv2 access, 32
- SNMPv3 access, 31
- SSH login, 28
- SSH login on device, 28
- Telnet login, 22
- Telnet login none authentication, 23
- Telnet login on device, 23
- Telnet login password authentication, 24
- Telnet login scheme authentication, 25
- temperature alarm thresholds, 114
- TFTP, 66
- configuring Tcl, 131
- console port
 - CLI console none authentication, 20
 - CLI local console port login, 19
 - common AUX user interface settings, 21
 - login procedure, 15
 - password authentication, 20
 - scheme authentication, 21
- content of configuration file, 74
- controlling
 - SNMP access, 34
 - SSH logins, 33
 - Telnet logins, 33
 - user access, 33
- controlling CLI output, 8
- copying file, 69
- copyright statement display, 103
- creating
 - file system directory, 71
 - RBAC user role, 40
- decompressing file, 70
- deleting
 - file, 70
 - file from recycle bin, 70
- deploying
 - server for automatic configuration, 129
- detection timer, 112
- device
 - access through SNMP, 31
 - automatic configuration, 125
 - CLI command abbreviation, 4
 - CLI command entry, 3
 - CLI command history function use, 7
 - CLI command hotkey use, 5
 - CLI command hotkeyconfiguration, 5
 - CLI command keyword alias configuration, 4
 - CLI command keyword alias use, 4
 - CLI command redisplay, 6
 - CLI command-line error messages, 6
 - CLI display command output filtering, 9
 - CLI display command output line numbering, 9
 - CLI display command output management, 13
 - CLI display command output save to file, 11
 - CLI display command output viewing, 13
 - CLI online help access, 2
 - CLI output control, 8
 - CLI running configuration save, 13
 - CLI string/text type argument value entry, 4
 - CLI undo command form, 3
 - CLI use, 1
 - CLI view hierarchy, 1
 - configuration types, 73
 - displaying command help information, 63
 - emergency shell management Ethernet interface configuration, 119
 - emergency shell reboot, 121
 - emergency shell server connectivity check, 120

- emergency shell system software image transfer from server, 120
- emergency shell system software image upload, 121
- emergency shell use, 118, 122
- enter system view from user view, 2
- factory default configuration, 73
- file system current working directory change, 71
- file system current working directory display, 71
- file system directory creation, 71
- file system directory management, 71
- file system directory removal, 71
- file system file compression, 70
- file system file copy, 69
- file system file decompression, 70
- file system file delete from recycle bin, 70
- file system file deletion, 70
- file system file information display, 69
- file system file management, 69
- file system file move, 70
- file system file name formats, 68
- file system file rename, 69
- file system file restore, 70
- file system management, 68
- file system storage media formatting, 72
- file system storage media management, 72
- file system storage media repair, 72
- file system text file content display, 69
- FTP basic server parameters configuration, 57
- FTP client, 60
- FTP client configuration, 64
- FTP client connection establishment, 60
- FTP configuration, 57
- FTP manual server connection release, 58
- FTP server, 57
- FTP server authentication, 58
- FTP server authorization, 58
- FTP server configuration, 59
- FTP server directory management, 61
- FTP server files, 61
- FTP user account switch, 63
- IPv4 TFTP client configuration, 66
- IPv6 TFTP client configuration, 66
- ISSU command series, 91
- ISSU guidelines, 92
- ISSU overview, 90
- ISSU prerequisites, 92
- ISSU restrictions, 92
- obtaining IPE file software images (ISSU), 98
- performing ISSU by install series commands, 98
- performing ISSU by issu series commands, 94
- return to upper-level view from any view, 2
- return to user view, 2
- running configuration, 73
- software upgrade, 82
- SSH login configuration on device, 28
- SSH server login, 29
- startup configuration, 73
- system startup process, 83
- Telnet login device configuration, 23
- terminating FTP connection, 63
- TFTP configuration, 66
- troubleshooting FTP connection, 63
- using for Telnet server login, 27
- device management
 - airflow direction configuration, 111
 - banner configuration, 103, 104
 - banner input modes, 103
 - banner types, 103
 - configuration, 102
 - copyright statement display, 103

- device name configuration, 102
 - device reboot, 105
 - device reboot (immediately at CLI), 106
 - device reboot (scheduling), 106
 - displaying configuration, 116
 - maintaining configuration, 116
 - memory usage thresholds, 112
 - port status detection timer, 112
 - system operating mode, 105
 - system time set, 102
 - task scheduling, 106, 108
 - temperature alarm thresholds, 114
 - transceiver module diagnosis, 115, 116
 - transceiver module verification, 115
 - USB interface disable, 115
- DHCP
- automatic configuration, 125
- diagnosing transceiver modules, 115, 116
- directory
- file system current working directory change, 71
 - file system current working directory display, 71
 - file system directory creation, 71
 - file system directory management, 71
 - file system directory removal, 71
 - file system management, 68
 - FTP server directory management, 61
- disabling
- USB interfaces, 115
- disabling pause between CLI output screens, 8
- displaying
- command help information, 63
 - configuration files, 81
 - copyright statement, 103
 - device management configuration, 116
 - file system current working directory display, 71
 - file system file information, 69
 - file system text file content, 69
 - FTP client, 64
 - FTP server, 58
 - displaying CLI login, 29
 - displaying device information in emergency shell mode, 121
 - displaying ISSU, 97, 101
 - displaying RBAC settings, 47
 - displaying software image settings, 88
- DNS
- automatic configuration, 125
- emergency shell, 82
- device reboot, 121
 - displaying device information, 121
 - file system management, 118
 - management Ethernet interface configuration, 119
 - server connectivity check, 120
 - system software image, 119
 - system software image transfer from server, 120
 - system software image upload, 121
 - use, 118, 122
- enabling
- default user role function, 44
- enabling
- automatic configuration archiving, 77
 - command redisplay, 6
 - configuration encryption, 75
 - copyright statement display, 103
- entered-but-not-submitted command redisplay, 6
- entering
- command, 3
 - string/text type argument value, 4
 - system view from user view, 2
- entering Tcl configuration view, 131

- error message (command-line), 6
- establishing
 - FTP client connection, 60
- Ethernet
 - emergency shell management Ethernet interface configuration, 119
- factory default (device configuration), 73
- feature group
 - RBAC feature group configuration, 42
- file
 - FTP server files, 61
 - managing (configuration), 73
 - system. *See* file system
- file system
 - current working directory change, 71
 - current working directory display, 71
 - directory creation, 71
 - directory management, 71
 - directory removal, 71
 - file compression, 70
 - file copy, 69
 - file decompression, 70
 - file delete from recycle bin, 70
 - file information display, 69
 - file management, 69
 - file move, 70
 - file name formats, 68
 - file rename, 69
 - file restore, 70
 - file/folder operation mode, 72
 - management, 68
 - storage media formatting, 72
 - storage media management, 72
 - storage media repair, 72
 - text file content display, 69
- file system management, 118
- File Transfer Protocol. *Use* FTP
- filtering CLI display command output, 9
- format
 - file name, 68
 - file system storage media, 72
- format of configuration file, 74
- FTP
 - basic server parameters configuration, 57
 - client configuration, 64
 - client connection establishment, 60
 - configuration, 57
 - device as client, 60
 - device as server, 57
 - displaying client, 64
 - displaying command help information, 63
 - displaying server, 58
 - emergency shell system software image retrieval, 119
 - emergency shell system software image transfer from server, 120
 - IPv4 TFTP client configuration, 66
 - IPv6 TFTP client configuration, 66
 - local server authentication, 58
 - local server authorization, 58
 - maintaining connection, 63
 - manual server connection release, 58
 - remote server authentication, 58
 - remote server authorization, 58
 - server configuration, 59
 - server directory management, 61
 - server files, 61
 - terminating connection, 63
 - TFTP configuration, 66
 - troubleshooting connection, 63
 - user account switch, 63
- guideline

- configuring DHCP server for automatic configuration, 130
 - configuring TFTP server for automatic configuration, 130
- guidelines and restrictions
 - configuration archive, 77
- history function, 7
- hotfix (ISSU), 90
- hotkey (command), 5
- HWTACACS
 - RBAC HWTACACS authentication user configuration, 52
- image
 - Comware image loading procedure, 82
 - Comware image redundancy, 82
 - displaying software image settings, 88
 - installing ISSU software images, 98
 - obtaining software images (ISSU), 98
 - removing ISSU inactive software image, 100
 - rolling back ISSU software configuration, 99
 - uninstalling ISSU patch images, 99
 - upgrading ISSU software images, 98
- inactive software image removal, 100
- incoming banner type, 103
- In-Service Software Upgrade. *See* ISSU
- installing ISSU software images, 98
- interface
 - emergency shell management Ethernet interface configuration, 119
- interface policy, 42
- IP
 - FTP configuration, 57
 - TFTP configuration, 66
- IPE file, 98
- IPv4
 - emergency shell system software image transfer from server, 120
 - FTP client connection establishment, 60
 - TFTP client configuration, 66
- IPv6
 - emergency shell system software image transfer from server, 120
 - FTP client connection establishment, 60
 - TFTP client configuration, 66
- IRF
 - completing software upgrade, 86
 - emergency shell device reboot, 121
 - emergency shell use, 118, 122
 - ISSU command series, 91
 - ISSU guidelines, 92
 - ISSU methods, 90
 - ISSU methods (compatible), 90
 - ISSU methods (incompatible), 91
 - ISSU overview, 90
 - ISSU prerequisites, 92
 - ISSU restrictions, 92
 - non-ISSU software upgrade approach, 88
 - performing ISSU by install series commands, 98
 - performing ISSU by issu series commands, 94
 - preloading software image to Boot ROM, 85
 - verifying software change confirmation status, 100
 - verifying software image integrity and consistency, 100
- ISSU
 - command series, 91
 - Comware image upgrade method, 84
 - displaying, 97, 101
 - emergency shell use, 118, 122
 - guidelines, 92
 - installing software images, 98
 - maintaining, 97, 101
 - methods, 90

- methods (compatible), 90
- methods (incompatible), 91
- non-ISSU software upgrade procedure, 85, 88
- non-ISSU upgrade method, 84
- obtaining IPE file software images, 98
- overview, 90
- performing, 94, 98
- preloading software image to Boot ROM, 85
- prerequisites, 92
- removing inactive software image, 100
- restrictions, 92
- rolling back software configuration, 99
- uninstalling patch images, 99
- upgrading software images, 98
- verifying software change confirmation status, 100
- verifying software image integrity and consistency, 100
- ISSU method
 - compatible, 90
 - incompatible, 91
 - overview, 90
- keyword alias configuration, 4
- legal banner type, 103
- loading system software image, 121
- local
 - AAA authentication user role assignment, 44
 - RBAC local AAA authentication user configuration, 47
- logging in
 - CLI, 18
 - CLI console none authentication, 20
 - CLI local console port login, 19
 - CLI login authentication modes, 19
 - CLI user interfaces, 18
 - CLI user roles, 19
 - common AUX user interface settings, 21
 - common VTY user interface settings, 26
 - console password authentication, 20
 - console port, 15
 - console scheme authentication, 21
 - SSH login, 28
 - SSH login configuration on device, 28
 - SSH server login, 29
 - Telnet login, 22
 - Telnet login device configuration, 23
 - Telnet login none authentication, 23
 - Telnet login password authentication, 24
 - Telnet login scheme authentication, 25
 - Telnet server login, 27
- login banner type, 103
- login management
 - CLI access, 18
 - CLI local console port login, 19
 - CLI login authentication modes, 19
 - CLI user interfaces, 18
 - CLI user roles, 19
 - common AUX common user interface settings, 21
 - common VTY user interface settings, 26
 - console none authentication, 20
 - console password authentication, 20
 - console port access, 15
 - console scheme authentication, 21
 - overview, 14
 - SSH login, 28
 - SSH login on device, 28
 - SSH server login, 29
 - Telnet login, 22
 - Telnet login device configuration, 23
 - Telnet login none authentication, 23
 - Telnet login password authentication, 24

- Telnet login scheme authentication, 25
- Telnet server login, 27
- main next-startup configuration file
 - backing up to TFTP server, 79
 - deleting, 80
 - restoring from TFTP server, 80
 - specifying, 79
- main software image set, 82
- maintaining
 - FTP connection, 63
- maintaining CLI login, 29
- maintaining device management configuration, 116
- maintaining ISSU, 97, 101
- management Ethernet interface configuration, 119
- managing
 - configuration files, 73
 - file system directories, 71
 - file system files, 69
 - file system storage media, 72
 - FTP server directories, 61
- managing CLI display command output, 13
- managing devices, 102
- managing file system, 68, 118
- manually releasing FTP server connection, 58
- mechanism
 - configuration rollback, 76
- memory usage thresholds, 112
- message-of-the-day (MOTD) banner type, 103
- method of software upgrade, 82
- MIB
 - device access through SNMP, 31
- mode
 - FTP active (PORT) operating mode, 57
 - FTP ASCII transfer mode, 57
 - FTP binary transfer mode, 57
 - FTP passive (PASV) operating mode, 57
 - system operating mode, 105
- module
 - transceiver module diagnosis, 115, 116
 - transceiver module verification, 115
- moving file, 70
- MPU
 - emergency shell device reboot, 121
 - emergency shell use, 118, 122
- multiple-line banner input mode, 103
- naming
 - file name formats, 68
 - file rename, 69
- network
 - airflow direction configuration, 111
 - banner configuration, 103, 104
 - banner input modes, 103
 - banner types, 103
 - CLI command abbreviation, 4
 - CLI command entry, 3
 - CLI command history function use, 7
 - CLI command hotkey use, 5
 - CLI command keyword alias configuration, 4
 - CLI command keyword alias use, 4
 - CLI command keyword hotkey configuration, 5
 - CLI command redisplay, 6
 - CLI command-line error messages, 6
 - CLI display command output filtering, 9
 - CLI display command output line numbering, 9
 - CLI display command output management, 13
 - CLI display command output save to file, 11
 - CLI display command output viewing, 13
 - CLI online help access, 2
 - CLI output control, 8
 - CLI running configuration save, 13

- CLI string/text type argument value entry, 4
- CLI undo command form, 3
- CLI view hierarchy, 1
- command accounting, 36
- command authorization, 35, 36
- copyright statement display, 103
- device as FTP client, 60
- device as FTP server, 57
- device name configuration, 102
- device reboot, 105
- device reboot (immediately at CLI), 106
- device reboot (scheduling), 106
- displaying command help information, 63
- emergency shell device reboot, 121
- emergency shell management Ethernet interface configuration, 119
- emergency shell server connectivity check, 120
- emergency shell system software image transfer from server, 120
- emergency shell system software image upload, 121
- enter system view from user view, 2
- file system current working directory change, 71
- file system current working directory display, 71
- file system directory creation, 71
- file system directory management, 71
- file system directory removal, 71
- file system file compression, 70
- file system file copy, 69
- file system file decompression, 70
- file system file delete from recycle bin, 70
- file system file deletion, 70
- file system file information display, 69
- file system file management, 69
- file system file move, 70
- file system file name formats, 68
- file system file rename, 69
- file system file restore, 70
- file system storage media formatting, 72
- file system storage media management, 72
- file system storage media repair, 72
- file system text file content display, 69
- FTP basic server parameters configuration, 57
- FTP client configuration, 64
- FTP client connection establishment, 60
- FTP server authentication, 58
- FTP server authorization, 58
- FTP server configuration, 59
- FTP server directory management, 61
- FTP server files, 61
- FTP user account switch, 63
- IPv4 TFTP client configuration, 66
- IPv6 TFTP client configuration, 66
- memory usage thresholds, 112
- port status detection timer, 112
- RBAC default user role function, 44
- RBAC feature group configuration, 42
- RBAC resource access policies, 42
- RBAC user role assignment, 43
- RBAC user role creation, 40
- RBAC user role interface policy, 42
- RBAC user role local AAA authentication assignment, 44
- RBAC user role non-AAA authentication assignment, 45
- RBAC user role remote AAA authentication assignment, 44
- RBAC user role rule configuration, 41
- RBAC user role switching, 46
- RBAC user role switching authentication configuration, 46
- RBAC user role switching configuration, 45
- RBAC user role VLAN policy, 43

- RBAC user role VPN instance policy, 43
- return to upper-level view from any view, 2
- return to user view, 2
- SNMP access control, 34
- SNMPv2 access configuration, 32
- SNMPv3 access configuration, 31
- SSH login control, 33
- system operating mode, 105
- system time set, 102
- task scheduling, 106, 108
- Telnet login control, 33
- temperature alarm thresholds, 114
- terminating FTP connection, 63
- transceiver module diagnosis, 115, 116
- transceiver module verification, 115
- troubleshooting FTP connection, 63
- USB interface disable, 115
- network management
 - automatic configuration, 125
 - CLI use, 1
 - device access through SNMP, 31
 - device management configuration, 102
 - emergency shell use, 118, 122
 - file system management, 68
 - FTP configuration, 57
 - ISSU command series, 91
 - ISSU guidelines, 92
 - ISSU inactive software image removal, 100
 - ISSU methods, 90
 - ISSU methods (compatible), 90
 - ISSU methods (incompatible), 91
 - ISSU overview, 90
 - ISSU patch image uninstallation, 99
 - ISSU prerequisites, 92
 - ISSU restrictions, 92
 - ISSU software image installation, 98
 - ISSU software image upgrade, 98
 - managing configuration files, 73
 - non-ISSU software upgrade procedure, 88
 - obtaining IPE file software images (ISSU), 98
 - performing ISSU by install series commands, 98
 - performing ISSU by issu series commands, 94
 - RBAC configuration, 38, 40
 - RBAC HWTACACS authentication user configuration, 52
 - RBAC local AAA authentication user configuration, 47
 - RBAC permission assignment, 38
 - RBAC RADIUS authentication user configuration, 49
 - RBAC user role assignment, 40
 - rolling back ISSU software configuration, 99
 - software upgrade, 82
 - Tcl configuration, 131
 - TFTP configuration, 66
 - user access control, 33
- NMS
 - device access through SNMP, 31
 - non-AAA authentication user role assignment, 45
 - none
 - CLI authentication mode, 19
 - console login none authentication, 20
 - Telnet login none authentication, 23
 - non-AAA authorization (RBAC), 40
 - numbering CLI display command output lines, 9
 - obtaining IPE file software images, 98
 - obtaining system software image, 119
 - online help access, 2
 - operation mode, 72
 - output
 - control keys (CLI), 8

- controlling, 8
- filtering, 9
- line numbering, 9
- management, 13
- save to file, 11
- viewing, 13
- overview
 - configuration file, 73
 - ISSU, 90
- parameter
 - device management configuration, 102
 - FTP basic server parameters configuration, 57
- passive (PASV) FTP operating mode, 57
- password
 - CLI authentication mode, 19
 - console login password authentication, 20
 - Telnet login password authentication, 24
 - Telnet login scheme authentication, 25
- patch images (ISSU), 99
- pausing between CLI output screens, 8
- performing
 - ISSU by install series commands, 98
 - ISSU by issu series commands, 94
- permitting
 - RBAC permission assignment, 38
 - RBAC predefined user roles, 39
 - RBAC user role assignment, 40
 - RBAC user role rules, 38
- policy
 - RBAC interface access policy, 39
 - RBAC resource access policies, 42
 - RBAC user role assignment, 43
 - RBAC user role interface policy, 42
 - RBAC user role local AAA authentication assignment, 44
 - RBAC user role non-AAA authentication assignment, 45
 - RBAC user role remote AAA authentication assignment, 44
 - RBAC user role VLAN policy, 43
 - RBAC user role VPN instance policy, 43
 - RBAC VLAN access policy, 39
 - RBAC VPN instance access policy, 39
- port status detection timer, 112
- preloading
 - software image to Boot ROM, 85
- procedure
 - abbreviating CLI command, 4
 - accessing CLI online help, 2
 - accessing server to transfer system software image, 120
 - assigning RBAC local AAA authentication user role, 44
 - assigning RBAC non-AAA authentication user role, 45
 - assigning RBAC remote AAA authentication user role, 44
 - assigning RBAC user role, 43
 - backing up configuration file by using TFTP, 79
 - changing current working directory, 71
 - changing RBAC resource access policies, 42
 - changing RBAC user role interface policy, 42
 - changing RBAC user role VLAN policy, 43
 - changing RBAC user role VPN instance policy, 43
 - checking server connectivity, 120
 - completing software upgrade, 86
 - compressing file, 70
 - configuring airflow direction, 111
 - configuring banner, 103, 104
 - configuring CLI command hotkey, 5
 - configuring CLI command keyword alias, 4
 - configuring CLI local console port login, 19

- configuring command accounting, 36
- configuring command authorization, 35, 36
- configuring common AUX user interface settings, 21
- configuring common VTY user interface settings, 26
- configuring configuration archive parameters, 76
- configuring configuration rollback, 76
- configuring console login none authentication, 20
- configuring console login password authentication, 20
- configuring console login scheme authentication, 21
- configuring device as IPv4 TFTP client, 66
- configuring device as IPv6 TFTP client, 66
- configuring device name, 102
- configuring FTP basic server parameters, 57
- configuring FTP client, 64
- configuring FTP server, 59
- configuring FTP server local authentication, 58
- configuring FTP server local authorization, 58
- configuring FTP server remote authentication, 58
- configuring FTP server remote authorization, 58
- configuring management Ethernet interface, 119
- configuring RBAC, 40
- configuring RBAC feature group, 42
- configuring RBAC for HWTACACS authentication user, 52
- configuring RBAC for RADIUS authentication user, 49
- configuring RBAC local AAA authentication user, 47
- configuring RBAC user role rules, 41
- configuring RBAC user role switching, 45
- configuring RBAC user role switching authentication, 46
- configuring SNMPv2 access, 32
- configuring SNMPv3 access, 31
- configuring SSH login, 28
- configuring SSH login on device, 28
- configuring Telnet login, 22
- configuring Telnet login none authentication, 23
- configuring Telnet login on device, 23
- configuring Telnet login password authentication, 24
- configuring Telnet login scheme authentication, 25
- configuring temperature alarm thresholds, 114
- controlling CLI output, 8
- controlling SNMP access, 34
- controlling SSH logins, 33
- controlling Telnet logins, 33
- copying file, 69
- creating directory, 71
- creating RBAC user role, 40
- decompressing file, 70
- deleting file, 70
- deleting file from recycle bin, 70
- deleting next-startup configuration file, 80
- diagnosing transceiver module, 115, 116
- disabling pause between CLI output screens, 8
- disabling USB interfaces, 115
- displaying CLI login, 29
- displaying command help information, 63
- displaying configuration files, 81
- displaying current working directory, 71
- displaying device information in emergency shell mode, 121
- displaying device management configuration, 116
- displaying file information, 69
- displaying FTP client, 64
- displaying FTP server, 58
- displaying ISSU, 97, 101

- displaying RBAC settings, 47
- displaying software image settings, 88
- displaying text file content, 69
- enabling automatic configuration archiving, 77
- enabling CLI redisplay of entered-but-not-submitted command, 6
- enabling configuration encryption, 75
- enabling copyright statement display, 103
- enabling default user role function, 44
- entering CLI command, 3
- entering CLI string/text type argument value, 4
- entering system view from user view, 2
- entering Tcl configuration view, 131
- establishing FTP client connection, 60
- filtering CLI display command output, 9
- formatting file system storage media, 72
- installing ISSU software images, 98
- maintaining CLI login, 29
- maintaining device management configuration, 116
- maintaining FTP connection, 63
- maintaining ISSU, 97, 101
- managing CLI display command output, 13
- managing file system, 118
- managing file system directories, 71
- managing file system files, 69
- managing file system storage media, 72
- managing FTP server directories, 61
- manually archiving running configuration, 78
- manually releasing FTP server connection, 58
- moving file, 70
- numbering CLI display command output lines, 9
- obtaining IPE file's software images (ISSU), 98
- obtaining system software image, 119
- pausing between CLI output screens, 8
- performing configuration rollback, 78
- performing ISSU by install series commands, 98
- performing ISSU by issu series commands, 94
- preloading software image to Boot ROM, 85
- preparing for non-ISSU software upgrade, 85
- preparing for non-ISSU upgrade, 85
- rebooting device, 105
- rebooting device (immediately at CLI), 106
- rebooting device (scheduling), 106
- removing directory, 71
- removing ISSU inactive software image, 100
- renaming file, 69
- repairing file system storage media, 72
- restoring configuration file by using TFTP, 80
- restoring file, 70
- returning to upper-level view from any view, 2
- returning to user view, 2, 131
- rolling back ISSU software configuration, 99
- saving CLI display command output to file, 11
- saving running configuration, 13, 75
- scheduling task, 106, 108
- setting file/folder operation mode, 72
- setting memory usage thresholds, 112
- setting port status detection timer, 112
- setting system operating mode, 105
- setting system time, 102
- specifying next-startup configuration file, 79
- switching FTP user accounts, 63
- switching RBAC user role, 46
- terminating FTP connection, 63
- troubleshooting FTP connection, 63
- understanding CLI command-line error messages, 6
- uninstalling ISSU patch images, 99
- upgrading ISSU software images, 98
- upgrading software with non-ISSU approach, 85, 88

- using CLI command history function, 7
- using CLI command hotkey, 5
- using CLI command keyword alias, 4
- using CLI undo command form, 3
- using device for SSH server login, 29
- using device for Telnet server login, 27
- using emergency shell, 122
- verifying software change confirmation status, 100
- verifying software image integrity and consistency, 100
- verifying transceiver module, 115
- viewing CLI display command output, 13
- working with FTP server files, 61

process

- automatic-configuration parameter acquisition, 127
- configuration file acquisition, 128
- overall automatic configuration, 125

process (system startup), 83

RADIUS

- RBAC RADIUS authentication user configuration, 49

RBAC

- AAA authorization, 40
- configuration, 38, 40
- default user role function, 44
- displaying settings, 47
- feature group configuration, 42
- HWTACACS authentication user configuration (on switch), 52
- local AAA authentication user configuration, 47
- none-AAA authorization, 40
- permission assignment, 38
- predefined user roles, 39
- RADIUS authentication user configuration, 49
- resource access policies, 39, 42
- troubleshooting, 55
- troubleshooting local users have more access permissions than intended, 55
- troubleshooting login attempts by RADIUS users always fail, 56
- user role assignment, 40, 43
- user role creation, 40
- user role interface policy, 42
- user role local AAA authentication assignment, 44
- user role non-AAA authentication assignment, 45
- user role remote AAA authentication assignment, 44
- user role rule configuration, 41
- user role rules, 38
- user role switching, 46
- user role switching authentication configuration, 46
- user role switching configuration, 45
- user role VLAN policy, 43
- user role VPN instance policy, 43

rebooting device, 105, 121

- reboot immediately at CLI, 106
- scheduling device reboot, 106

redundancy

- backup next-startup configuration file, 73
- main next-startup configuration file, 73
- startup configuration file, 73

remote AAA authentication user role assignment, 44

removing

- file system directory, 71

removing ISSU inactive software image, 100

renaming file, 69

repairing

- file system storage media, 72

resource access policies, 42

- restoring file, 70
- restriction
 - Tcl, 131
- returning
 - to upper-level view from any view, 2
 - to user view, 2
- returning to user view, 131
- role-based access control. See RBAC
- rolling back
 - ISSU software configuration, 99
- routing
 - FTP configuration, 57
 - TFTP configuration, 66
- rule
 - RBAC command rule, 38
 - RBAC feature execute rule, 38
 - RBAC feature group rule, 38
 - RBAC feature read rule, 38
 - RBAC feature write rule, 38
 - RBAC user role rule configuration, 41
- running (device configuration), 73
- running configuration, 13
 - archiving, 76
 - encryption, 75
 - rollback, 76
 - saving (fast mode), 75
 - saving (safe mode), 75
- saving
 - CLI display command output to file, 11
 - CLI running configuration, 13
 - running configuration, 75
- scheduling task, 106, 108
- scheme
 - AUX common user interface settings, 21
 - CLI authentication mode, 19
 - console login scheme authentication, 21
- security
 - command accounting, 36
 - command authorization, 35, 36
 - RBAC configuration, 38, 40
 - RBAC default user role function, 44
 - RBAC feature group configuration, 42
 - RBAC HWTACACS authentication user configuration, 52
 - RBAC local AAA authentication user configuration, 47
 - RBAC permission assignment, 38
 - RBAC predefined user roles, 39
 - RBAC RADIUS authentication user configuration, 49
 - RBAC resource access policies, 39, 42
 - RBAC user role assignment, 40, 43
 - RBAC user role creation, 40
 - RBAC user role interface policy, 42
 - RBAC user role local AAA authentication assignment, 44
 - RBAC user role non-AAA authentication assignment, 45
 - RBAC user role remote AAA authentication assignment, 44
 - RBAC user role rule configuration, 41
 - RBAC user role rules, 38
 - RBAC user role switching, 46
 - RBAC user role switching authentication configuration, 46
 - RBAC user role switching configuration, 45
 - RBAC user role VLAN policy, 43
 - RBAC user role VPN instance policy, 43
 - SNMP access control, 34
 - SSH login control, 33
 - Telnet login control, 33
 - USB interface disable, 115
 - user access control, 33

- security (configuration)
 - enabling configuration encryption, 75
- server connectivity check, 120
- setting
 - memory usage thresholds, 112
 - port status detection timer, 112
 - system operating mode, 105
 - system time, 102
- setting file/folder operation mode, 72
- shell banner type, 103
- single-line banner input mode, 103
- SNMP
 - access control, 34
 - device access, 31
 - login management overview, 14
 - SNMPv2 access configuration, 32
 - SNMPv3 access configuration, 31
- SNMPv1
 - device access through SNMP, 31
- SNMPv2
 - access configuration, 32
 - device access through SNMP, 31
- SNMPv3
 - access configuration, 31
 - device access through SNMP, 31
- software
 - Boot ROM image type, 82
 - completing upgrade, 86
 - Comware Boot image type, 82
 - Comware image loading procedure, 82
 - Comware image redundancy, 82
 - Comware image type, 82
 - Comware patch package, 82
 - Comware system image type, 82
 - displaying image settings, 88
 - file naming, 82
 - installing ISSU software images, 98
 - ISSU command series, 91
 - ISSU guidelines, 92
 - ISSU methods, 90
 - ISSU methods (compatible), 90
 - ISSU methods (incompatible), 91
 - ISSU overview, 90
 - ISSU prerequisites, 92
 - ISSU restrictions, 92
 - non-ISSU upgrade procedure, 85, 88
 - obtaining IPE file software images (ISSU), 98
 - performing ISSU by install series commands, 98
 - performing ISSU by issu series commands, 94
 - preloading image to Boot ROM, 85
 - preparing for non-ISSU upgrade, 85
 - removing ISSU inactive software image, 100
 - rolling back ISSU software configuration, 99
 - uninstalling ISSU patch images, 99
 - upgrade, 82
 - upgrade methods, 84
 - upgrading ISSU software images, 98
- software update
 - emergency shell system software image retrieval, 119
 - emergency shell system software image upload, 121
 - emergency shell use, 118, 122
- specifying
 - backup next-startup configuration file, 79
 - main next-startup configuration file, 79
- SSH
 - login, 28
 - login configuration on device, 28
 - login control, 33
 - login management overview, 14

- server login, 29
- startup
 - preloading software image to Boot ROM, 85
 - system startup process, 83
 - upgrading software with non-ISSU approach, 85, 88
- startup (device configuration), 73
 - specifying next-startup file, 79
 - startup file selection, 74
- storage media
 - file system management, 68
 - formatting, 72
 - management, 72
 - repair, 72
- string type argument value, 4
- switch
 - RBAC HWTACACS authentication user configuration, 52
 - RBAC local AAA authentication user configuration, 47
 - RBAC RADIUS authentication user configuration, 49
- switching RBAC user role, 45, 46
- switching to another FTP user account, 63
- system
 - Comware image loading procedure, 82
 - Comware image redundancy, 82
 - Comware patch package, 82
 - Comware system software image type, 82
 - startup process, 83
- system administration
 - airflow direction configuration, 111
 - automatic configuration, 125
 - automatic-configuration parameter acquisition process, 127
 - banner configuration, 103, 104
 - banner input modes, 103
 - banner types, 103
 - CLI c string/text type argument value entry, 4
 - CLI command abbreviation, 4
 - CLI command entry, 3
 - CLI command history function use, 7
 - CLI command hotkey configuration, 5
 - CLI command hotkey use, 5
 - CLI command keyword alias configuration, 4
 - CLI command keyword alias use, 4
 - CLI command redisplay, 6
 - CLI command-line error messages, 6
 - CLI display command output filtering, 9
 - CLI display command output line numbering, 9
 - CLI display command output management, 13
 - CLI display command output save to file, 11
 - CLI display command output viewing, 13
 - CLI local console port login, 19
 - CLI login authentication modes, 19
 - CLI login overview, 18
 - CLI online help access, 2
 - CLI output control, 8
 - CLI running configuration save, 13
 - CLI undo command form, 3
 - CLI use, 1
 - CLI user interfaces, 18
 - CLI user roles, 19
 - CLI view hierarchy, 1
 - command accounting, 36
 - command authorization, 35, 36
 - common AUX user interface settings, 21
 - common VTY user interface settings, 26
 - configuration file acquisition process, 128
 - configuration file management, 73
 - console login none authentication, 20
 - console login password authentication, 20

- console login scheme authentication, 21
- console port login procedure, 15
- copyright statement display, 103
- deploying and configuring server (automatic configuration), 129
- device management configuration, 102
- device name configuration, 102
- device reboot, 105
- device reboot (immediately at CLI), 106
- device reboot (scheduling), 106
- DHCP server configuration guideline (automatic configuration), 130
- emergency shell file system management, 118
- emergency shell system software image retrieval, 119
- emergency shell use, 118, 122
- enter system view from user view, 2
- entering Tcl configuration view, 131
- file system current working directory change, 71
- file system current working directory display, 71
- file system directory creation, 71
- file system directory management, 71
- file system directory removal, 71
- file system file compression, 70
- file system file copy, 69
- file system file decompression, 70
- file system file delete from recycle bin, 70
- file system file deletion, 70
- file system file information display, 69
- file system file management, 69
- file system file move, 70
- file system file name formats, 68
- file system file rename, 69
- file system file restore, 70
- file system file/folder operation mode, 72
- file system management, 68
- file system storage media formatting, 72
- file system storage media management, 72
- file system storage media repair, 72
- file system text file content display, 69
- login management overview, 14
- memory usage thresholds, 112
- non-ISSU software upgrade procedure, 88
- overall automatic configuration process, 125
- port status detection timer, 112
- return to upper-level view from any view, 2
- return to user view, 2
- returning to user view, 131
- SNMP access control, 34
- software upgrade, 82
- SSH login, 28
- SSH login configuration on device, 28
- SSH login control, 33
- SSH server login, 29
- system operating mode, 105
- task scheduling, 106, 108
- Tcl configuration, 131
- Telnet login, 22
- Telnet login control, 33
- Telnet login device configuration, 23
- Telnet login none authentication, 23
- Telnet login password authentication, 24
- Telnet login scheme authentication, 25
- Telnet server login, 27
- temperature alarm thresholds, 114
- TFTP server configuration guideline (automatic configuration), 130
- time set, 102
- transceiver module diagnosis, 115, 116
- transceiver module verification, 115
- USB interface disable, 115
- user access control, 33

- system software image retrieval, 119
- task list
 - configuration rollback, 76
- task scheduling, 106, 108
- Tcl
 - configuration, 131
 - entering configuration view, 131
 - restrictions, 131
 - returning to user view, 131
- TCP
 - device as FTP client, 60
 - device as FTP server, 57
 - FTP client connection establishment, 60
 - FTP configuration, 57
 - IPv4 TFTP client configuration, 66
 - IPv6 TFTP client configuration, 66
 - TFTP configuration, 66
- Telnet
 - common VTY user interface settings, 26
 - login, 22
 - login control, 33
 - login device configuration, 23
 - login management overview, 14
 - login none authentication, 23
 - login password authentication, 24
 - login scheme authentication, 25
 - server login, 27
- temperature alarm thresholds, 114
- terminating FTP connection, 63
- text file content display, 69
- text type argument value, 4
- TFTP. *See also* FTP
 - automatic configuration, 125
 - configuration, 66
 - emergency shell system software image retrieval, 119
 - emergency shell system software image transfer from server, 120
 - IPv4 client configuration, 66
 - IPv6 client configuration, 66
- threshold
 - memory usage, 112
 - temperature alarm, 114
- time setting, 102
- timer
 - port status detection, 112
- tool command language. *Use* Tcl
- transceiver
 - module diagnosis, 115, 116
 - module verification, 115
- transferring system software image from server, 120
- Trivial File Transfer Protocol. *Use* TFTP
- troubleshooting
 - FTP connection, 63
 - RBAC, 55
 - RBAC local users have more access permissions than intended, 55
 - RBAC login attempts by RADIUS users always fail, 56
- understanding automatic configuration, 125
- understanding command-line error messages, 6
- undo command form, 3
- uninstalling
 - ISSU patch images, 99
- upgrading
 - completing software upgrade, 86
 - ISSU software images, 98
 - non-ISSU software upgrade approach, 85, 88
 - preloading software image to Boot ROM, 85
 - preparing for non-ISSU upgrade, 85
 - software, 82
- USB interface disable, 115

user access

- RBAC configuration, 38, 40
- RBAC feature group configuration, 42
- RBAC HWTACACS authentication user configuration, 52
- RBAC local AAA authentication user configuration, 47
- RBAC permission assignment, 38
- RBAC predefined user roles, 39
- RBAC RADIUS authentication user configuration, 49
- RBAC resource access policies, 39, 42
- RBAC user role assignment, 40, 43
- RBAC user role creation, 40
- RBAC user role interface policy, 42
- RBAC user role local AAA authentication assignment, 44
- RBAC user role non-AAA authentication assignment, 45
- RBAC user role remote AAA authentication assignment, 44
- RBAC user role rule configuration, 41
- RBAC user role rules, 38
- RBAC user role switching, 46
- RBAC user role switching authentication configuration, 46
- RBAC user role switching configuration, 45
- RBAC user role VLAN policy, 43
- RBAC user role VPN instance policy, 43

user access control

- command accounting, 36
- command authorization, 35, 36
- login control, 33

SNMP access control, 34

SSH login control, 33

Telnet login control, 33

user view

- entering configuration view, 131
- returning from configuration view, 131

using

- CLI, 1
- command history function, 7
- command hotkey, 5
- command keyword alias, 4
- device as FTP client, 60
- device as FTP server, 57
- device for SSH server login, 29
- device for Telnet server login, 27
- undo command form, 3

using emergency shell, 118, 122

verifying

- software change confirmation status, 100
- software image integrity and consistency, 100

verifying transceiver modules, 115

viewing CLI display command output, 13

VLAN

- RBAC user role VLAN policy, 43
- RBAC VLAN access policy, 39

VPN

- RBAC user role VPN instance policy, 43
- RBAC VPN instance access policy, 39

VTY user interface settings, 26

working with FTP server files, 61